АПИНО
ICAIT

11TH INTERNATIONAL CONFERENCE
ON ADVANCED INFOTELECOMMUNICATIONS ICAIT 2022

XI МЕЖДУНАРОДНАЯ НАУЧНО-ТЕХНИЧЕСКАЯ
И НАУЧНО-МЕТОДИЧЕСКАЯ КОНФЕРЕНЦИЯ
«АКТУАЛЬНЫЕ ПРОБЛЕМЫ ИНФОТЕЛЕКОММУНИКАЦИЙ
В НАУКЕ И ОБРАЗОВАНИИ»

2022

СБОРНИК НАУЧНЫХ СТАТЕЙ

APINO.SPBGUT.RU

СПбГУТ)))

ИНФОРМАЦИОННЫЕ ПАРТНЁРЫ

НАУЧНО-ТЕХНИЧЕСКИЙ ЖУРНАЛ
ИНФОРМАЦИЯ
КОСМОС

НАУЧНЫЙ ЖУРНАЛ
ТУЗС
«ТРУДЫ УЧЕБНЫХ ЗАВЕДЕНИЙ СВЯЗИ»

ИНФОРМАЦИОННАЯ ПОДДЕРЖКА

WWW.IIT.SUT.RU
ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ
научное рецензируемое издание • электронный научный журнал
Telecom IT — ISSN 2307-1303

УДК 001:061.3(082)
ББК 72 А43

Актуальные проблемы инфотелекоммуникаций в науке и образовании. XI Международная научно-техническая и научно-методическая конференция; сб. науч. ст. в 4 т. / Под. ред. А. В. Шестакова; сост. В. С. Елагин, Е. А. Аникевич. СПб. : СПбГУТ, 2022. Т. 1. 880 с.

В научных статьях участников конференции исследуются состояние и перспективы развития мирового и отечественного уровня IT и телекоммуникаций. Предлагаются методы и модели совершенствования научно-методического обеспечения отрасли связи и массовых коммуникаций.

Предназначено научным работникам, аспирантам и студентам старших курсов телекоммуникационных и политехнических вузов, инженерно-техническому персоналу и специалистам отрасли связи.

Научное издание
Литературное редактирование,
корректура Е. А. Аникевич
Оформление Г. И. Юрьев
Верстка Е. М. Аникевич
Подписано в печать 01.08.2022.
Вышло в свет 31.08.2022. Формат 60×90 1/8.
Уст. печ. л. 55,00. Заказ № 095-ИТТ-2022.
пр. Большевиков, д. 22, корп. 1.
Россия, Санкт-Петербург, 193232

ISBN 978-5-89160-265-6

СОДЕРЖАНИЕ

ПЛЕНАРНОЕ ЗАСЕДАНИЕ

УДК 004; 341.16:001; 378.147; 621.39
ГРНТИ 02.31.31; 06.51.77; 12.09; 49.01.11

ПЕРСПЕКТИВНЫЕ НАПРАВЛЕНИЯ ПО ИТОГАМ ГОДА НАУКИ И ТЕХНОЛОГИЙ В РОССИЙСКОЙ ФЕДЕРАЦИИ И СПбГУТ

А. В. Шестаков

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Научная деятельность Санкт-Петербургского государственного университета телекоммуникаций имени профессора М.А. Бонч-Бруевича развивается в соответствии с мировыми тенденциями в прикладных научных исследованиях прорывных технологий цифровизации всех сфер человеческой деятельности, в том числе в организации и обеспечении подготовки специалистов новой формации по национальным программам и федеральным проектам Российской Федерации. Рассматриваются основные векторы перспективной научной проблематики вуза и изменений концепции гармонизации нормативного регулирования в стране с учетом международной деятельности представителей университета на специализированных площадках различных институтов Организации Объединенных Наций, таких как Исследовательские комиссии Международного Союза Электросвязи и Всемирной Организации по Стандартизации. В створе деятельности организации международного сотрудничества в сфере образования, науки и коммуникаций (ЮНЕСКО) представлены результаты теоретических и практических подходов к реализации концепции мобильного обучения вуза, которые базируются на авторских моделях цифровой трансформации образовательного контента, технологиях доступности к цифровым образовательным ресурсам с учетом современных международных факторов и рисков.

прикладные исследования, технологи, телекоммуникации, цифровая трансформация.

Научная работа Федерального государственного бюджетного образовательного учреждения высшего образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича» (СПбГУТ, Университет) организуется в соответствии с приори-

тетами, целями и задачами, поставленными перед отраслью «Связь» Президентом Российской Федерации, Правительством Российской Федерации, федеральными и региональными органами исполнительной власти, в рамках реализуемых национальных проектов и программ развития Российской Федерации. Нормативная база организации научной деятельности Университета содержит: Указы Президента Российской Федерации «Стратегии научно-технологического развития Российской Федерации» от 01.12.2016 № 642; «О национальных целях развития Российской Федерации на период до 2030 года» от 21.07.2020 № 474. Главными особенностями организации научной работы Университета в 2021 году заключались в проведении Года науки и технологий в Российской Федерации (Указ Президента Российской Федерации от 25.12.2020 № 812) и условия пандемии.

Год науки и технологий продемонстрировал новые вызовы компетенциям. За год в России состоялось более 6 000 мероприятий во всех регионах, которые проводились в различных формах: научно-технологические проекты (22 %), конгрессно-выставочные мероприятия (20 %), конкурсы и соревнования (20%), научно-популярные акции (20 %), мультимедиа (7 %) с участием более 12 млн человек (официальный сайт мероприятий – годнауки.рф). При этом наиболее значимые из них 31 федеральное и 42 регулярных мероприятия, в которых Университет принял активное участие (рис. 1–).

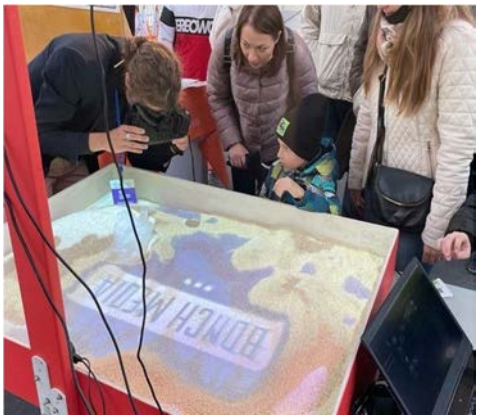


Рис. 1. Спектр решений СПбГУТ для обучения на Фестивале «Техносреда»

Рис. 2. СПбГУТ на Фестивале «Техносреда»: Смотри, учись, делай

Приоритетные направления исследований Университета сфокусированы по основным тематикам, которые соответствуют деятельности учредителя СПбГУТ (Минцифры России) в мировом сообществе, в национальных программах и федеральных проектах, в частности: перспективным цифровым сервисам и инфраструктурам; цифровым сквозным технологиям; информационной безопасности в инфокоммуникациях.

Рис. 3. Образовательный центр «Сириус» Сочи – подведение итогов Года науки и технологий и определение приоритетов российской науки на будущие годы

Основными заказчиками научно-технической продукции Университета являются федеральные органы исполнительной власти (Минцифры России, Минобрнауки, Росатом и др.), головные организации и исполнители национальных проектов и программ.

Направления научно-производственной кооперации Университета традиционные: выполнение совместных прикладных научных исследований (АО «НИИ телевидения», АО «Завод «КРИЗО» и др.); различные формы организации подготовки специалистов (АО «НПП «Радар ммс», ФГУП «Российская телевизионная и радиовещательная сеть» и др.). Достаточно активно развивались онлайн-встречи студентов с представителями предприятий реального сектора экономики, например, компании РТЛабс – разработчиком портала gosuslugi.ru, которая объединяет более 1300 специалистов в 13 офисах по всей стране, и компании DIS Group, которая является частью международного холдинга Aman Group.

СПбГУТ, как и другие подведомственные организации Минцифры России, принимает активное участие в федеральных программах «Кадры для цифровой экономики», «Информационная инфраструктура». По национальной программе «Цифровая экономика Российской Федерации» Университет в 2021 году не только продолжил выполнение текущих научно-исследовательских работ, а на высоко конкурентной конкурсной основе приступил к исполнению ряда новых исследовательских работ по таким тематикам как перспективные сетевые средства (НИР «Мульти-Цод»), технологии проектирования базовых компонент (НИР «Растр») и интеллектуальная транспортная инфраструктура (НИР «Приоритетный проезд», рис. 4). Впервые результаты этих работ были переданы Минцифры России в виде объектов интеллектуальной собственности как нематериальные активы (например, Свидетельство на программу для ЭВМ № 2021681348 от 14.12.2021).

Рис. 4. Натурные испытания элементов экспериментального образца аппаратно-программной платформы предоставления приоритетного проезда регулируемых перекрестков для общественного, грузового и специального транспорта

В апреле 2021 года представители СПбГУТ и ПАО «Ростелеком» впервые участвовали в работе комиссии «ИК-16 – Мультимедиа» сессии МСЭ-Т. В ходе сессии была представлена совместная разработка – проект международного стандарта-рекомендации «Платформа распределенных автомобильных мультимедийных услуг с системой граничных вычислений на основе V2X» на основе научно-исследовательских работ, выполненных СПбГУТ. По результатам сессии «ИК-16 – Мультимедиа» проект поддержан. Новый стандарт планируется представить в 2023 году.

Существенную помощь в международной деятельности Университета такого уровня оказывает научно-исследовательская и испытательная лаборатория ПАО «Ростелеком» в СПбГУТ, соглашение о создании которой было подписано 22.02.2018, торжественное открытие проведено в 2020 году, а в сентябре 2021 года на Форуме МСЭ-Т позиционирование лаборатории – как международного центра исследований, разработок и испытаний инновационного оборудования, технологий и услуг (рис. 5–6).

Рис. 5. Открытие лаборатории (2020)

Рис. 6. Презентация лаборатории на Форуме МСЭ-Т (2021)

Университет продолжил реализацию нескольких перспективных проектов для различных сфер экономики, в том числе атомной энергетики. Например, результаты проекта «Прямой внутренний рециклинг D/T в DEMO с помощью сверхпроницаемых мембран» (руководитель профессор А. И. Лившиц) были успешно апробированы на конференции "World Online Conference on Sustainable Technologies" и обусловили целесообразность подачи заявки о включении представителей СПбГУТ в состав рабочих групп подкомитета ПК 3 «Реакторные технологии» Технического комитета по стандартизации 322 «Атомная техника».

Успешно апробированы новые способы формирования научного задела для новых проектов отрасли на период 2022–2024 годов через прикладные научные исследования Университета (на примере, творческого коллектива по тематике создания сетей связи 2030, включая услуги телеприсутствия с сетевой поддержкой, и экспериментальная проверка решений при подготовке отраслевых кадров).

Практически все подразделения Университета приняли участие в мероприятиях и работах по подтверждению соответствия системы менеджмента качества (СМК) СПбГУТ в сфере разработки продукции международным и национальным требованиям, локальных норм и правил. Сертификат СМК Университета в сфере разработки широкой номенклатуры продукции действует до октября 2024 года.

Публикационная активность Университета в 2021 году, судя по базе данных Российского индекса научного цитирования, имеет многолетнюю тенденцию устойчивого прироста количественных показателей. Аналогичные показатели Университета (рис. 7), зафиксированные по базам данных высокорейтинговых журналов (*Web of Science* и *Scopus*) подтверждают тенденции устойчивого роста и 5 % превышение. В разрезе научного уровня международных публикаций Университета просматривается существенное смещение акцентов в 2021 году в категорию публикаций квартиля Q1 и Q2 в среднем на 30–40 % (рис. 8).

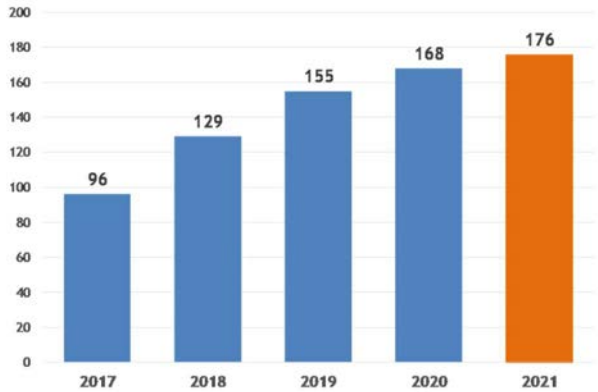


Рис. 7. Динамика международных публикаций

Рис. 8. Фокус группа публикаций

Научный журнал Университета «Труды учебных заведений» существенно поднялся в рейтинге SCIENCE INDEX по тематике «Связь» на 6-е место с 24-го места, и по ряду других показателей. Впервые занял 1-е место в рейтинге по 2-летнему импакт-фактору без самоцитирования по тематике «Связь» из ядра РИНЦ. В перечне справа позиция таких журналов как СибГУТИ (17), ПГУТИ (19) и МТУСИ (23). Другой научный журнал СПбГУТ – сетевое издание «Информационные технологии и телекоммуникации» (ИТТ) – в рейтинге SCIENCE INDEX по тематике «Связь» опережает ТУЗС на 5-м месте, а по тематике «Электроника. Радиотехника» – на 12-м, «Автоматика. Вычислительная техника» – 43. Последовательная редакционная политика и постоянное внимание Ученого совета Университета к развитию научных журналов обеспечивают движение ТУЗС к международному статусу (рис. 9–10), а ИТТ – ВАК.

Рис. 9. Наукометрия ТУЗС

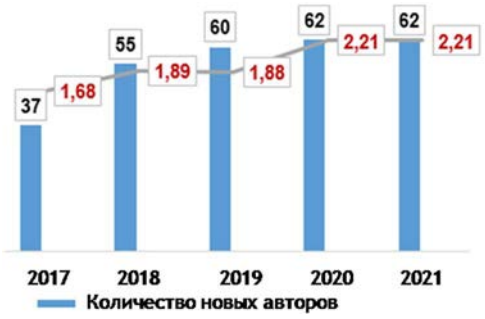


Рис. 10. Прирост числа новых авторов ТУЗС

Характеристики создания и регистрации новых инновационных решений СПбГУТ в Роспатенте соответствуют текущим требованиям (табл.), ведь показатели зарегистрированных результатов интеллектуальной деятельности (РИД) являются обязательными для отнесения Университета к 1-й категории научных и образовательных организаций.

ТАБЛИЦА. Количественный показатели регистрации РИД

Показатели	2016	2017	2018	2019	2020	2021
Количество зарегистрированных в Роспатенте, шт.	10	14	8	21	69	70

В 2021 году конкурсная и грантовая активность подразделений Университета, таких как ИКСС, РТС, ИСИТ по количеству поданных заявок относительно запланированных превышала плановые. Количество побед в конкурсах и полученных грантов в 2021 году составило 25, а в 2020 – 24. Наиболее значимые конкурсные достижения Университета: грант РНФ для поддержки малых отдельных научных групп по тематике; грант МТУСИ-2021 по информационной безопасности; победители конкурса лучших инновационных проектов в сфере науки и высшего образования Санкт-

Петербурга. Проекты СПбГУТ: «Разработка методов, моделей и средств производительности и отказоустойчивости программно-определяемых систем хранения данных с помощью автоматизированного контроля и анализа диагностической информации с использованием нейронной сети» и «Применение метода реагентной ультрафильтрации для повышения экологической безопасности гидрометаллургических методов переработки электронных отходов» (рис. 11–12).

Рис. 11. Награда «Лучшая инновационная идея»

Рис. 12. Награждение авторского коллектива СПбГУТ

В рамках федерального проекта «Информационная безопасность» национальной программы «Цифровая экономика Российской Федерации» 18.11.2021 состоялся финал олимпиады «КиберСПбГУТ» для студентов университетов СЗФО на базе СПбГУТ. В финале олимпиады приняли участие 8 команд из разных вузов Санкт-Петербурга (СПбГУТ, ФГБОУ ВО «ГУМРФ имени адмирала С. О. Макарова», ФГАОУ ВО «СПбПУ», ФГАОУ ВО ГУАП, Университет ИТМО), Архангельска (САФУ имени М. В. Ломоносова), Петрозаводска (ПетрГУ) и Калининграда (ФГБОУ ВО «Калининградский государственный технический университет»).

Победители олимпиады: 1 место – команда «Null_none» (СПбГУТ); 2 место – команда "TTPI" (САФУ имени М. В. Ломоносова); 3 место – команда "PTZCTF" (ПетрГУ) (рис. 13–14).

Год науки и технологий научные конференции Университета отметили юбилеями: X Юбилейная международная конференция АПИНО 2021; 75-я Региональная конференция Студенческая весна – 2021.

Рис. 13. Олимпиада «КиберСПбГУТ»

Рис. 14. Финал олимпиады «КиберСПбГУТ»

В конференции АПИНО 2021, Международной научно-технической и научно-методической конференции «Актуальные проблемы инфотелекоммуникаций в науке и образовании», которая интегрировала серию пленарных заседаний и круглых столов, тематических секций и выставку научно-технических разработок, приняли участие более 100 человек: представители телекоммуникационных и IT компаний, ученые, аспиранты и студенты, а также партнеры – ООО «Сертек», ООО «НТЦ Аргус», ООО «Т8» (рис. 15–18).

Рис. 15. АПИНО 21: Регистрация

Рис. 16. АПИНО 21: Выставка

Рис. 17. АПИНО 21: Пленарное заседание

Рис. 18. Бачевский С. В.: доклад

Несмотря на условия пандемии в «Студенческой весне – 2021» приняли участие около 700 человек, а на заседаниях 27 секций было заслушано около 600 докладов, из которых наиболее значимые были опубликованы в 87 статьях 2-х -томника и 23-х статьях специального выпуска.

В Год науки и технологий в рамках конференции АПИНО 2021 проведен Круглый стол «Открытия в СССР и России», модератором которого выступил Георгий Николаевич Фурсей, лауреат Государственной премии СССР, Заслуженный деятель науки РФ, почетный работник высшего и среднего профессионального образования РФ, Кавалер ордена Дружбы, доктор физико-математических наук, почетный профессор СПбГУТ, Председатель Санкт-Петербургского отделения РАЕН. Тематика Круглого стола – 55-летие научного открытия взрывной электронной эмиссии, обнаруженной группой ученых Томского политехнического института и ленинградской науки (рис. 19–20).

Рис. 19. Георгий Николаевич Фурсей

Рис. 20. Круглый стол «Открытия в СССР и России» в режиме онлайн

В 1966 году Комитет по делам изобретений и открытий при Совете Министров СССР признал явление взрывной электронной эмиссии открытием № 176. Документом учтены результаты исследований Георгия Фурсея и Павла Воронцова-Вельяминова, молодых ученых нашего города, которые показали, что появление вакуумной дуги инициируется не просто нагревом и испарением микроэмиттеров (микроострий), а их взрывом. Результаты послужили основой для разработки методов генерирования сверхмощных электрических импульсов, потоков заряженных частиц и электромагнитных излучений, их воздействия на вещество, а также развития физики вакуумного и газового разрядов. Обеспечен прорыв в сверхвысокочастотных генераторах, мощных ускорителях электронов и лазерах на основе объемного электрического разряда в газе повышенного давления.

В СПбГУТ успешно проведена вторая Всероссийская научно-методическая конференция магистрантов и их руководителей (ПКМ-21), в которой в режиме онлайн участвовало более 600 человек из 20 вузов Санкт-Петербурга, Москвы, Казани, Новосибирска, Самары, Омска, Томска и других городов России. На пленарном заседании выступили с докладами Министр связи и информационных технологий Архангельской области П. А. Окладников, первый проректор-проректор по учебной работе СПбГУТ Г. М. Машков, директор института магистратуры СПбГУТ А. Н. Бучатский и другие (рис. 21–22).

Рис. 21. ПКМ-21: Окладников П. А.

Рис. 22. ПКМ-21: Бучатский А. Н.

СПбГУТ традиционно для декабря календарного года провел XXIII Международный Коммуникационный Балтийский Форум «Глобальные и региональные коммуникации: настоящее и будущее» (BAFO-2021) – масштабное научно-практическое мероприятие, цель которого – обмен актуальными знаниями, развитие профессиональных навыков, установление и поддержание контактов между студентами, преподавателями и представителями деловой среды. Партнеры Форума: копицентр OQ, мастерская рекламы Advertka, компания 3D Printy, Державинский институт, Городской студенческий пресс-центр. В программу BAFO-2021 включены: студенческая научно-практическая конференция и конкурс докладов; научно-практическая конференция преподавателей, аспирантов и магистрантов; мастер-классы и тренинги по развитию профессиональных навыков и soft skills; Круглый стол «30 лет с момента распада СССР: причины, события и исторические последствия»; Круглый стол «Инновации в политическом управлении: влияние цифровой трансформации на гражданскую активность» (Проект *Erasmus+ Jean Monnet* №°620089-EPP-1-2020-1-RU-EPPJMO-MODULE «Цифровая трансформация европейского управления, политики и общественных коммуникаций»).

На Межвузовском научном семинаре «Искусственный интеллект: математика и сети связи» (руководители семинара д.т.н., профессор А. Е. Кучерявый и д.т.н., профессор К. Е. Самуйлов), впервые организованном СПбГУТ и РУДН, в ноябре 2021 года была продемонстрирована модельная лаборатория услуг телеприсутствия на базе кафедры ССиПД СПбГУТ (рис. 23–24). Состав участников семинара был достаточно представительным: СПбГУТ, РУДН, ИПУ РАН им. В. А. Трапезникова, ИПМ РАН им. М. В. Келдыша, СПбГЭТУ «ЛЭТИ», ПАО «Ростелеком», МИЭМ им. А. Н. Тихонова, ВлГУ им. А. Г. и Н. Г. Столетовых, МТУСИ, ПГУТИ, ГУАП, НИИР им. М. И. Кривошеева, Tampere University (*Finland*), Egypt-Japan University of Science and Technology (E-JUST), Zagazig University (*Egypt*), Menoufia University (*Egypt*), Jeju National University (*R.Korea*), Al-Azhar University (*Qena, Egypt*), Arab Open University and Sohar University (*Oman*). По результатам обсуждения итогов семинара принято решение о необходимости ознакомления мировой научной общественности с успехами российской науки в области искусственного интеллекта в сетях и системах связи.

Рис. 23. Руководители научного семинара «ИИ: математика и сети связи»

Рис. 24. Модельная лаборатория услуг телеприсутствия

В Нанкине (КНР) с 21 по 25 июня 2021 года прошла Неделя технологий (2021 *Nanjing Tech Week*), организованная Министерством науки и технологий КНР, а также департаментом науки и технологий провинции Цзянсу и города Нанкин. В мероприятии в онлайн формате приняли участие ведущие российские университеты: СПбГУТ, СПбГУ, СПбПУ, СПбГЭТУ «ЛЭТИ», МГТУ им. Н. Э. Баумана, Университет ИТМО и др. На совещании глав учебных заведений в рамках конференции проректор по научной работе СПбГУТ представил результаты научных исследований университета, вклады, подготовленные учеными университета для МСЭ и ВОС, и пригласил коллег к международному научно-техническому сотрудничеству.

СПбГУТ 15.04.2021 впервые принял участие в работе рабочей группы SE Комитета по электронным средствам связи Европейской конференции администраций почт и электросвязи в составе группы «Полевые измерения

активных антенных систем» проектной группы SE21» с целью разработки методологии полевых измерений характеристик базовых станций 5G с активными антеннами системами на основе эквивалентной изотропно-излучаемой мощности в рабочей полосе частот, а также в области внеполосных и побочных излучений и методологии расчета суммарной излучаемой мощности в рабочей полосе частот.

Возросла активность научной деятельности студентов, что в условиях пандемии было существенным прогрессом. Заслуживает особого внимания рост количества научных публикаций, выполненных студентами без соавторства, а также высокий научный уровень, что безусловно необходимо развивать и поощрять.

Значительно увеличилось количество участников студенческого научного общества Университета в различных конкурсах. Комитет по научной работе Студенческого совета СПбГУТ совместно с научно-образовательными центрами и исследовательскими лабораториями Университета (НОЦ «Технологии информационных образовательных систем», НОЦ «Программно-определяемые системы», НОЦ «Медиацентр», НИЛ «Интернет вещей») провел 1 сентября 2021 года для первокурсников квест "Trail of science" цель которого – познакомить студентов с научными центрами и лабораториями вуза, расширить кругозор и продемонстрировать, что наука является не только интересной, но и доступной (рис. 25). СПбГУТ 26.10.2021 года стал одним из пяти российских вузов, принимающих однодневные фестивали Huawei Cup 2021 – Евразийские соревнования в сфере ИКТ для студентов и молодых специалистов (рис. 26).

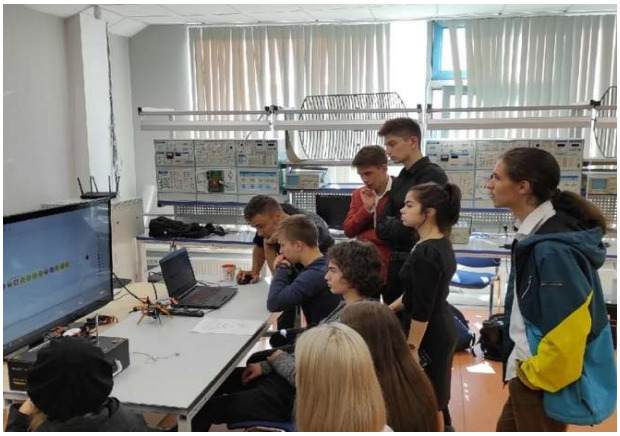


Рис. 25. Участники Trail of science

Рис. 26. Участники Huawei Cup 2021

Участники фестивали Huawei Cup 2021 попробовали свои силы в нескольких номинациях: 5G (Технологии и стандарты мобильной связи нового поколения), AI (Модели и методы искусственного интеллекта), Storage (Компоненты ЦОД), IP (Технологии и протоколы IP-сетей),

APP (Проектирование мобильных приложений Huawei), ICT Observer (ИКТ-Обозреватель).

СПбГУТ 25–26.11.2021 принял участие в III Всероссийских соревнованиях по перспективным направлениям развития радиосвязи «Радиофест-2021», которые организовали Минпромторг России, Минобрнауки России, Фонд перспективных исследований, Технополис «Москва» и НИУ «МИЭТ» Команда "Bonch_tx" стала победителем в направлении «Радионавигация»; команда "Bonch_rx" заняла второе место в направлении «Радионавигация» и третье место в направлении «Радиосвязь», а также получила специальный приз от Минобрнауки России «За самое точное решение» (рис. 27–28).

Рис. 27. Радиофест-2021

Рис. 28. СПбГУТ: Радиофест-21

В конкурсах наиболее важными являются победы в таких как «Я-профессионал», «Радиофест-2021» и ряде других (рис. 20). В 2021 году студентами Университета завоевано 39 призовых места, в то время как в 2020 только 36.

Общее распределение аспирантов Университета по направлениям подготовки характеризуется традиционным предпочтением направлений связи, информатики и информационной безопасности (по 11, 09 и 10 укрупненным группам подготовки).

На базе СПбГУТ успешно работают диссертационные советы: 55.2.004.01 (Д 219.004.04) по двум специальностям; 99.2.038.03 (Д 999.121.03) (объединенный) по трём специальностям; на базе ОАО «Авангард»: ДСО 999.017.02 (409.027.02) (объединенный) – по двум специальностям. Всего в 2021 году в ДСС защищено 17 диссертаций, а в 2020 – 16. Научно-педагогическими работниками Университета в 2021 году защищено 10 диссертационных работ, из них докторских – 2, кандидатских – 8 (рис. 29–30). Количество аспирантов, успешно защитивших кандидатские диссертации – 8, как и в предыдущем году.

Рис. 29. Лобастова М.В.
на защите диссертационной работы

Рис. 30. Аспирант Фан Ван Дай
на защите диссертационной работы

СПбГУТ в 2021 году с направлением перспективных инфокоммуникационных технологий вошел в состав межвузовской кооперации, сформированной СПбГЭТУ «ЛЭТИ», как победитель гранта Минобрнауки России «Территориальное и (или) отраслевое лидерство» (группа 2) в реализации новой программы «Приоритет-2030» в рамках федерального проекта «Исследовательское лидерство» из национального проекта «Наука и университеты». По федеральному проекту «Интеграция» Университет вошел в состав консорциума «Арктический Альянс «Холодные земли» для развития кадрового потенциала в научно-технологической сфере и обеспечения подготовки квалифицированных научных кадров, сформированном Правительством Республика Саха (Якутия) – победителем гранта межрегионального НОЦ мирового уровня «Север – территория устойчивого развития», в котором участвуют 5 регионов Российской Федерации, 9 университетов, 18 научных организаций и 17 организаций реального сектора экономики.

Инициативы СПбГУТ основывались на опыте формирования НОЦ мирового уровня «Цифровые экосистемы всепроникающих сетей, NET-2030 и сетей 5G» в 2019 году и Меморандуме о сотрудничестве по созданию в Санкт-Петербурге НОЦ мирового уровня в области сетей 5G в партнерстве с Правительством Санкт-Петербурга, ПАО «Ростелеком», ГУАП, СПбГЭТУ «ЛЭТИ» и Университет ИТМО, подписанном на площадке II Петербургского цифрового форума 29.08.2019 (рис. 31–32).

Рис. 31. Подписание Меморандума

Рис. 32. Проект СПбГУТ на рабочей группе
Госсовета Российской Федерации

Университетом в октябре 2021 года по запросу Комитета по Арктике Санкт-Петербурга согласно Плану мероприятий по реализации Стратегии развития Арктической зоны и Основ государственной политики в Арктике (Распоряжение Правительства РФ от 15.2021 № 996-р) была сформирована кооперация предприятий промышленности научно-производственного Арктического кластера Санкт-Петербурга (ПО «Интелтех», ОАО «СУПЕРТЕЛ») и представлена заявка на выполнение проекта «Полярный экспресс-3 Комм» по созданию защищенных коммуникационных ресурсов (сервисов) с интегрированной системой управления ресурсами (сервисами), промышленной, технической и информационной безопасностью для критически важных инфраструктур морских портов Арктического региона (Северного морского пути) на основе защищенных коммуникационных порталов на объектах проекта «Полярный экспресс» – береговых станций с оборудованием линейного волоконно-оптического тракта трансарктической подводной волоконно-оптической линии связи Мурманск – Владивосток.

Пандемия COVID 19 внесла значительные коррективы в процесс обучения, еще значительнее сместив фокус предпочтений участников образовательного процесса в сторону электронного формата взаимодействия с использованием современных цифровых технологий. Повышение доступности информации и изменение способов ее представления, переосмысление форм и методов организации и проведения учебного процесса, апробирование новых моделей и методов, в том числе, на основе системы знаний о технологиях и содержании (TPACK, *Technology Pedagogical and Content Knowledge*) требуют модификации существующей системы образования.

В условиях цифровой трансформации и динамично меняющейся информационной образовательной среды, одной из главных тенденций в образовании становится m-Learning (*mobile-Learning*) – разновидность электронного обучения (*e-learning*), которое предполагает обучение с применением индивидуальных электронных коммуникационных средств.

Смартфоны и планшетные компьютеры дают обучающимся возможность обращаться к необходимой информации в любой момент времени при условии наличия сети, что позволяет сделать процесс обучения технологически непрерывным. Технология m-Learning предполагает наличие инструментов, которые повышают скорость получения информации, обеспечивают возможность своевременной актуализации представленного материала посредством использования облачных технологий.

Одним из таких инструментов является применение QR-кодов в образовательном процессе, использование которых было предложено в концепции регламентированного смещения образовательного и дидактического контента учебного материала в доверенные цифровые электронные ресурсы.

Концепция впервые была реализована в Университете в соответствии с формальным ее описанием на множестве отношений (К) как: К = <Q, C, F{S, P→T, W}>, где S, W, P, T – подмножество структурных компонент и контента учебного материала и информационных ресурсов, компонент TRACK и ядра трансформации соответственно.

Графическое представление модели цифровой трансформации контента учебного материала на множестве отношений (К) приведено на рис. 33.

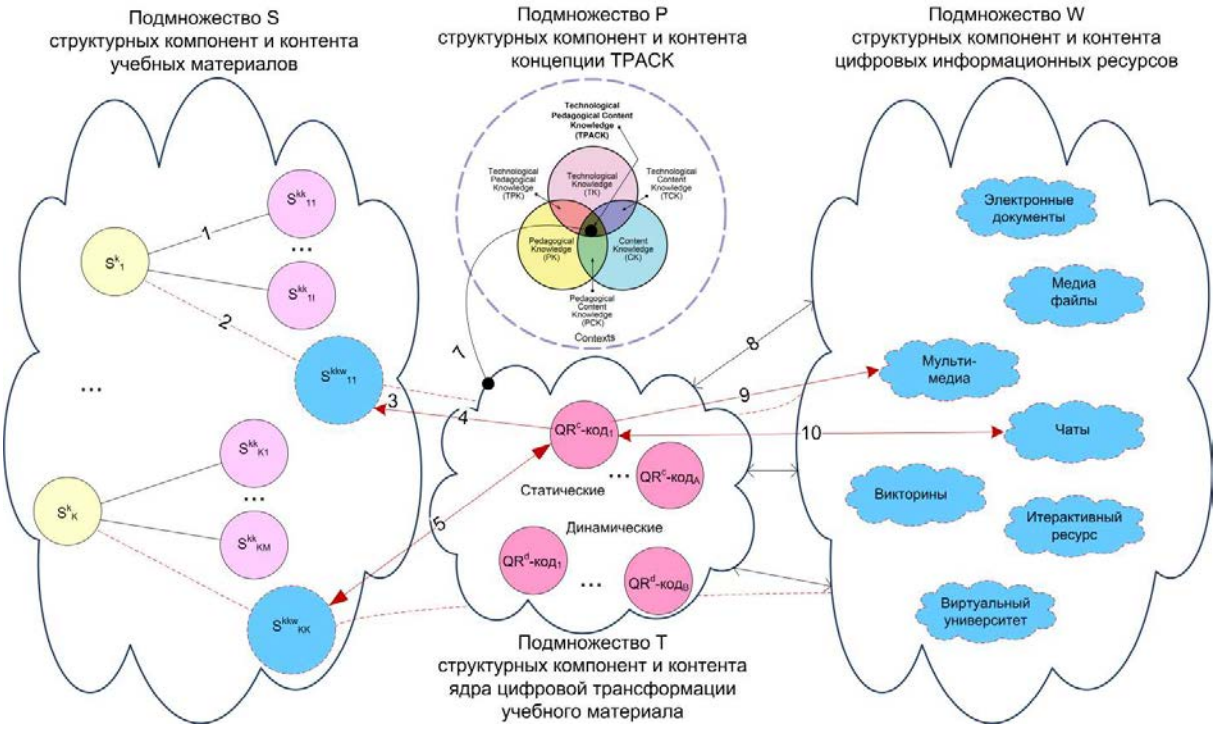


Рис. 33. Модель цифровой трансформации контента учебного материала

Предложенная концепция обеспечивает достижение целей, сформулированных в рекомендациях ЮНЕСКО: создание, популяризация образовательных ресурсов для использования на мобильных устройствах; использование мобильных технологий для повышения качества управления коммуникациями и образовательным процессом; расширение и улучшение способов, гарантирующих равный доступ к ресурсам. Кроме того, концепция позволяет структурировать основные элементы образовательного контента и реализует идею непрерывного и эффективного образовательного процесса за счет возможности актуализации учебного материала.

В условиях динамично меняющей мировой ситуаций российская система высшего образования сталкивается с необходимостью модификации существующих способов преподавания, перехода к использованию современных образовательных технологий, адаптированных под обучающихся

и более понятных им, а также смещению образовательного контента в цифровые ресурсы. Повышение доступности информации и изменение способов ее представления дает возможность преподавателю изменить структуру и качество преподаваемого материала, предложив обучающемуся различные варианты познания, взаимодействия и оценки знаний.

Вклад университетской науки в мониторинг результативности деятельности научных организаций (БД РД НО) по показателю «Популяризация науки и технологий» характеризуется не только новостной и событийной лентой Университета в сети интернет, а также и сведениями на сайтах Правительства Санкт-Петербурга и Минцифры России и других информационных ресурсах средств массовой информации. Рубрикатор новостной ленты охватил все мероприятия Университета, посвященные Году науки и технологий, с их активной 10 % динамикой (рис. 34–35).

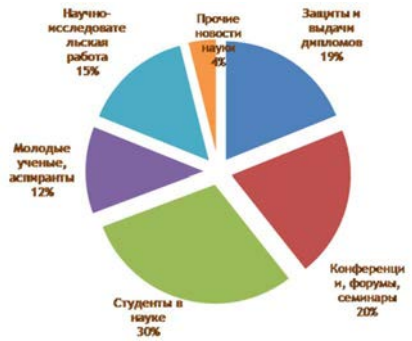


Рис. 34. Рубрикатор новостной ленты

Рис. 35. Динамика новостной ленты СПбГУТ

СПбГУТ в 2021 году по отношению к другим подведомственным вузам Минцифры России добился лидирующих показателей, практически по всем позициям: от результатов интеллектуальной деятельности и публикационной активности, до качества подготовки научных кадров и объемов, выполненных научных работ по актуальным направлениям развития цифровой экономики Российской Федерации.

К тематике перспективных направлений по итогам науки и технологий в Российской Федерации и СПбГУТ, по нашему мнению, целесообразно отнести: технологии программно-конфигурируемого радио; промышленный интернет вещей; речесинтезирующие технологии двойного назначения; алгоритмы обработки адаптивных антенных систем; технологии промышленного проектирования РЭС; технологии натурного моделирования инфраструктуры связи; гармонизации регуляторных изменений с требованиями спецпотребителей.

УДК 004.77
ГРНТИ 49.38.99

МИГРАЦИЯ ИНТЕЛЛЕКТУАЛЬНЫХ УСЛУГ В РАСПРЕДЕЛЕННОЙ СРЕДЕ КАК ОДНО ИЗ КЛЮЧЕВЫХ НАПРАВЛЕНИЙ РАЗВИТИЯ ИНФОКОММУНИКАЦИЙ

А. С. А. Мутханна

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Сети 5G и следующие поколения предназначены для интеграции всех сетей мобильной и фиксированной связи для обеспечения сверхвысоких скоростей передачи данных, что позволяет использовать ряд новых услуг с новыми структурами облачных вычислений, такими как туманные вычисления и граничные вычисления. Важным направлением развития технологий коммуникационных сетей являются URLLC (Ultra-Reliable Low Latency Communication), которые создается в целях достижения минимально возможных показателей задержки, сохраняя высокую надежность передачи. В этой статье основное внимание будет уделено технологии URLLC. Эта задача должна решаться за счет использования Искусственного интеллекта и инструментов живой миграции с учетом современных тенденций в области коммуникаций.

5G, миграция сервисов, граничные вычисления.

Введение

Всем знаком закон Мура о росте вычислительной мощности микроэлектроники. Однако скорость роста технологий, возникающих на основе открывшихся возможностей микроэлектроники еще не формализована и не оценена. На протяжении 20-го века, основной связью считалась телефонная связь, где использовалась коммутация каналов, понятная и четкая логика и алгоритмика расчета нагрузки в сетях связи. Однако, за последние 20 лет, технологии связи стали меняться со скоростью, не позволяющей оценить все возможности, которые появились «в руках» человечества [1]. В частности появились такие концепции, как Интернет Вещей и его направления, такие как: Умный город, Умный дом, Умное сельское хозяйство и так далее, следуя логики критеризации направления деятельности человека. Данный объем возможно оценить через призму случившегося на данный момент мягкого перехода (естественного перерождения) концепции сетей связи пятого поколения к сетям связи 6G [2]. Если провести оценку множества появившихся в последнее время исследований в области инфраструктурных

технологий сетей связи, их приложений, а также международных регламентирующих документов (рекомендаций и стандартов), можем заметить, что концепция сетей связи 6G представляет собой комплекс неразрешенных задач и тех идей, которые не были реализованы в рамках сетей связи пятого поколения и/или отсутствовала технологическая возможность их реализации. Под отсутствием технологической возможности подразумевается определенный ряд ограничений, сложившихся на основе физических фактов и противоречий. К примеру, всем известное требование к круговой задержке 1 мс для URLLC-услуг сетей связи, с одной стороны является вроде и реализующимся требованием, но с другой стороны, если взять во внимание диаграмму сетей связи «в любом месте, в любое время, с любого устройства», то мы увидим естественное противоречие (в данном случае лучше использовать наверное термин «ограничение») через призму закона распространения света, в частности в оптоволокне. Так, появились различные исследования, затрагивающие вопросы либо решения данных ограничений через пересмотр технологий физического уровня модели OSI, либо децентрализации сетей связи и систем вычислений [3]. В данной статье будет рассмотрен второй вектор решения задачи предоставления требований услуг URLLC-сетей.

Следуя концепции сетей 5G/IMT-2020, где были определены «три кита», на которых она должна базироваться, а именно: URLLC (*Ultra-reliable Low Latency Communications*), EMB (*Enhanced Mobile Broadband*) and MMTC (*Massive Machine Type Communications*), а также определенным направлениям услуг,

При этом, стоит обратить внимание на достаточно справедливое требование к современным и перспективным системам связи и в общем – инфокоммуникациям, а именно к необходимой мягкой их интеграции между собой с поддержкой множества интерфейсов, в том числе открытых интерфейсов с разделением на абстрагированные (логически) уровни.

В данной статье будет рассматриваться вопрос перераспределения вычислений в сетях 5G с целью предоставления требований URLLC-сети. В частности, данный вопрос будет рассматриваться через призму использования систем для URLLC приложений, учитывая рекомендации Международного Союза Электросвязи F.749.3, а также архитектуру сетей связи IMT-2020, описанную в Y.3102

Распределение вычислений – задача, требующая новых подходов к использованию математически обоснованных инструментов. В рамках данной статьи будет рассматриваться выгрузка трафика с последующим определением устройства и/или группы устройств, на которые будет произведена миграция трафика на обработку [4, 5]. Как пример в статье рассматривается вопрос реализации технологий MEC и SDN для внедрения приложений URLLC.

Переход от централизованных к децентрализованным системам

Ключевая цель сетей 5G заключается в обеспечении нового класса виртуальных приложений с разнородными и чрезвычайно сложными требованиями. Поэтому сообщество 5G использует технологии SDN, NFV и MEC. Они «заточены» на процессе, который превратит инфраструктуры сетевых операторов в распределенные центры обработки данных с расширенными возможностями виртуализации.

В рабочей группе ETSI MEC (WG) указано, что MEC использует платформу виртуализации для запуска приложений на границе мобильной сети [6]. NFV предоставляет платформу виртуализации для сетевых функций путем делегирования и переноса сетевых функций от специализированных выделенных устройств на универсальные сервера. Учитывая схожесть требований к инфраструктуре обоих подходов, целесообразно применение конвергентной инфраструктуры виртуализации. В соответствии с определением 3GPP и MGMN сетевой сегмент представляет собой логическую сквозную сеть, предоставляющую определенные сетевые услуги 5G (например, поставщик телекоммуникационных услуг TSP). Однако до настоящего времени комплексное использование взаимодополнения технологий NFV и MEC, а также их интеграция и взаимодействие в экосистеме 5G до сих пор в значительной степени не изучены.

Объединение технологий SDN/NFV и MEC/Fog позволит достичь следующих целей [7, 8]:

– быстрая масштабируемость сети и облаков;
– полный контроль потоков передачи данных;
– разделение ресурсов;
– повышенная устойчивость и самовосстановление;
– быстрая живая миграция услуг в любую точку сети и возможность разработки сервисов Искусственного интеллекта по модели SaaS.

Достижение вышеуказанных целей обеспечит возможность предоставления тех требований к качеству предоставляемых услуг, которые стали вызовом для всего мирового научного сообщества.

Использование микросервисной архитектуры в граничных вычислениях

Облачные вычисления основаны на концепции микросервисов. Приложения разбиваются на граф локальных облачных микросервисов. Каждый граф имеет небольшие, но конкретные цели обработки. Он упаковывается в независимые виртуальные среды выполнения тем самым достигается высокая гибкость и масштабируемость. Центральный объект – оркестратор приложений, отвечает за реализацию бизнес-логики приложения, управляет

жизненным циклом и взаимосвязью микросервисов через облачные ресурсы [9].

В зависимости от особенностей приложения оркестратор может изменять граф приложения, добавляя/удаляя новые:

– типы микросервисов для включения/обновления определенных функций приложения;

– экземпляры существующих типов микросервисов для масштабирования общей вычислительной мощности приложения, где это необходимо.

Вышеуказанные операции обычно поддерживаются с помощью подходящего управления сетевыми соединениями. Например, операции горизонтального масштабирования выполняются за счет балансировки нагрузки трафика на прикладном уровне внутри одного и того же микросервиса или запрашивается как услуга для менеджеров виртуальной инфраструктуры.

Модельная сеть микросервисных архитектур

В лаборатории ССиПД был разработан стенд для микросервисной архитектуры (рис.), в котором в режиме «реального времени» передавались тактильные ощущения от перчатки с датчиками робо-руки. Но данный стенд был доработан, так как ранее в нём применялась плата Arduino, которая работала с частотой ~ 16 МГц. Был проведён эксперимент, в котором плата Arduino не применялась в стенде и была заменена на Wi-Fi модули ESP 32, у которых частота ровнялась ~ 160 МГц, что примерно в 10 раз выше, чем у платы. В итоге остались только 2 Wi-Fi модуля, что помогло делать вычисления на высоких скоростях с наименьшей задержкой в дальнейшем.

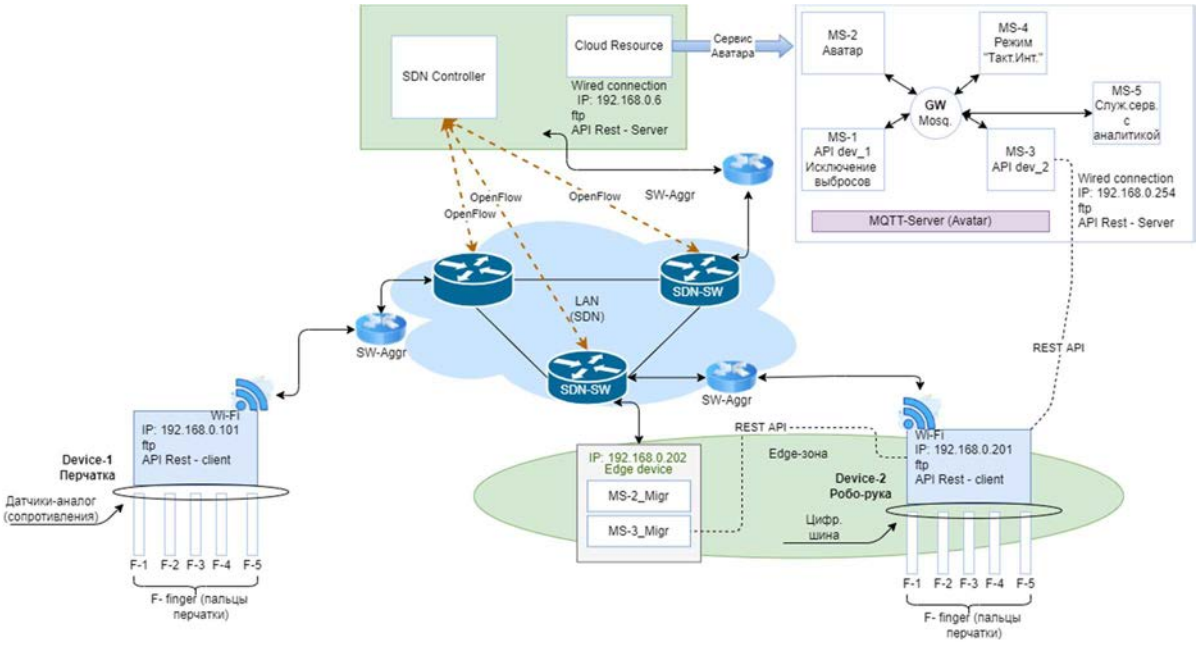


Рисунок. Модельная сеть

Система на рисунке подразумевает собой архитектуру сети SDN (программно-определяемая сеть) – это сеть передачи данных, в которой уровень управления сетью отделён от устройств передачи данных и реализуется программно, которая позволяет создать более гибкие и экономически эффективные сети.

Ключевые особенность SDN:

- Отделение плоскости управления сетью (контроллер SDN) от плоскости передачи данных.
- Логически централизованный контроллер, взаимодействующий с плоскостью данных по открытым и стандартизированным интерфейсам и протоколам (OpenFlow).
- Управляющие приложения (Rest API), работающие поверх контроллера.

Так же, как и сеть SDN наша схема делится на 3 уровня. Плоскость данных или инфраструктурный первый уровень в схеме служит основой для архитектуры SDN. Эта плоскость состоит из физических и виртуальных сетевых устройств, таких как коммутатор, в нашем случае, с 3 портами (оранжевые провода в лаборатории). Эти устройства реализуют протокол OpenFlow (стандартный протокол, является основным элементом концепции SDN, который обеспечивает взаимодействие контроллера с сетевыми устройствами) для поддержания связи с плоскостью управления (вторым уровнем), а также реализуют стандартные методы пересылки трафика с использованием правил потока. На этом уровне находится вся наша локальная сеть SDN с роутерами (SDN-SW).

Второй уровень управления помогает оптимально распределять запросы услуг на первом уровне инфраструктуры используя динамическую настройку. Он действует как мозг для всей сетевой экосистемы. Плоскость управления отделена от базовой инфраструктуры плоскости данных для обеспечения единого централизованного представления всей сети. Плоскость управления использует OpenFlow для связи с устройствами плоскости и обмен этими данными с сетевыми приложениями, работающими в плоскости приложений. Контроллер SDN – это логически отдельная структура, отвечающая за получение инструкций от прикладного уровня (уровня приложений) и их реализацию на устройствах плоскости данных. Он также отвечает за сбор информации о сетевых устройствах, событиях и статистике. На уровне управления данные переходят на коммутаторы агрегации SW-Aggr. Они объединяют физические каналы, предназначенные для передачи данных, в единый логический канал и второй задачей, которую решают коммутаторы агрегации – обеспечение отказоустойчивости: в случае выхода из строя одного из каналов, данные будут передаваться по остальным каналам, находящимся с ним в «связке».

Третий уровень – уровень приложения или доступ (как в архитектуре Cisco), на котором у нас находятся 2 девайса: первый – перчатка с регистрами, а второй – робо-рука с сервоприводом в граничной Edge-зоне, в которой записываются и отправляются данные на Cloud Resource с сервером MQTT для робота-аватара.

Message Queue Telemetry Transport (MQTT) – это сетевой протокол обмена сообщениями по шаблону издатель-подписчик (pub/sub). Он общается путём пересыла сообщения о своём состоянии с помощью Wi-Fi сети и брокера, который слушает сеть, получает и передаёт полученные данные(значения), а также хранит их при необходимости.

Устройства протокола MQTT:

Клиент (client), который делится на:

– издателя (publisher);
– подписчика (subscriber);
– брокером (broker) или сервер.

Кроме всего прочего используется понятие топик – это канал отправки и получения сообщений между устройствами.

Здесь же появляются программные интерфейсы приложения API (*Application Programming Interface*), а в частности для нашей схемы применяется архитектурный стиль Rest API? который отвечает за все взаимодействия между сервером и клиентом и позволяет использовать для общения между программами протокол HTTP (зашифрованная версия – HTTPS), например, с помощью URL-адресов мы можем запросить нужные нам данные. Так же есть FTP (File Transfer Protocol) – протокол передачи файлов по сети.

Предметом исследования является организация передачи кинестетической информации – представляющую положение и движение конечностей, генерирующие механические рецепторы, которые находятся в сухожилиях, мышцах и суставах человека, посредством разработанного программно-аппаратного комплекса, который описывается ниже.

Основным результатом является разработка программно-аппаратного комплекса для сбора, передачи и воспроизведения кинестетической информации, а также миграция сервиса «сглаживание ошибок» с сервера MQTT на граничный сервер. Практическая значимость работы состоит в возможности реализации Тактильного Интернета при помощи разработанного программно-аппаратного комплекса и изучении взаимодействия роботизированной и человеческой руки.

Идея всего эксперимента заключается в разработке веб-серверного приложения, которое будет находиться между перчаткой и робо-рукой. Данное приложение должно реализовывать принцип микросервисной архитектурой с возможностью мониторинга происходящих процессов между микросервисами.

Вся миграция будет заключаться в разработке и создании веб-сервисного приложения, которое мы записываем (мигрируем) на граничный сервер, создавая/делая подписчиков sub_service Glove и sub_service Hand. На рис. показана схема передачи данных (сигналов) на сервере MQTT с перчатки (Glove) и робо-руки (Hand) посредством топиков (Status_Glove, Glove, Glove_results, Hand_results, Hand, Status_Hand) и обработка этих данных на sub-сервисах (Glove Process, Hand Process), использованных в натурном эксперименте. Обе стороны отправляют данные на свои топики, а сервисы получают данные от этих топиков, обрабатывают их и отправляют на другие топики. При этом Glove и Hand подписаны на топики друг друга.

Наша перчатка отправляет данные на топик Glove. Этот топик отправляет данные на sub-сервис Glove Process, обрабатывает их и отправляет на топик Glove-results. Робо-рука же будет направлять данные (с датчика температуры, давления) на топик Hand и sub-сервис Hand Processing будет получать данные от этого топика и направит их на топик Hand-results. Боссами являются sub-сервисы на сервере MQTT, и они будут ждать вопросы от наших устройств (например, про калибровку). Топики Status Glove и Status Hand помогают общаться о своих состояниях робо-руки и перчатки (например, сделать ли калибровку).

С усовершенствованием эксперимента возможно добавление на сервер sub-сервиса Искусственного Интеллекта, который сможет сам определять, как действовать с данными (куда направить, какие записать и хранить, управлять конфигурациями на наших сервисов на сервере, будет иметь доступ ко всем топикам и т. д.) и будет реализован топик Data_Store с sub-сервисом Data_Store service.

Заключение

Приложения сети URLLC требуют пересмотра принципов построения существующих и перспективных сетей связи, в том числе и сетей связи пятого поколения. Основной проблемой при этом является реализация требований по круговой задержке величиной в 1000 мкс. Для борьбы с ними используют такие технологии как: NFV, MEC, SDN, и миграция сервисов. На сегодняшний день область сетевых технологий расширяется во всех направлениях. Увеличение ширины канала, улучшение скорости работы оборудования уже не приносит значимых результатов, ведь требования к URLLC и пятому поколению мобильной сети передачи данных превосходят все из известных физических явлений.

Список используемых источников

1. Мутханна, А. С. Интеллектуальная распределенная архитектура сети связи для поддержки беспилотных автомобилей // Электросвязь. 2020. № 7. С. 29–34.

2. Al-Ansi, A., Al-Ansi, A. M., Muthanna, A., Elgendy, I. A., & Koucheryavy, A. (2021). Survey on intelligence edge computing in 6G: Characteristics, challenges, potential use cases, and market drivers. Future Internet, 13 (5), 118.

3. Khayyat, M., Elgendy, I. A., Muthanna A. et al. Advanced deep learning-based computational offloading for multilevel vehicular edge-cloud computing networks // IEEE Access. 2020. Vol. 8. pp. 137052–137062.

4. Artem, V., Vadim, K., Elgendy, I. A., Muthanna, A., & Koucheryavy, A. DD-FoG: Intelligent Distributed Dynamic FoG Computing Framework // Future Internet. 2021. 14 (1). p. 13.

5. Khakimov, A., Elgendy, I. A., Muthanna, A., Mokrov, E., Samouylov, K., Maleh, Y., & Abd El-Latif, A. A. Flexible architecture for deployment of edge computing applications // Simulation Modelling Practice and Theory. 2022. 114, 102402.

6. Мутханна А. С., Тараскин Д. Н. Методы управления интеллектуальной распределенной архитектуры сети связи 2030 // СПбНТОРЭС: труды ежегодной НТК. 2021. № 1. С. 172–174.

7. Recommendation Q.5001. Signalling requirements and architecture of intelligent edge computing. 2018. 25 c.

8. Recommendation Y.3102. Framework of the IMT-2020 network. ITU-T, Geneva. May 2018.

9. Мутханна А. С. А., Тараскин Д. Н. Организация сервисов умного города на основе микро-сервисной архитектуры // Информационные технологии и телекоммуникации. 2021. Том 9. № 3. С. 48–55. DOI 10.31854/2307-1303-2021-9-3-48-55.

ИНФОКОММУНИКАЦИОННЫЕ СЕТИ И СИСТЕМЫ

UDC 004.42
SCSTI 50.41.25

DEVELOPMENT OF QR-CODE AUTHENTICATION SOFTWARE AS INTERNET-SERVICE

M. Gordeev, A. Urago, A. Shestakov

Bonch-Bruevich Saint-Petersburg State University of Telecommunications

Expansion of information technologies in our everyday life has been continuously increasing over the last decades as well as the necessity of more advanced cybersecurity measures. But according to various research, the human factor plays a drastic part in cybersecurity concerns. The article analyzes existing authentication methods and describes one of the possible solutions to this problem which is development of a software that will help to greatly simplify credential handling, provide its security on the user side, and encourage ones to use more complex and secure credential combinations. This software can be divided into three parts: mobile application (password manager), web application, and developer tool for third-party integration.

QR code, authentication, internet-service, cybersecurity, data protection, passwords.

Introduction

IT and Internet services came into everyday life almost two decades ago and despite the great benefits it gives, it came with new threats and challenges. The most important one is information security. 71 % of all cybercrimes are targeting confidential data [1]. Research conducted by Google has shown that 83 % of respondents use weak passwords which are easy to be guessed [2].

Solutions and concerns

To solve this issue companies and researchers create new methods to prevent data leaks like 2FA, biometrics or SSO systems that allow users to minimize the number of passwords they need to memorize, though only a few of all internet

resources utilize it [3], so from time-to-time users will still be required to use their regular login/password credentials to access a resource.

Another solution is to create software that will help users to manage their passwords thus encouraging them to use more secure combinations. Though, there are few scenarios remaining which refrain users from using secure passwords for their accounts. For example, when a user needs to access their account from a shared workstation (e. g., a computer in university lab). Here users won't be able to access their passwords on the target computer which will require them either to retype it from their smartphone, go through a complex process of acquiring their password on the target computer by accessing password manager via web browser, or use a weak password that is easy to memorize. Usually, users tend to choose the latter option.

Basic concept

So, since designing a new authentication standard which presumably won't become widespread and remain being one of the many, it is better to concentrate on improving the mechanics of password managers which have only one issue: absence of simple credential delivery mechanisms for shared workstations.

Assume that user have two devices: a target machine on which user needs to authenticate (TM) and their personal mobile device (PD) with a password manager application installed which contains the necessary keychain for access an abstract authentication service.

The easiest way to connect a pair of devices is to generate connection information (e. g., authentication code or PIN) and enter it into the other device. When connection is established, it is doubtful that it is secure enough to use for credentials transport, so it is preferred to use symmetric or asymmetric encryptions.

In case of asymmetric encryption, a public key can be transferred to PD via a regular TCP/IP connection. However, if a symmetric encryption is used, the Internet is not secure enough to do that. Instead, it is possible to use a visual method of transmission. A QR code can be a suitable solution for this purpose for many reasons: it cannot be read by humans; it can contain enough data; it excludes typo possibilities.

For simple understanding, assume that TM uses symmetric AES-128 encryption, and there is a proxy server which manages real-time connections between TM and PD. When user accesses TM, it establishes a real-time connection with the proxy server which returns a connection ID (Fig. , 1). Then TM generates a random encryption key and embeds these into QR code which is shown on the TM's output display (Fig. , 2). User scans the QR code with their PD, thus acquiring the necessary information for consequent data transmission (Fig. , 3). The PD encrypts required credentials with the acquired encryption key and sends the encrypted data to the proxy server with connection ID reference (Fig. , 4). The

proxy server sends encrypted data back to the TM (Fig. , 5) which decrypts it and sends it to the internet service server which requires user authentication (Fig. , 6).

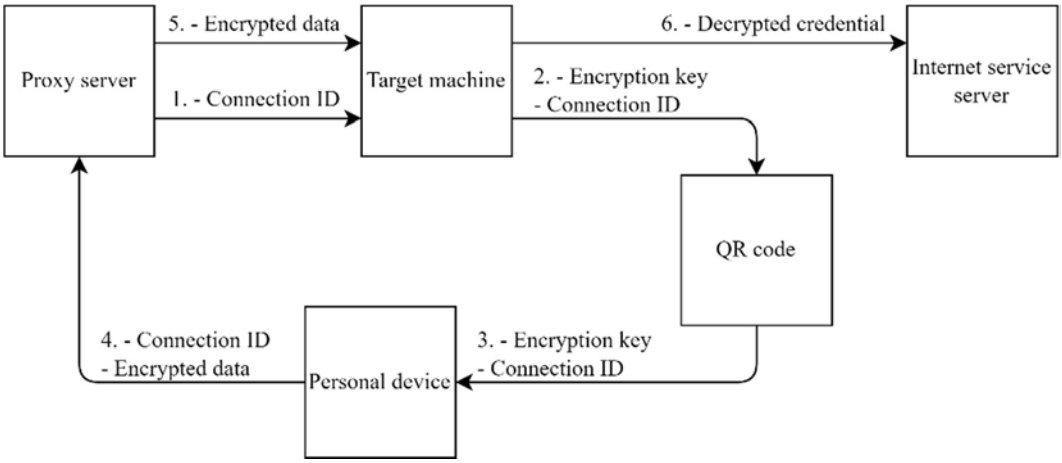


Fig. 1. Basic QR code authentication concept

Even though existence of the proxy server theoretically is not required, it significantly simplifies a process of development and maintaining such software with no significant reduction in security.

This system can be compromised in four different ways:

1. TM or PD are compromised.
2. Proxy server is compromised.
3. Connection between PD, proxy server and/or TM is compromised.
4. Connection between TM and internet service server is compromised.

Cases 1 and 4 will not be reviewed here since these are not related to the topic of the article and are a matter for another discussion.

Cases 2 and 3 can potentially lead to DoS attack which can result in service unavailability but will not result in data leaks since all data coming via the proxy server is encrypted and the encryption key is unknown to the server.

Software architecture

To make this concept work there are three components required to be developed: mobile application, web application, and optional plug-in software.

Mobile application will function as a password manager that stores and gives access to user's credentials, so it will require secure storage for credentials. Besides, this application should be capable of reading QR codes, parsing received data, encryption of data and its transmission via HTTP requests (Fig.).

Web application should consist of two separate parts: SPA which runs on client side (frontend) and API endpoints processing software that runs on the server (backend).

The backend should run on server indefinitely and be able to process incoming HTTP requests.

The frontend is loaded from the server via standard HTTP connection. SPA should be capable of generating random byte arrays, generating, and displaying a QR code, data decryption based on the same algorithms as mobile application and broadcast messages across the internet browser application it runs in. In addition, it should contain tools to establish RTC connection with the server and be able to exchange data with it.

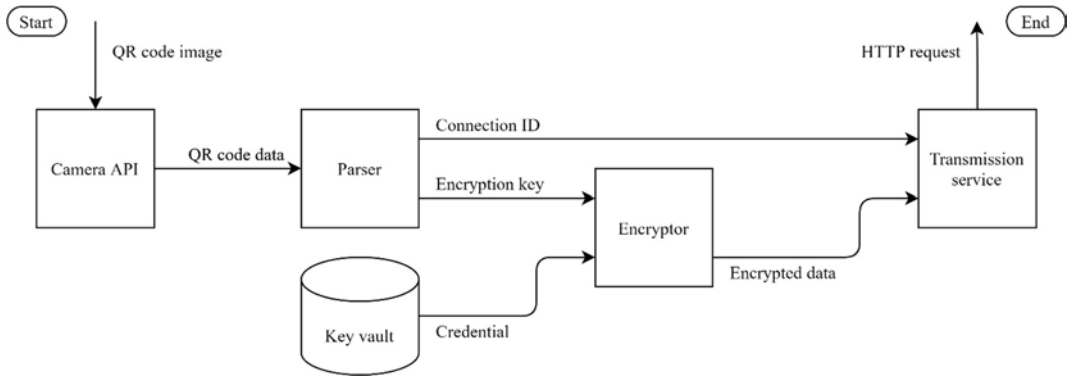


Fig. 2. Basic mobile application architecture

Fig. demonstrates all vital components of the web application and interaction between. First, SPA executables are downloaded via SPA endpoint to run it on TM (1). When SPA is downloaded and launched, an initialization phase commences. RTC client on SPA connects to RTC gateway on the backend (2). After a series of handshakes, the RTC gateway returns a connection ID to the client. RTC client and random number generator (RNG) pass connection ID and encryption key to QR code generator (3, 4) which generates a QR code image and displays it on TM's display monitor (6). After the QR code is scanned by mobile application (6) and encrypted data and connection ID are passed to the receiver endpoint (7), the backend triggers RTC gateway (8) which returns encrypted data to the client with matching connection ID (9). When data is received by the SPA it is passed to the decryptor (10) along with the encryption key generated by RNG on step 4 (11). When target data is acquired based on what primary goal is, decryptor passes data either to cross-origin broadcast API (12) which delivers credentials to the internet service which requested authentication (13) or displays it on TM's monitor for user to manually type it into target authentication system.

Plug-in software is a complimentary component of the system which is supposed to streamline credential delivery to authentication service. Due to security measures most internet browsers restrict access to data acquired from another source (Fig. 1, a). Though there is another way. Most browsers possess a cross-origin broadcast service which allows one resource to broadcast its data to any other resources, active in the current browser session and these resources can decide whether to accept incoming data or ignore it. Here is where the proxy software comes to use. It runs in the same container the authentication service does and listens to incoming messages from credential delivery system. And as soon

as credentials were received it passes these into authentication service with no need for user to involve (Fig. 1, b).

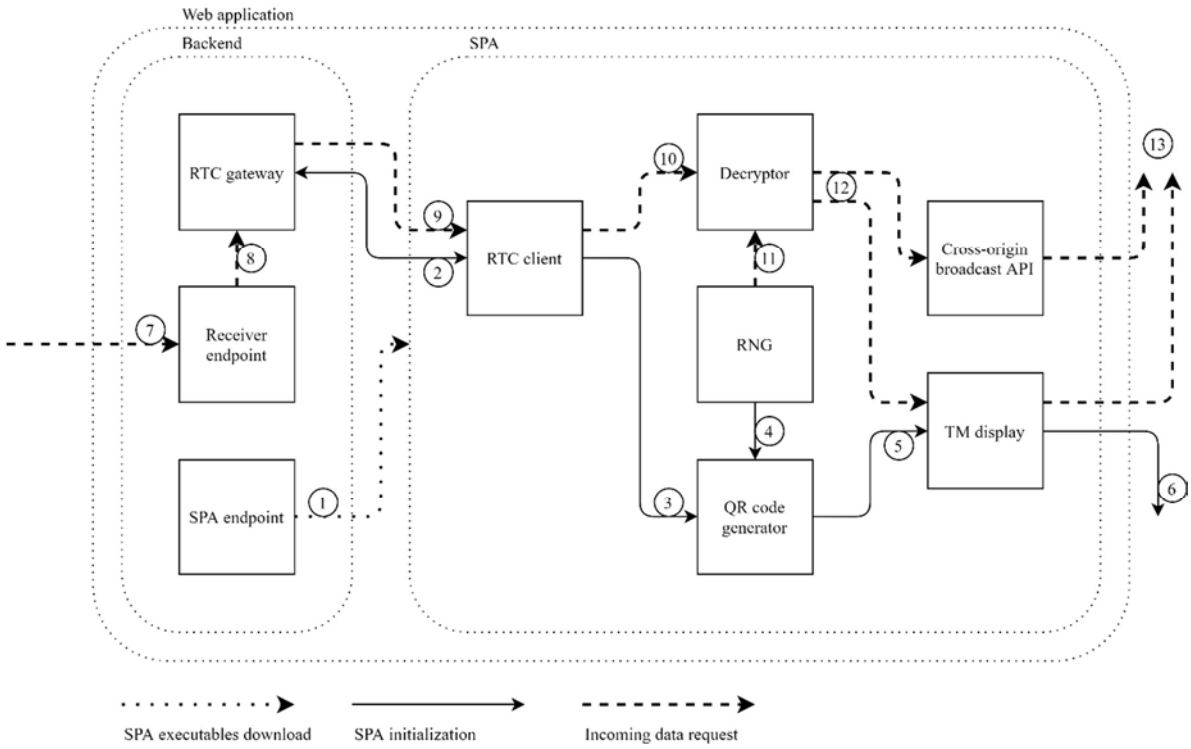


Fig. 3. Basic web application architecture

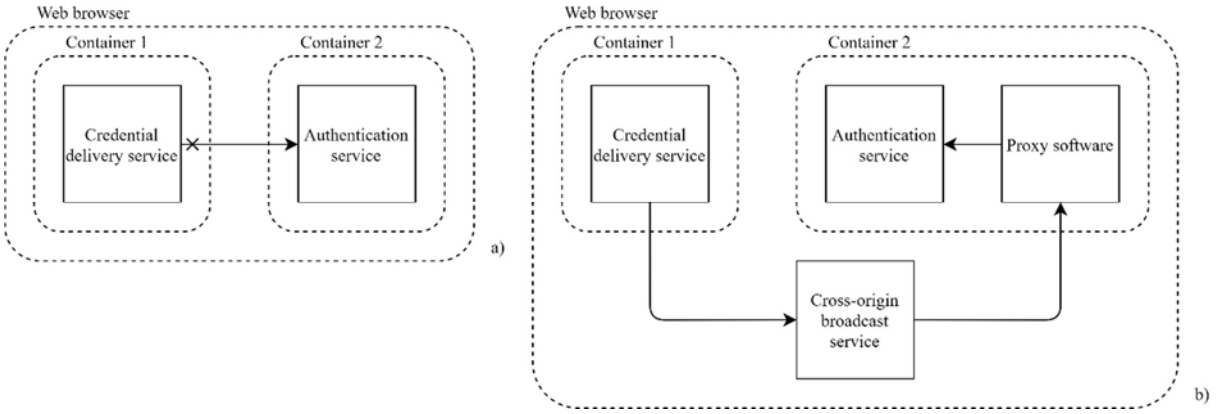


Fig. 1. Cross-origin data transmission in web browsers

Perspectives and conclusion

Since the plug-in is optional this concept can work on any internet service, even those that do not implement the plug-in software into their websites. In this case, the user must manually paste credentials into authentication form which is still faster than using regular password managers and much secure than using weak passwords. Besides, this architecture makes it possible to use globally without any global changes in existing authentication systems.

Aside from solving the problem, architecture of the solution number of possible applications is almost limitless. Authentication anywhere on any device can be simplified to scan a QR code by developing a right proxy plug-in: authentication on a workstation operating system, authentication on industrial control systems, credit card and addresses autofill, etc.

References

1. Ukwandu E. [et al.] Cyber-Security Challenges in Aviation Industry: A Review of Current and Future Trends [Journal]. [s. l.] : Information, 2022. 3 : Vol. 13.

2. Google, Harris The United States of P@ssw0rd$ [Online] // Google. Google, October 02, 2019. 1. – March 29, 2022. URL: https://storage.googleapis.com/gweb-uniblog-publish-prod/documents/PasswordCheckup-HarrisPoll-InfographicFINAL.pdf.

3. San-Tsai Sun Yazan Boshmaf, Kirstie Hawkey, Konstantin Beznosov A billion keys, but few locks: the crisis of web single sign-on [Conference] // In Proceedings of the 2010 New Security Paradigms Workshop. New York: Association for Computing Machinery, 2010.

Работа выполнена в рамках прикладных научных исследований СПбГУТ по государственному заданию Минцифры России в 2022 году.

UDCC 629.12
SCSTI 20.53.01

INTELLIGENT SYSTEMS FOR ANALYZING THE TECHNICAL RELIABILITY OF MOBILE DATA CENTERS

A. V. Mikhaylichenko, I. B. Parashchuk

Marshal Budyonny Military Signal Academy

The issues of automated analysis of technical reliability of modern mobile data centers are considered, a formal description of the composition of intelligent systems for analyzing their technical reliability is implemented. These intelligent systems contain elements designed to quantify the technical reliability of modern mobile data centers in an automated mode. They are designed to act as a decision support system in the interests of guaranteed durability and maintainability of data centers, which will increase the objectivity of management of such centers, as well as the accuracy and efficiency of solving the problem of analyzing the technical reliability of systems of this class.

intelligent system, analysis, technical reliability, mobile data center, fuzziness, durability, maintainability.

Mobile data centers (MDC) of various classes used in the interests of building a unified information space of the country are complex information and technical systems and require high costs for their creation, operation and maintenance of uninterrupted functioning [1–3].

This leads to the need for a quantitative analysis of the mobile data center's technical reliability indicators (TRI) in order to ensure their durability and maintainability in the process of achieving the tasks assigned to them, as well as in order to optimize the process of allocating various resources to maintain their smooth operation. At the same time, special attention at the present stage is paid to the financial resources spent on creating and ensuring reliable operation of the MDC.

The technical reliability of a MDC is understood as its condition in which it is able to continue its functioning regardless of the operability of its individual elements and nodes, and also has the means to restore functioning after failures or errors.

The authors of a number of works devoted to the problems of current and predictive control of technical reliability of complex targeted information technical systems, systems and communication networks traditionally consider several stages in the development of reliability theory, in the selection of criteria for its evaluation [4, 5, 6, 7]. In addition, the methodology of reliability analysis of complex technical systems, such as mobile data centers, was able to achieve a new qualitative level, relying on the extensive capabilities of modern computing systems, which made it possible to formulate and consider the problems and prospects of automated technical reliability analysis (ATRA).

The use of computing systems has dramatically reduced computing costs and made even such cumbersome (from the point of view of computing capacity) methods as dynamic and multi-criteria assessment of technical reliability – step-by-step analysis of an integral TRI that takes into account all or almost all the variety of aspects (facets) of MDC reliability available and popular among researchers.

Moreover, ATRA allows you to touch on mathematically complex and time-consuming methodological areas of reliability theory, which researchers of previous years could only dream of. We are talking about taking into account incomplete, fuzzy or contradictory parameters of durability and maintainability of the analyzed mobile data center when analyzing reliability (based on the theory of fuzzy sets, the theory of expert systems). And also about the use of a set of private methods of reliability analysis as an interactive "knowledge base" available to the user (based on the provisions of the theory of artificial intelligence).

Thanks to the development and improvement of hardware, software and methodological tools for assessing reliability, it became possible to develop a method and algorithms for automated analysis of the technical reliability

of a MDC with fuzzy set (observed) parameters. Specialists in the field of technical reliability of systems for various purposes are aware of the urgency of the task of developing a method and algorithms for vector evaluation of the technical reliability of the MDC, taking into account the objective qualitative and quantitative (linguistic) uncertainty of the source data, the fuzziness of the mobile data center's TRI caused by various types of impacts and other types of fuzziness [8].

The cases characteristic of the fuzzy description of the TRI of the MDC, in general, have been well studied, here are some of them:

mobile data centers operate in non-stationary modes, under the influence of destabilizing factors arising from natural disasters or meaningful activity of an antagonistic system;

limitations on the resources of modeling the process of changing the states of the TRI and the lack of statistical data on the parameters of the technical reliability of the MDC do not allow us to obtain clear information about the values of reliability characteristics and force us to use a fuzzy (linguistic) form of description;

a priori, there is uncertainty (fuzziness) of goals, i.e. when there are a number of alternative options for building a reliable MDC and a fuzzy evaluation of their TRI is performed in order to choose the best one. Here the task is already in its original form "immersed" in a fuzzy environment.

The purpose of solving this particular problem with the help of modern technological approaches is to increase the reliability and efficiency of the analysis of the technical reliability of the MDC for the case of stochastic estimation of their fuzzy variables (fuzzy values of the TRI of the MDC) and identification of the parameters of their membership functions determined by all types of impacts. It is obvious that solving the problems of analyzing the technical reliability of the MDC is the task of developers of systems of this class. Do not forget that the requirements for the efficiency and quality of management decisions to maintain the reliability, durability and maintainability of the MDC are traditionally high.

When solving these tasks, automation complexes and automated control systems come to the rescue. But even automation complexes and automated control systems solve the problems of analyzing the technical reliability of the MDC in the interests of optimal control of their durability and maintainability, assuming that the available initial data are unambiguous and reliable. In the case of unreliable, fuzzy, contradictory information, the creative capabilities of the developer or operator of the MDC come to the rescue.

In this case, the solutions developed with the help of automation complexes and automated control systems of the MDC are corrected by developers or operators, administrators-managers, relying on their experience and intuition. Their unformalized knowledge makes it possible to make optimal decisions within the framework of the analysis of the technical reliability of the MDC under conditions

of uncertainty (fuzziness) of various nature. That is why the creation and implementation of intellectual decision support tools in the activities of administrators, managers, developers and operators of the MDC is of particular relevance.

One of the promising ways to solve the ATRA problem in the interests of guaranteed durability and maintainability of the MDC and their elements is, in our opinion, the creation of intelligent systems for analyzing the technical reliability (ISATR) of the MDC. These are technical or software systems, the structure of which should include an interface (communication system), a logical inference system, an explanation system, a scheduler of ATRA program modules, a knowledge base (private methods of reliability analysis), a knowledge base management system of ISATR, a functional semantic network and a library of application programs for automated analysis of technical reliability. Intelligent systems of technical reliability analysis are capable, based on the use of artificial intelligence methods, in an automated mode, to solve the tasks of assessing the TRI of both stationary and mobile (container) data centers based on new information technologies and data processing and storage technologies – tasks traditionally considered creative, belonging to a specific subject area, knowledge of which is stored in the system memory [9].

The solution of this scientific problem is aimed at eliminating the contradiction between the requirements for ensuring the durability and maintainability of the MDC and their elements and the capabilities of existing generalized methods for analyzing the reliability of both the MDC itself and a large number of subsystems included in them.

At the same time, an effective analysis of the reliability of the MDC is carried out on the basis of the introduction of a qualitatively new decision support system, in which the ISATR plays a central role. This makes it possible to reduce the cost of financial, time and management resources in the process of designing, developing and operating the MDC, as well as to increase the degree of validity of decisions made to manage the structure, parameters and modes of their operation.

The purpose of this scientific development is achieved by setting and solving a number of theoretical and practical problems: generalization of experience in the development and application of modern and promising methods of multi-criteria ATRA systems of information exchange and data processing; analysis of modern methods for assessing the technical reliability of a MDC based on mathematical modeling of processes occurring in systems of this class; creation of the theoretical foundations of the ATRA of MDC in various conditions of a priori uncertainty using an artificial intelligence system; development of a methodology for building intelligent ATRA of MDC systems; synthesis of algorithms for the functioning of ISATR of MDC at various stages of their life cycle.

One of the possible approaches to solving particular ATRA problems, when using a decision support system in the form of an ISATR, can be based on artificial neural network technology. This technology can be used to solve a particular

problem – the formulation of a system of indicators of technical reliability of the MDC.

Modern approaches to solving this problem are mathematically correct, however, they do not take into account the subjective factor introduced by the user when classifying particular indicators of technical reliability of the MDC, they do not take into account the uncertainty when including individual components (particular reliability indicators) in the global system of reliability indicators of the MDC. As part of the proposed new decision support system – ISATR, an approach is considered that allows predicting the composition of the system of indicators of the reliability of the MDC based on available a priori data, an approach using the so-called extrapolating neural networks, which are a kind of well-known models of associative memory [10].

This approach expands the capabilities of existing artificial neural networks used in the interests of decision support to ensure the durability and maintainability of the MDC, allowing you to make informed decisions on the composition of the vector of reliability indicators to be analyzed.

An artificial neural network of this type traditionally consists of two layers of neurons – an input and an output layer. Unlike the synaptic map used in a conventional artificial neural network, an extrapolating neural network uses a so-called cognitive map, completely defined by a matrix of connections. A cognitive map is understood as an oriented graph, the nodes of which represent some objects or concepts (in our case, these are indicators of the technical reliability of the MDC), and arcs are connections between them that characterize causal relationships (causal correlations between various indicators of the technical reliability of the MDC). As a rule, an expert or a group of experts is involved in drawing up such maps.

The developed cognitive maps characterize the cause-and-effect relationships between some indicators of the technical reliability of the MDC, allow us to naturally combine the knowledge of several experts in reliability control issues for a more adequate description of the process of ensuring the durability and maintainability of the MDC.

Filling in the matrix of connections between the indicators of technical reliability of the MDC and the input vector of preferences is the starting point in the work of the neural network. As a result, the output layer of the neural network forms a vector of essential aspects of the reliability of the MDC to be analyzed, its system of indicators of technical reliability.

Thus, the use of the proposed decision support system in the interests of guaranteed durability and maintainability of the MDC will significantly increase the objectivity of the decisions made and the efficiency of solving the problem of analyzing the technical reliability of systems of this class.

References

1. Kusakin D. G. Building a Data Center: designing a Data Center // Data Centers of the Russian Federation. Design, construction, operation. 2015, No. 9. pp. 53–59. [in Russian].
2. Lisiecki Yu. M. The Building of a geographically-distributed data centre // Software products and systems. 2008. No. 2. pp. 14–16. [in Russian].
3. Parashchuk I. B., Mikhaylichenko N. V. Features of the design and analysis of quality data centers as the basic elements of IT infrastructure // Perspective directions of development of national information technologies: Materials of the IV Interregional scientific and practical conference (PDDNIT-2018). Sevastopol: SevGU, 2018. pp. 28–29. [in Russian].
4. Andreev A. V., Yakovlev V. V., Korotkaya T. Yu. Theoretical foundations of reliability of technical systems. Study guide. St. Petersburg: Publishing House of the Polytechnic University, 2018. 164 p. [in Russian].
5. Gromov Yu. Yu., Ivanova O. G., Mosyagina N. G., Nabatov K. A. Reliability of information systems. Tambov : Publishing house of GOU VPO TSTU, 2010. 160 p. [in Russian].
6. Kryukova E. S., Tkachenko V. V., Mikhaylichenko A. V., Parashchuk I. B. Issues of reliability assessment of modern data storage systems for mobile data centers // High-tech technologies in Earth space research. 2021. Vol. 13. No. 5. pp. 86–95. [in Russian].
7. Gurov S. V., Utkin L. V. Reliability of systems with incomplete information. St. Petersburg : Lyubavich, 1999. 160 p. [in Russian].
8. Parashchuk I. B., Bobrik I. P. Fuzzy sets in problems of communication network analysis. St. Petersburg : VUS, 2001. 80 p. [in Russian].
9. Sovetov B. Ya., Tsekhanovsky V. V., Chertovskoy V. D. Intelligent systems and technologies. M.: Publishing center "Academy", 2013. 320 p. [in Russian].
10. Parashchuk I. B., Ivanov Yu. N., Romanenko P. G. Neural network methods in modeling and analyzing the effectiveness of communication networks. St. Petersburg: VUS, 2010. 104 p. [in Russian].

УДК 004.051
ГРНТИ 50.41.23

БАЛАНСИРОВКА НАГРУЗКИ В СЕТИ

М. Ф. Аббасов, А. В. Дагаев

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье произведен краткий обзор по основным принципам балансировки глобальных и локальных сетей. Предложены этапы решения задачи балансировки нагрузки. Рассматриваются уровни балансировки, а также её основные алгоритмы: DNS, Round Robin, Weighted Round Robin, Random, IP Hash, которые могут быть реализованы в зависимости от специфики конкретного проекта для достижения дальнейшей цели.

Load Balancing, балансировка нагрузки, сетевая модель OSI, DNS, Round Robin, Weighted Round Robin, Random, IP Hash, равновероятная балансировка.

Введение

В настоящее время получили большое развитие технологии виртуализации серверов в связи с потребностями в рациональном распределении аппаратных ресурсов. Однако, одновременно с этим повышается сложность администрирования таких систем – в частности, в отношении распределения нагрузки между серверами: на каждый сервер можно назначить некое конечное число нагрузок, и каждая нагрузка имеет требования по мощности, которые могут часто меняться. Отсюда происходит проблема балансировки нагрузки.

Балансировка нагрузки (*Load Balancing*, LB) распределяет высокий сетевой трафик между несколькими серверами, позволяя организациям масштабироваться для удовлетворения рабочих нагрузок с высоким трафиком [1]. Балансировка направляет запросы клиентов на доступные серверы, чтобы равномерно распределять рабочую нагрузку и улучшать скорость отклика приложений, тем самым повышая доступность веб-сайта или сервера.

Балансировка нагрузки может осуществляться при помощи как аппаратных, так и программных инструментов, а также на различных уровнях сетевой модели OSI (*Open Systems Interconnection Basic Reference Model* – базовая эталонная модель взаимодействия открытых систем).

Процедура балансировки осуществляется при целом комплексе алгоритмов и методов, соответствующим следующим уровням модели OSI:

– сетевому;
– транспортному;
– прикладному.

На рис. 1 представлен пример работы балансировки нагрузки.

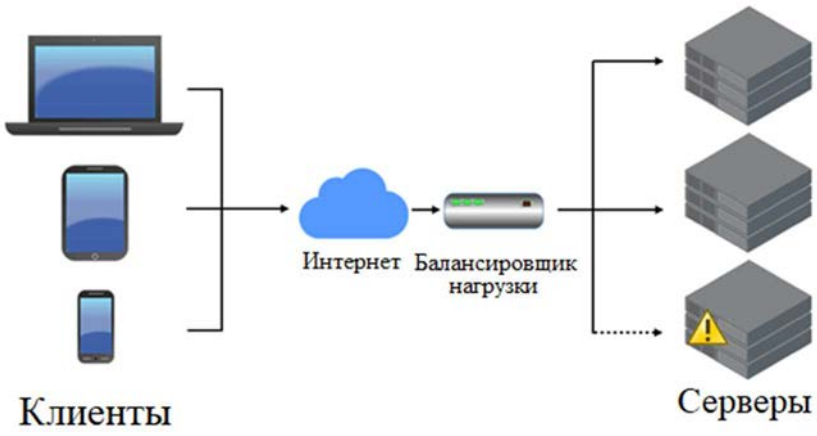


Рис. 1. Пример работы балансировки нагрузки

Этапы решения задачи балансировки нагрузки

Обычно практичное и полное решение задачи балансировки нагрузки состоит из четырех шагов:

– оценка нагрузки вычислительных узлов;
– инициация балансировки нагрузки;
– принятие решения о балансировке;
– перемещение объектов.

Уровни балансировки

Стоит рассмотреть по отдельности уровни балансировки нагрузки в сети.

Сетевой уровень

Этот метод предполагает использование набора физических серверов. Достаточно дорогой, но очень эффективный метод, который надежно защищает вебмастера от превышения нагрузки на сервер. Суть его сводится к тому, что несколько разных машин отвечают за работу одного IP-адреса.

Транспортный уровень

Этот тип методов отличается простотой и эффективностью. Транспортное снижение нагрузки на сервер предполагает использование балансировщика, который распределяет запросы по пулу в соответствии с заданными алгоритмами. Балансировщик передает выбранному серверу запросы, а затем получает на них ответ и перенаправляет его обратно пользователю.

Прикладной уровень

Прикладная балансировка похожа на транспортную – здесь тоже используется прокси, и запросы пользователей передаются на серверы. Но, в отличие от транспортной балансировки, прикладная распределяет нагрузку с учетом запрашиваемых страниц, контента или действий. Например, запись на сайт (создание учетных записей и подобные действия) будут проводиться через один сервер, а чтение – через другой.

Методы балансировки

Выделяют два метода балансировки: локальная и глобальная. Рассмотрим каждый из них подробнее и дадим краткую характеристику.

Методы локальной балансировки

Различают следующие методы локальной балансировки:

– на канальном уровне, как с использованием отдельного балансировщика, так и без него;
– на сетевом уровне;
– на транспортном уровне.

Методы глобальной балансировки

Из методов глобальной балансировки можно выделить следующие наиболее распространенные методы:

– балансировка на уровне DNS;

– балансировка на прикладном уровне – проксирование и redirect запросы;

– балансировка на сетевом уровне – алгоритм Anycast.

Алгоритмы балансировки

Существует много различных алгоритмов и методов балансировки нагрузки [2]. Выбирая конкретный алгоритм, нужно исходить, во-первых, из специфики конкретного проекта, а во-вторых, из целей, которые планируется достичь.

Все современные балансировщики имеют поддержку множества алгоритмов, которые позволяют оптимально распределить запросы. Самих алгоритмов есть огромное множество, но основных всего несколько:

– DNS;
– Round Robin;
– Weighted Round Robin;
– Random;
– IP Hash;
– Равновероятная балансировка.

Использование DNS – это лёгкий способ распределить запросы. Он позволяет работать клиентам с несколькими серверами и повысить их доступность. Достаточно зарегистрировать несколько серверов на одно доменное имя. Когда клиент запрашивает IP адрес, DNS возвращает список адресов серверов, который каждый раз начинается с другого адреса.

Алгоритм Round Robin считается самым простым. Связано это с тем, что балансировщик держит обычную очередь из серверов и не зависит от времени. Первый сервер в очереди обрабатывает запрос и помещается в конец очереди и так по кругу [3]. Таким образом сервера равномерно нагружены.

Алгоритм Weighted Round Robin тот же Round Robin, но с дополнительным свойством – вес сервера. Мы можем указать балансировщику сколько трафика отправлять на тот или иной сервер. Сервера помощнее будут иметь больший вес и соответственно обрабатывать больше запросов чем другие сервера.

Random является одним из простейших алгоритмов балансировки. Имеется пул серверов, балансировщик генерирует случайное число, которые соответствует номеру сервера в пуле и отправляет на него заявку.

Алгоритм Hash использует в своей основе механизм хеширования. Он позволяет распределить запросы на основе хеша, для которого обычно используется IP-адрес или URL. Такой алгоритм используют, когда сервер хранит какие-то локальные данные, которые нужны для ответа.

Под равновероятной балансировкой понимается, что распределение модулем балансировки нагрузки поступающих задач производится на основании вероятности передачи задачи на обработку на один из узлов кластера.

Сравнение алгоритмов балансировки

Моделирование выполнялось на основе равномерного распределения внешних запросов на логический сервер в симметричной структуре. Для каждого алгоритма был реализован код на языке Java с использованием имитации списка IP. Принцип алгоритма Round Robin заключается в том, что каждый запрос пользователя присваивается внутреннему серверу по очереди, от 1 до N (количество серверов), а затем перезапускается цикл. Преимущество алгоритма заключается в его простоте: ему не нужно записывать состояние всех текущих подключений. Реализация алгоритма Random заключается в случайном выборе сервера. Идея алгоритма Hash состоит в том, чтобы получить значение, вычисленное хеш-функцией в соответствии с IP-адресом клиента. Когда клиент с одним и тем же IP-адресом имеет одинаковый список внутренних серверов, он будет сопоставлен с аналогичным внутренним сервером. Работа алгоритма Weighted Round Robin схожа с Round Robin, единственное отличие заключается в процедуре присвоения веса серверам. Далее по порядку производятся запросы. Чем больше вес, тем больше запросов получает сервер при каждом круге. Алгоритм Weight Random также присваивает веса серверам в соответствии с конфигурацией серверной части. Разница заключается в том, что он произвольно запрашивает сервер в соответствии с весом, а не порядком.

Для сравнения алгоритмов был выбран пул серверов, состоящий из 10, 40, 80 и 160 машин. В балансировщике используется один из 5-ти алгоритмов (*Hash, Random, Round Robin, Weight Random, Weighted Round Robin*). Сначала заявка отправляется в балансировщик, затем, в зависимости от алгоритма, выбирается сервер, который будет обрабатывать эту заявку.

Для моделирования работы пула серверов используются следующие входные данные: размер пула серверов (10, 40, 80, 160), число заявок (1000) и количество итераций (10000). Результат сравнения алгоритмов представлен на рис. 2.

На графике видно, что алгоритмы, которые учитывают вес, работают значительно медленнее алгоритмов, которые вес не учитывают. Алгоритмы, которые не учитывают вес, показывают примерно одинаковый результат. Однако алгоритм Round Robin показал себя лучше остальных.

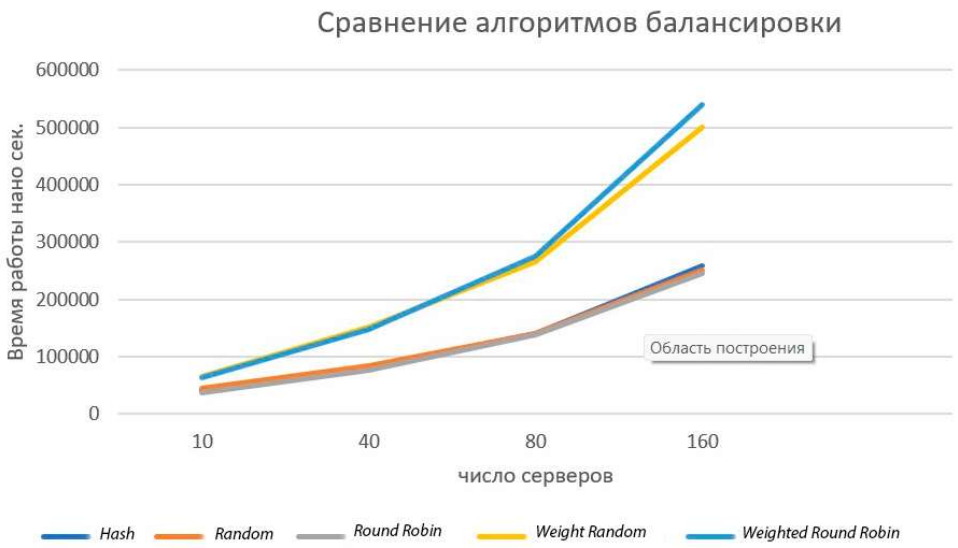


Рис. 2. Результат сравнения алгоритмов балансировки

Таким образом, на основании вышеизложенного можно сделать вывод, что Round Robin является самым простым способом снижения нагрузки на сервер. Запросы направляются поочередно на сервера. Следующий запрос снова вернется к первому серверу, и цикл начнется заново. Плюсы подхода очевидны: простота, низкая стоимость и эффективность. При этом серверы из пула могут не быть связаны между собой – через DNS и этот алгоритм можно перенаправлять запросы на любые машины [4].

Моделирование выполнялось трижды и все результаты приблизительно идентичные. Следует указать, что использование быстрого алгоритма не приведёт к ожидаемым результатам, если для его работы понадобится больше памяти, чем есть у компьютера.

Заключение

В данной работе были проанализированы общие постановки задачи балансировки, рассмотрены виды и уровни балансировки, а также существующие основные алгоритмы и методы. Данная сфера еще молодая и у нее есть большой потенциал в развитии. Индустрия активно движется в сторону типовых OSS-аппаратных и программных решений. По мере роста динамичности распределённых систем в равной степени будут усложняться и лежащие в их основе сети, и балансировочные системы.

Список используемых источников

1. Зубов С. Сравнительный анализ методов балансировки трафика. URL: https://habr.com/ru/company/oleg-bunin/blog/319262/ (дата обращения: 25.01.2022).

2. Балансировка нагрузки: основные алгоритмы и методы. Статья в блоге компании Селектел. URL: https://selectel.ru/blog/balansirovka-nagruzki-osnovnye-algoritmy-i-metody/ (дата обращения: 25.01.2022).

3. Айвалиотис Д. Администрирование сервера NGINX. М. : ДМК Пресс, 2018. 288 с.: ил. ISBN 978-5-97060-610-0.

4. Oracle Cloud Infrastructure Documentation. URL: https://docs.oracle.com/en-us/iaas/Content/Balance/Concepts/balanceoverview.htm (дата обращения: 25.01.2022).

УДК 004.056.53
ГРНТИ 81.93.29

ОБЗОР СРЕДСТВ МОНИТОРИНГА ЛОКАЛЬНЫХ СОБЫТИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Г. Т. Абраменко[1,2], Л. А. Виткова[2], М. В. Мельник[1,2]

[1]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

[2]Санкт-Петербургский Федеральный исследовательский центр Российской академии наук

Сегодня как никогда ключевое значение занимает информация, которая обрабатывается, хранится и передается между различными информационными системами. Для государства и бизнеса критически важно непрерывное и корректное выполнение всех процессов, и обеспечение конфиденциальности, целостности и доступности. В статье рассматриваются функциональные характеристики СУИБ и сравниваются SIEM системы от иностранного и отечественного производителя.

анализ локальных инцидентов, мониторинг информационной безопасности, SIEM, СУИБ.

Введение

В современном мире, ключевое значение занимает информация, которая обрабатывается, хранится и передается между различными информационными системами. Для государства и бизнеса критически важно непрерывное и корректное выполнение всех процессов, и обеспечение конфиденциальности, целостности и доступности [1, 2].

С ростом объемов передаваемой информации, увеличивается и количество инцидентов информационной безопасности. Как правило, встроенные механизмы защиты информационных систем не могут в полной мере гарантировать защиту информации. Для борьбы с различными возможными инцидентами информационной безопасности, необходимо иметь собирать и обрабатывать данные различных источников. Источниками событий могут служить журналы операционной системы, системы мониторинга сети и любые другие источники расположены в инфраструктуре организации.

Функциональные требования к СУИБ

В процессе анализа существующих систем мониторинга инцидентов информационной безопасности авторы учитывали количество источников событий, которые могут приниматься и обрабатываться конкретной системой в режиме реального времени. Возможен ли анализ событий, является ли система удобной для пользования ею (консольное управление, создание собственных правил по обнаружению событий информационной безопасности, возможность выбора источников событий). А также имеет ли система возможность визуализировать данные и предоставить отчёт [3].

Функциональные характеристики СУИБ были разделены на следующие модули:

1. Модуль сбора и агрегации данных.

Осуществляет сбор данных из различных источников (различные сервисы, сетевые устройства, систем безопасности, журналы логов, различные приложения и т.д. Позволяет производить мониторинг производительности и доступности узлов, фильтровать полученные данные.

2. Модуль анализа данных.

Анализ данных осуществляется по правилам определяемых экспертами. Учитываются заданные параметры, условия, которые могут включать в себя набор параметров: типы событий, временные условия, типы источников событий, последовательность и частота событий и другие.

3. Модуль оповещения.

Выявленные инциденты информационной безопасности могут в автоматизированном режиме выводиться в различные каналы оповещения: на экран монитора, в файл, по электронной почте и т. д.

4. Модуль визуализации.

Полученные результаты могут быть графически представлены в виде диаграммы, графиков, таблиц.

5. Модуль хранения.

Полученные данные могут долговременно хранится в хранилищах и приведены к единому стандартному виду, в дальнейшем могут использоваться для расследования инцидентов.

Сравнительный анализ

В ходе исследования были рассмотрены следующие системы:

1. QRadar Security Intelligence Platform (*QRadar*).

Данная платформа позволяет фиксировать события информационной безопасности, выявляет аномальную активность. Поддерживает функционал реагирования на инциденты информационной безопасности. Имеет встроенные журналы и поддерживает возможность работы с большим объемом данных. В QRadar есть функции обеспечения безопасности вирту-

ализованных инфраструктур, расширенный и улучшенный визуальный контроль, анализ защищенности и расследование инцидентов. Отличительными преимуществами данной платформы является то, что платформа выполняет полный цикл по обнаружению и реагированию на инциденты информационной безопасности, начиная от сбора и анализа событий ИБ, выявления аномальной сетевой активности, сканирования уязвимостей и выявления небезопасных конфигураций, заканчивая интеграцией с искусственным интеллектом.

2. ФГУП «НПП «Гамма» – Платформа Visor [4].

Данная платформа позволяет вести сбор событий информационной безопасности, собирать данные о конфигурации защищаемых узлов, обрабатывать и хранить собранные события информационной безопасности, выявляет и сообщает об инцидентах информационной безопасности. Плюсом данной системы является то, что система отслеживает доступность узлов и проводит их инвентаризацию как на аппаратном уровне, так и на уровне программного обеспечения. Собранные данные сохраняются в базу Visor. В Visor существует возможность отправки инцидентов в ГосСОПКА.

3. Positive Technologies Max Patrol SIEM [5].

Согласно заявлениям производителя, целью данного решения является: построение системы, гарантирующую возможность обеспечить проведения следующих мероприятий (1) Управление активами; (2) Управление уязвимостями. Продукт поддерживает сбор событий информационной безопасности от разных внешних источников, их около. Все данные нормализуются и приводятся к общему стандарту, что способствует их дальнейшей обработке. Все повторяющиеся события либо объединяются, либо удаляются, что в свою очередь экономит пространство. Также производится анализ взаимосвязи между событиями по заданным критериям и правилам, в случае срабатывания правила создается инцидент информационной безопасности и сохраняется в архив. Архивы могут быть представлены в виде срезов состояний наблюдаемых систем, что способствует проведения глубокого анализа и расследования инцидентов.

Комплект поставки содержит рекомендации по реагированию на инциденты и руководства по обнаружению атак, которые описывают настройку как различных источников в инфраструктуре предприятия, так и самой системы. В продукте присутствует инструмент разработки, который позволяет создавать свои собственные формулы нормализации и свои правила.

Заключение

В отличии от QRadar отечественные системы Платформа Visor и Max Patrol SIEM имеют действующие сертификаты ФСЬЭК России и могут быть внедрены на госпредприятиях, а также на объектах критически-важной инфраструктуры. Например, известно, что Max Patrol SIEM используется ГК

Росатом. QRadar SIEM является одним из лидеров в мире, но по функционалу выбранные отечественные СУИБ не уступают продукту от компании IBM.

Работа выполнена при частичной финансовой поддержке FFSU-2019-0002-Бюджетная тема в СПб ФИЦ РАН.

Список используемых источников

1. Булатов Н. А., Виткова Л. А., Шашкин В. С. Теоретические аспекты управления информационной безопасности на предприятии // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VI Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4-х т. Санкт-Петербург, 2017. Т. 2. С. 117–122.

2. Виткова Л. А., Дудникова М. Н., Петрова А. Н. Вопросы управления информационной безопасностью // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VII Международная научно-техническая и научно-методическая конференция : сб. научн. ст. в 4-х т. Санкт-Петербург, 2018. Т. 2. С. 143–146.

3. Аникевич Е. А., Виткова Л. А., Сацук Е. Н., Сергеева И. Ю. Предотвращение утечек конфиденциальной информации в информационных системах // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VI Международнаая научно-техническая и научно-методическая конференция : сб. научн. ст. в 4-х т. Санкт-Петербург, 2017. Т. 2. С. 46–51.

4. SIEM-система Visor // Сайт ФГУП «НПП «Гамма». URL: https://nppgamma.ru/catalog/produktsiya_proizvodstva_fgup_npp_gamma/siem_sistema_visor/ (дата обращения: 29.03.2022).

5. MaxPatrol Security Information and Event Management. URL: https://www.ptsecurity.com/ru-ru/products/mpsiem/ (дата обращения: 29.03.2022).

УДК 004
ГРНТИ 20.53

АНАЛИЗ ОСОБЕННОСТЕЙ СУБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ РОССИЙСКОЙ ФЕДЕРАЦИИ, ФУНКЦИОНИРУЮЩИХ В СФЕРЕ НАУКИ

Г. Т. Абраменко, Н. Н. Лансере, И. И. Фадеев

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье рассматриваются типовые объекты критической информационной инфраструктуры Российской Федерации субъектов КИИ, функционирующих в сфере науки, определена специфика критических процессов для данной сферы, проведен анализ

типовых объектов КИИ, оцениваются уязвимости для применяемых программных и программно-аппаратных средств.

критическая информационная инфраструктура, КИИ, уязвимости, актуальные угрозы, импортозамещение, сфера науки.

Сфера науки в которой функционируют субъекты критической информационной инфраструктуры Российской Федерации (КИИ) является достаточно многогранной и перекликается с другими сферами, определенными Федеральным законом № 187-ФЗ от 26 июня 2017 г. «О безопасности критической информационной инфраструктуры» (187-ФЗ) [1]. КИИ – это информационные системы (ИС), информационно-телекоммуникационные сети (ИТКС), автоматизированные системы управления (АСУ) субъектов критической информационной инфраструктуры (государственные органы, государственные учреждения, российские юридические лица и (или) индивидуальные предприниматели) функционирующие в 12 сферах, представленных на рис.

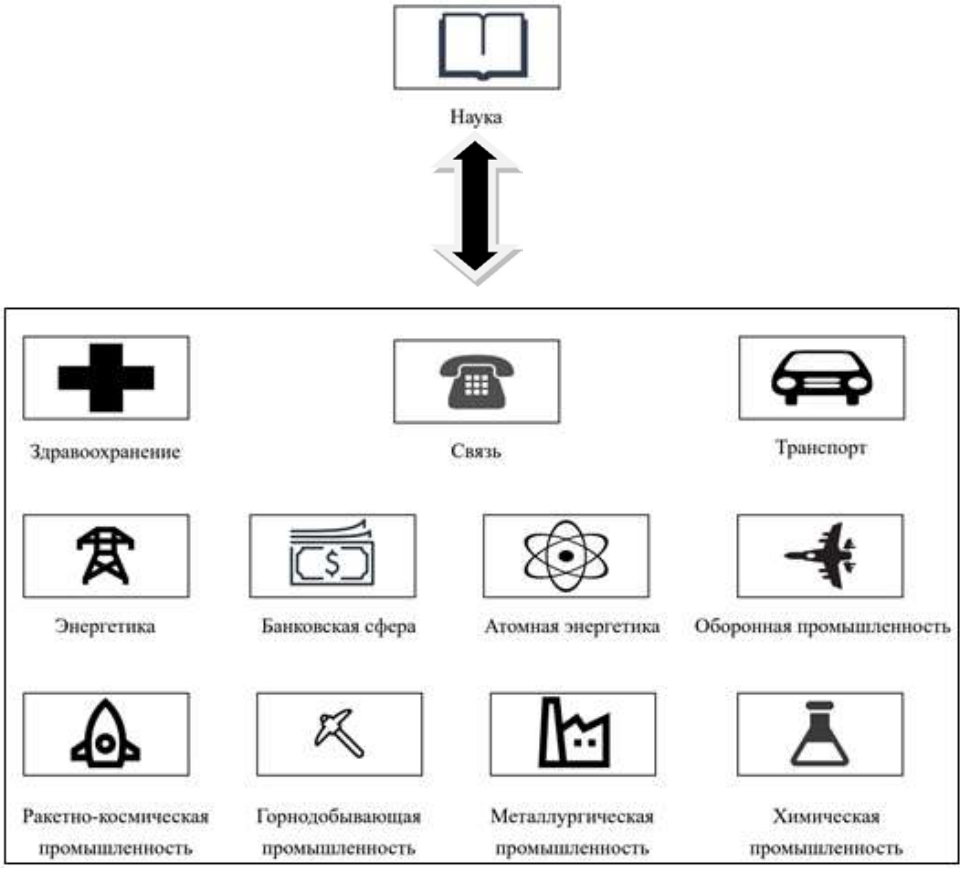


Рисунок. Сферы деятельности КИИ

В ходе анализа 12 сфер и областей, на которые распространяется действие 187-ФЗ, определено, что выявление критических процессов таких

субъектов КИИ осложняется особенностями функционирования отдельных организаций. Реальные действующие субъекты КИИ в сфере науки перекликаются с остальными 11 сферами и областями и, более того, постоянно совершенствуют свои объекты в рамках проектов по цифровой трансформации. Сложно представить современную науку без новейших средств или систем вычислительной техники, но данный фактор осложняет выявление отдельных управленческих, технологических, производственных, финансово-экономических и (или) иных процессов в рамках выполнения функций (полномочий) или осуществления научно-исследовательской деятельности. В рамках данной статьи предлагается рассмотреть информационные системы, автоматизированные системы управления и информационно-телекоммуникационные сети, реализующие выполнение научно-исследовательские и опытно-конструкторские работы (НИКОР).

Особенности функционирования субъектов КИИ в сфере науки приводят к сложностям в оценке возможных негативных последствий и ущерба в соответствии с показателями критериев значимости [2].

Дополнительно субъектами могут быть рассмотрены внутренние финансовые риски, связанные с:

выполнением, разработкой и хранением НИОКР;

закупкой оборудования и его установки;

получением и реализацией крупных грантов;

выплатой зарплат и премий научным сотрудникам.

При этом необходимо учитывать стоимость защиты объектов информатизации, контроль обрабатываемой информации и других мер по информационной безопасности (ИБ) и ее защиты.

Обрабатываемые научные достижения, при должном подходе, потенциально могут нанести вред гражданам или государству в целом. Основными сведениями, подлежащими защите в рамках выполнения НИОКР могут являться:

сведения о ходе выполнения и результатах НИОКР;

коммерческая тайна субъекта КИИ по возможностям выполнения НИОКР и затратам на них.

Типовыми объектами КИИ, подлежащими защите в рамках выполнения НИОКР для субъектов КИИ могут являться:

локальные вычислительные сети (ЛВС);

лабораторное оборудование;

ИС для хранения конструкторской документации;

испытательные среды;

ИС для разработки и моделирования проектной документации;

ИС управления ресурсами, позволяющие осуществлять планирование, учет, контроль и анализ ресурсов;

информационные (автоматизированные) системы управления производственными ресурсами в ходе технологического процесса (АСУ ТП);

информационные (автоматизированные) системы управления станками с числовым программным управлением (ЧПУ).

Дополнительной особенностью данных объектов КИИ является их наличие не только в научно-исследовательских институтах, центрах или лабораториях, но и в высших учебных заведения нашей страны, реализующих НИОКР.

В результате анализа зарубежных открытых источников установлено, что для реализации критических процессов в сфере науки, часто используются следующие системы и программное обеспечение (ПО), представленные в таблице 1.

ТАБЛИЦА 1. Используемое оборудование и ПО в субъектах КИИ

№ п/п	Системы реализации критических процессов	Оборудование и ПО
1	ЛВС	Маршрутизаторы, коммутаторы, сетевые экраны (Cisco, Huawei, Astra Networks, HP Enterprise, Juniper Networks [3])
2	Лабораторное оборудование	На базе ОС Windows, UNIX-подобные, собственные
3	ИС для хранения конструкторской документации	Oracle, MySQL, MS SQL Server, PostgreSQL, Mongo DB, IBM lotus Notes, MS Access [4]
4	Испытательные среды	Собственные, либо на базе лабораторного оборудования
5	ИС для разработки и моделирования проектной документации	AutoCAD, Wings, Компас 3D
6	ИС управления ресурсами, позволяющие осуществлять планирование, учет, контроль и анализ ресурсов	1С, SAP, Microsoft Dynamics AX (Axapta), Oracle ERP, Парус, Галактика
7	АСУ ТП, ЧПУ	Не рассматривается

В рамках проведения анализа связи уязвимостей с угрозами безопасности информации (УБИ) оценены актуальные УБИ.

Согласно приложению 9 Методики оценки угроз безопасности [5] определены базовые (минимально) актуальные нарушители, ими являются «нарушитель со средним и низким потенциалом», которые представлены в таблице 2.

Оценка УБИ, связанных с уязвимостями и базовых актуальных нарушителей позволяет определить минимальный перечень УБИ в соответствии с банком данных угроз безопасности информации ФСТЭК России [6] и при минимальных рисках, основанных на исходных данных, количество угроз оценивается в количестве более 80.

ТАБЛИЦА 2. Модель нарушителя для КИИ в сфере науки применимая к ВУЗам

	Внутренний нарушитель	Внешний нарушитель
С низким потенциалом	Авторизованные пользователи систем и сетей (сотрудники, преподаватели и студенты)	Системные администраторы и администраторы безопасности
Со средним потенциалом	Отдельные физические лица (хакеры)	Разработчики программных, программно-аппаратных средств, Преступные группы (криминальные структуры)

В результате анализа были определены актуальные угрозы ИБ для объектов КИИ в сфере науки, использующие популярное западное оборудование [3]. Такой вариант реализуется, но в нынешних реалиях недальновиден:

использование иностранного несертифицированного оборудования, влечет за собой определенные последствия, касательно скрытых закладок в ПО, микросхемах и другие потенциальные проблемы;

никто не учитывает сторонние факторы, которые могут привести к проблемам с использованием иностранных платформ и оборудования в случае их блокировки [7];

не исключены целевые компьютерные атаки объектов КИИ со стороны недружественных стран на оборудование, поставляемое в рамках международных договоров [8].

Подтверждается необходимость разработки отечественных продуктов, для сферы науки и остальных взаимосвязанных с ней сфер, учитывая рекомендации регуляторов.

Список используемых источников

1. Федеральный закон № 187-ФЗ от 26 июня 2017 г. «О безопасности критической информационной инфраструктуры».

2. Постановление Правительства Российской Федерации от 8 февраля 2018 г. № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры».

3. Трепалина Ю. Рост рынка сетевого оборудования в I квартале 2021 года предвещает дальнейший подъем // «Nag.Ru»: информационно-аналитический портал. 11.06.2021. URL: https://nag.ru/material/41392 (дата обращения: 25.02.2022).

4. Какие СУБД используют федеральные органы власти России. Отчет. URL: https://www.tadviser.ru/a/277817 (дата обращения: 27.02.2022).

5. Методика оценки угроз безопасности информации (утв. ФСТЭК России 05.02.2021).
6. Банк данных угроз безопасности информации ФСТЭК России. URL: https://bdu.fstec.ru/threat (дата обращения: 28.02.2022).
7. В России бешеный рост цен на технику. URL: https://www.cnews.ru/news/top/2022-02-25_v_rossii_beshenyj_rost_tsen_1 (дата обращения: 10.03.2022).
8. Правительство утвердило перечень недружественных России стран. URL: https://ria.ru/20220307/perechen-1777030742.html (дата обращения: 10.03.2022).

Статья представлена заведующим кафедрой ЗСС СПбГУТ, кандидатом технических наук, доцентом А. В. Красовым.

УДК 621.391.827.4
ГРНТИ 47.05.09

МЕТОДЫ СИНТЕЗА ИНВАРИАНТНЫХ СИСТЕМ ПЕРЕДАЧИ СООБЩЕНИЙ С ПОСТОЯННЫМИ ПАРАМЕТРАМИ И ИНВАРИАНТНЫХ К АДДИТИВНОЙ ПОМЕХЕ

С. С. Абрамов, Е. С. Абрамова, И. И. Павлов, М. С. Павлова

Сибирский государственный университет телекоммуникации и информатики

В статье рассматриваются методы, лежащие в основе синтеза систем передачи сообщений с постоянными параметрами, инвариантных к аддитивной помехе. Первый метод заключается в нахождении инвариантного оператора, который обладает рядом существенных недостатков. Второй метод – находит оптимальный сигнал, при этом методе достигается наименьшая вероятность ошибки.

абсолютная инвариантность, аддитивная помеха, модуляция, демодуляция, инвариантная система, инвариантные системы передачи сообщений.

Рассмотрим методы, лежащие в основе синтеза систем передачи сообщений с постоянными параметрами, инвариантных к аддитивной помехе.

Первый метод синтеза, который целесообразно назвать методом нахождения инвариантного оператора, заключается в следующем. Сначала безотносительно к полезному сигналу находится линейное преобразование (оператор), которое обозначим через $\Phi_{invar\xi}$, удовлетворяющее условию абсолютной инвариантности:

$$\Phi(\xi) = 0 \quad (\xi \in \Xi), \tag{1}$$

т. е. такое, что при всех $\xi \in \Xi$

$$\Phi_{invar\xi}(\xi) \equiv 0. \quad (2)$$

Затем выбирается сигнал S^* такой, что

$$\Phi_{invar\xi}(S^*) \neq 0. \quad (3)$$

Очевидно, что полученные $\Phi_{invar\xi}$ и S^* являются решениями задачи синтеза системы, абсолютно инвариантной к помехе Ξ.

Проиллюстрируем метод нахождения инвариантного оператора следующим примером [1].

Пусть помеха ξ принадлежит множеству Ξ полиномов $(n-1)$-й степени со случайными коэффициентами $a_0, a_1, ..., a_n$:

$$\xi(t) = a_0 + a_1 t + a_2 t^2 + ... + a_{n-1} t^{n-1}. \quad (4)$$

Очевидно, инвариантным к данному множеству Ξ является линейный оператор n-кратного дифференцирования, а именно:

$$\Phi_{invar\xi}[x(t)] = \frac{d^n[x(t)]}{dt^n}. \quad (5)$$

Действительно, при любых $a_0, a_1, ..., a_{n-1}$, $\Phi_{invar\xi}[\xi(t)] = 0$, что отвечает условию (2). Теперь в качестве полезного сигнала выберем следующую функцию времени:

$$S^*(t) = a_n t^n, \quad (6)$$

которая удовлетворяет условию (3), так как

$$\frac{d^n[\mathrm{S}^*(\mathrm{t})]}{dt^n} = a_n n!. \quad (7)$$

Полученные алгоритм (2) и сигнал (6) полностью определяют абсолютную инвариантную к помехе (4) систему. Необходимо еще определить метод модуляции сигнала (6); поскольку он имеет только один параметр a_n, то информация, очевидно, может быть заложена в величине или знаке этого параметра.

Хотя система, определяемая выражениями (5) и (6), абсолютно инвариантная, она не является оптимальной в присутствии помехи N. Для нахождения оптимальной абсолютной инвариантной помехе Ξ системы с оператором демодуляции $\Phi_{invar\xi}$ следует найти сигнал, максимизирующий полезный эффект на выходе демодулятора. Если этот эффект не зависит от времени, как в случае (7), то задача сводится к максимизации функционала:

$$\left\{ \max_{S(t)} \frac{d^n[S(t)]}{dt^n} \right\}.$$

Рассмотренный метод синтеза, обладая подкупающей простотой, имеет, в то же время, значительные недостатки.

Во-первых, полученный оператор демодуляции $\Phi_{invar\xi}$ абсолютно инвариантный к помехе Ξ, может быть весьма далеким от оптимальности по отношению к помехе N, например, к белому гауссовскому шуму. Поэтому, синтезированная таким способом система, будучи абсолютно инвариантной к помехе Ξ, может обладать сравнительно низкой помехоустойчивостью, т. е. может не удовлетворять левой части определяющего неравенства:

$$p_{доп} \geq p = in \operatorname{var} \Xi . \qquad (8)$$

Этот недостаток несуществен, если помеха N мала или отсутствует.

Во-вторых, не всегда удается подобрать сигнал S^*, удовлетворяющий условию (3), т. е. это функциональное уравнение может не иметь решения, если учесть условия физической реализуемости системы. Например, сигнал, полученный в результате решения (3), может содержать частотные составляющие, лежащие вне полосы пропускания канала связи.

Наконец, в-третьих, и это, пожалуй, самый большой недостаток метода, может не существовать преобразования в классе линейных операторов, удовлетворяющих условию (2) для данной помехи Ξ. В этом случае можно попытаться найти нелинейный оператор, удовлетворяющий условию (2). Однако для нелинейных операторов (1) не является достаточным условием абсолютной инвариантности. Поэтому, если оператор нелинейный, то после нахождения сигнала S^*, удовлетворяющего (2), необходимо найти путем непосредственного расчета результата совместного воздействия сигнала и помехи Ξ на нелинейную систему и проверить выполнение общих условий абсолютной или относительной инвариантности. Следует также рассчитать помехоустойчивость полученной системы при совместном действии сигнала S^* и помех Ξ и N и убедиться в выполнении определяющего требования (8). К сожалению, эти расчеты весьма сложные. Заметим, что наибольший интерес использование нелинейных операторов представляет в системах с пассивной паузой (системах обнаружения сигнала). В этом случае, при отсутствии помехи N и сигнала соответствующая система оказывается абсолютно инвариантной к помехе Ξ, а влияние нелинейности проявляется только при поступлении сигнала.

Таким образом, синтез инвариантных систем, основанный на методе нахождения инвариантного оператора, обладает рядом существенных недостатков. Однако, в некоторых случаях он может дать хорошие результаты. Данное направление создания инвариантных систем развивается, например, в работах [1, 2], где на основе общих идей использования структурных свойств сигналов [1, 3] найдены конкретные алгоритмы и предложены

схемы фильтров (как правило, нелинейных), предназначенных для режектирования случайных помех определенной функциональной структуры, а также произведен анализ воздействия на них сигналов и помех.

Второй метод синтеза инвариантной к аддитивной помехе Ξ системы с постоянными параметрами назовем методом нахождения оптимального сигнала.

В соответствии с этим методом оператор демодуляции выбирается безотносительно к помехе Ξ как оптимальный по критерию вероятности ошибки алгоритм обработки произвольного сигнала S в присутствии аддитивного шума N. Обозначим, этот оператор через $\Phi_{опт}\, N$, подчеркнув этим, что он является оптимальным по отношению к помехе N. Такой выбор оператора демодуляции оправдан тем, что в этом случае абсолютно инвариантная к помехе система будет идеальной инвариантной системой, а относительно инвариантная система будет приближаться к идеальной. Тем самым устраняется недостаток метода нахождения инвариантного алгоритма – ухудшение помехоустойчивости при действии помехи N. С учетом введенного обозначения уравнения (1),

$$\max_{\xi \in \Xi} \left|\Phi(\xi)\right| = \min_{S,\Phi}$$

и

$$\int_{\Omega} [\Phi(\xi)]^2 d\omega = \min_{\Phi,S}$$

примут вид:

$$\Phi_{опт N}(\xi) = 0 \quad (\xi \in \Xi); \tag{9}$$

$$\max_{\xi \in \Xi} \left|\Phi_{опт N}(\xi)\right| = \min_{S}; \tag{10}$$

$$\int_{\Omega} [\Phi_{опт N}(\xi)]^2 d\omega = \min_{S}. \tag{11}$$

Поскольку оператор приемника в (9)–(11) задан, синтез инвариантной системы передачи сообщений по этим уравнениям сводится к синтезу сигнала S, входящего в известный оператор $\Phi_{опт}\, N$.

Здесь уместно отметить отличия данного метода отыскания оптимального сигнала от рассмотренного выше метода отыскания инвариантного оператора. В первом методе оператор демодуляции Φ находится из условия обеспечения абсолютной инвариантности, по отношению к помехе Ξ, а сигнал S – из условия обеспечения наибольшей помехоустойчивости при заданном операторе Ф и помехе N. Во втором методе оператор Ф находится из условия обеспечения наибольшей помехоустойчивости по отношению к помехе N, а сигнал S – из условия обеспечения инвариантности по отношению к помехе Ξ.

Во втором методе оператор Ф находится обычными методами статистической теории оптимального приема сигналов [4, 5], и своеобразное решение задачи связано исключительно с отысканием оптимального сигнала *S*. Например, если *N* – гауссовский белый шум, то оптимальным оператором демодуляции является алгоритм когерентного приема, при котором вычисляется свертка принятого сигнала $x(t)$ и варианта передаваемого сигнала

$$\Phi_{опт N}(\mathrm{x}) = \int_0^T x(t)S(t)dt\,.$$

Тогда (9)–(10) абсолютной и оптимальной относительной инвариантности примут вид:

$$\int_0^T \xi(t)S(t)dt = 0 \quad (\xi \in \Xi)\,; \tag{2.52}$$

$$\max_{\xi(t)} \left| \int_0^T \xi(t)S(t)dt \right| = \min_{S(t)}\,. \tag{2.53}$$

Обычно на сигнал накладываются определенные ограничения по полосе занимаемых частот и энергии. Частотные ограничения позволяют с большей или меньшей точностью представить сигнал как вектор конечномерного гильбертова пространства:

$$S(t) = \sum_{i=n_1}^{n_2} a_i \varphi_i(t)\,,$$

где $\varphi_i(t)$ – система ортонормированных функций.

Ограничение по энергии можно представить, как принадлежность коэффициентов a_i к множеству A такому, что

$$\int_0^T S^2(t)dt = \sum_{i=n_1}^{n_2} a_i^2 = Q\,.$$

Поскольку сигнал и помеха принадлежат одному и тому же пространству функций, определяемому характеристиками канала связи, представим помеху так же, как и сигнал, в виде разложения по системе ортонормированных функций $\{\varphi_i\}$:

$$\xi(t) = \sum_{i=n_1}^{n_2} b_i \varphi_i(t)\,.$$

Коэффициенты b_i являются случайными величинами и принадлежат множеству случайных величин B, определяемых помехой Ξ. Тогда (12) и (13) примут вид:

$$\sum_{i=n_1}^{n_2} a_i b_i = 0 \quad (\mathrm{b}_i \in \mathrm{B}); \tag{14}$$

$$\max_{b_i \in B} \left| \sum_{i=n_1}^{n_2} a_i b_i \right| = \min_{a_i = A}. \tag{15}$$

Условия, при которых эти уравнения имеют решения, удовлетворительные с точки зрения инвариантности соответствующих систем по отношению к помехе Ξ, рассматриваемые способы практического решения задач синтеза оптимальных сигналов по (14) и (15) [6].

Здесь же подчеркнем, что метод нахождения оптимального сигнала далеко не всегда приводит к удовлетворительному, с точки зрения инвариантности, результату. По существу, возможность построения относительно инвариантной системы передачи сообщений по этому методу определяется результатом решения экстремальной задачи общего вида (10) или (11). Если существует сигнал, при котором:

$$\min_{S} \max_{\xi \in \Xi} \left| \Phi_{onmN}(\xi) \right| \le \gamma(\varepsilon), \tag{16}$$

где $\gamma(\varepsilon)$ в соответствии с условием:

$$d\{\Phi[F(S,n,\xi)], \Phi[F_0(S,n)]\} \le \gamma(\varepsilon)$$

допустимое изменение выходного сигнала демодулятора в инвариантной до ε системе, то задача построения оптимальной относительно инвариантной системы передачи сообщений может считаться решенной. Если же неравенство (16) не выполняется, то при использовании данного оператора демодуляции Φ_{onm}N инвариантную до ε к помехе Ξ систему построить нельзя.

Основное практическое значение второй метод синтеза имеет при построении широкополосных систем с составными сигналами, в которых именно благодаря выбору соответствующей формы сигнала удается подавить сосредоточенную по спектру помеху и другие виды помех.

Упомянем еще о третьем способе синтеза инвариантных систем передачи сообщений с постоянными параметрами, который можно назвать методом нахождения оптимального алгоритма.

В соответствии с этим методом оператор демодуляции находится при помощи методов статистического синтеза как оптимальный по критерию минимума вероятности ошибки по отношению к смеси помех N и Ξ при произвольном сигнале $S(t)$. Если при полученном фиксированном операторе демодуляции, который обозначим $\Phi_{onm}N\Xi$, вероятность ошибки p зависит

от формы сигнала, то далее следует решить вариационную задачу, заключающуюся в минимизации функционала, связывающего вероятность ошибки с параметрами сигнала при заданном алгоритме демодуляции

$$p[S(t);\Phi_{optN\Xi}] = \min_{S(t)}.$$

На первый взгляд этот метод, типичный для синтеза оптимальных приемников, не имеет отношения к инвариантным системам передачи сообщений. Однако, хотя при его использовании не ставится в явном виде задача достижения инвариантности, в ряде ситуаций полученный оптимальный алгоритм $\Phi_{optN\Xi}$ при определенных сигналах обладает свойством инвариантности по отношению к помехе Ξ. При этом, естественно, достигается и наименьшая вероятность ошибки, так как оператор $\Phi_{optN\Xi}$ получен из условия минимизации последней – в этом заключается привлекательность данного метода.

Найдены, в частности, алгоритмы оптимального приема сигналов на фоне флуктуационной помехи N и сосредоточенной по спектру помехи Ξ с известной средней частотой. Принцип работы оптимального приемника заключается в компенсации сосредоточенной помехи путем вычитания её оценки из принятой смеси сигнала с помехами. Авторы указывают на возможность практически полной компенсации сосредоточенной помехи, т. е. достижения абсолютной инвариантности системы по отношению к Ξ.

Обратим внимание на возможность сочетания третьего и второго методов синтеза инвариантных систем передачи сообщений. Если оптимальный алгоритм обработки произвольного сигнала $S(t)$ при наличии помех N и Ξ известен, то далее можно отыскивать оптимальный сигнал из условий абсолютной или относительной инвариантности (9)–(11), заменив в них оператор Φ_{optN} оператором $\Phi_{optN\Xi}$. Такая процедура возможна, если алгоритм приема и сигнал могут быть выбраны независимо.

Следует отметить, что описанный в общих чертах метод синтеза, основанный на нахождении оптимального алгоритма, обладает рядом недостатков. Во-первых, не всегда удается найти $\Phi_{optN\Xi}$, так как для этого необходимы сведения о помехе. Если при использовании первых двух методов синтеза, как правило, достаточно знать форму помехи, то при использовании третьего необходимы данные о статистических характеристиках параметров помехи. Во-вторых, алгоритм оптимальной обработки сигнала на фоне обеих помех N и Ξ, как правило, сложен с точки зрения реализации, а в ряде случаев практически нереализуем. Вместе с тем, открываемый третьим методом путь синтеза инвариантных систем еще мало исследован и его возможности полностью не раскрыты [7].

Список используемых источников

1. Заездный А. М., Плоткин Е. И., Черкасский Ю. А. Основы разделения и измерения сигналов по структурным свойствам. М. : ЛЭИС. 1971.
2. Контрович В. Я. К вопросу об оптимальном приеме сигналов на фоне одного класса негауссовых помех. М. : Труды учебных институтов связи. Вып. 48. 1970.
3. Заездный А. М. Сб. трудов НТК по вопросам разделения и измерения сигналов по их структурным свойствам.М. : ЛЭИС. 1968.
4. Теплов Н. Л. Помехоустойчивость систем передачи дискретной информации. М. : Связь. 1964.
5. Гут Р. Э. О помехоустойчивости автокорреляционного приема сигналов однократной фазоразностной манипуляции. М. : Радиотехника. 1972. № 9.
6. Абрамов С. С., Абрамова Е. С., Павлов И. И., Павлова М. С. общие понятия адаптивной системы радиосвязи // Актуальные проблемы инфотелекоммуникаций в науке и образовании. IX Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2020. Т. 1. С. 29–33.
7. Окунев Ю. Б. Основы теории разделения и кодирования сигналов : учебное пособие. Вып. 2. М. : ЛЭИС. 1968.

УДК 004.832
ГРНТИ 28.23.15

ИСПОЛЬЗОВАНИЕ ТЕХНОЛОГИИ БЕГГИНГА ДЛЯ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ КЛАССИФИКАЦИИ ДАННЫХ НА ОСНОВЕ МЕТРИЧЕСКОЙ БЛИЗОСТИ

И. В. Александров, В. В. Фомин

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Рассматривается задача распознавания образов как задача классификации на основе обучения с учителем. Исследуется возможность применения беггинга для методов решающих функций, проверяется возможность применения метода "bootstrap aggregating" для повышения точности классификации в рамках задачи диагностики заболеваний диабетом. Измерения проведены по двум критериям эффективности – метрикам полноты и точности. Приводятся результаты эксперимента, доказывающие целесообразность интегрирования отдельных методов в ансамбль для повышения точности классификации.

распознавание образов, методы решающих функций, классификация данных, беггинг.

Задача классификации данных как одна из востребованных задач распознавания образов являются неотъемлемой частью многих актуальных

прикладных направлений интеллектуального анализа, в том числе в финансовой и банковской сфере, медицинской диагностике заболеваний по результатам анализов и другие. Распознавание образов (*Pattern Recognition*) [1] – одно из направлений искусственного интеллекта, задачей которого является определение принадлежности предъявляемых объектов (процессов) к определенным классам на основе набора отличительных характеристик объектов.

В зависимости от количества известной первоначальной информации об объектах, задачу распознавания образов разделяют на следующие категории [2]:

1) без обучения;

2) на основе обучения с учителем;

3) на основе самообучения.

В рамках текущего исследования анализируется только распознавание образов, на основе обучения с учителем.

В теории распознавания образов на основе обучения с учителем рассматриваются следующие элементы:

1) множество объектов (образов) X;

2) множество меток классов объектов (отклики, ответы) Y;

3) неизвестная целевая функция (зависимость) $f^*: X \rightarrow Y$, связывающая объекты и их метки. Функция f^* известна лишь для объектов конечного множества $X^* = \{x_1,\ldots, x_s\}$ ($X^* \subset X$), значения которой равны y_i^* ($y_i^* = f^*(x_i)$). Кортежи “объект-метка” $<x_i, y_i^*>$ называются прецедентами.

4) ссовокупность кортежей $<x_i, y_i^*>$ ($i = 1..s$) образуют учебную выборку U.

Таким образом, задача распознавания образов на основе обучения с учителем формулируется следующим образом: требуется по имеющиеся учебной выборки U построить (найти, восстановить) неизвестную функцию f^*. Формулировка задачи классификации – если множество Y конечно, его необходимом разбить на c непересекающихся классов, т. е. представить в виде $Y = \{1,.., c\}$.

Для исследования была выбрана группа классических методов интеллектуального анализа, основанная на метриках близости – методы решающих функций [3]. Методы решающих функций основаны на алгоритмах метрической классификации и оценивании сходства объектов. Классифицируемый объект относится к тому классу, которому принадлежат ближайшие к нему объекты обучающей выборки. Рассматриваемые методы неявно опираются на одно важное предположение, называемое гипотезой компактности: если мера сходства объектов введена достаточно удачно, то схожие объекты гораздо чаще лежат в одном классе, чем в разных. В этом случае граница между классами имеет простую форму, а классы образуют компактно локализованные области в пространстве объектов.

В качестве объекта исследования выбрана одна из технологий алгебраической композиции – метод бэггинга (“*bootstrap aggregating*”) [4]. Алгоритм бэггинга основан на идеи коллективного «голосования» независимо обучаемых классификаторов, т. е. классифицируемый объект относят к наиболее часто встречаемому классу среди полученных результатов. Метод бэггинга хорошо поддаётся распараллеливанию по классу распределённых вычислительным систем, алгоритмизации автоматического планирования и распределения вычислительных ресурсов в задачах классификации (рис. 1).

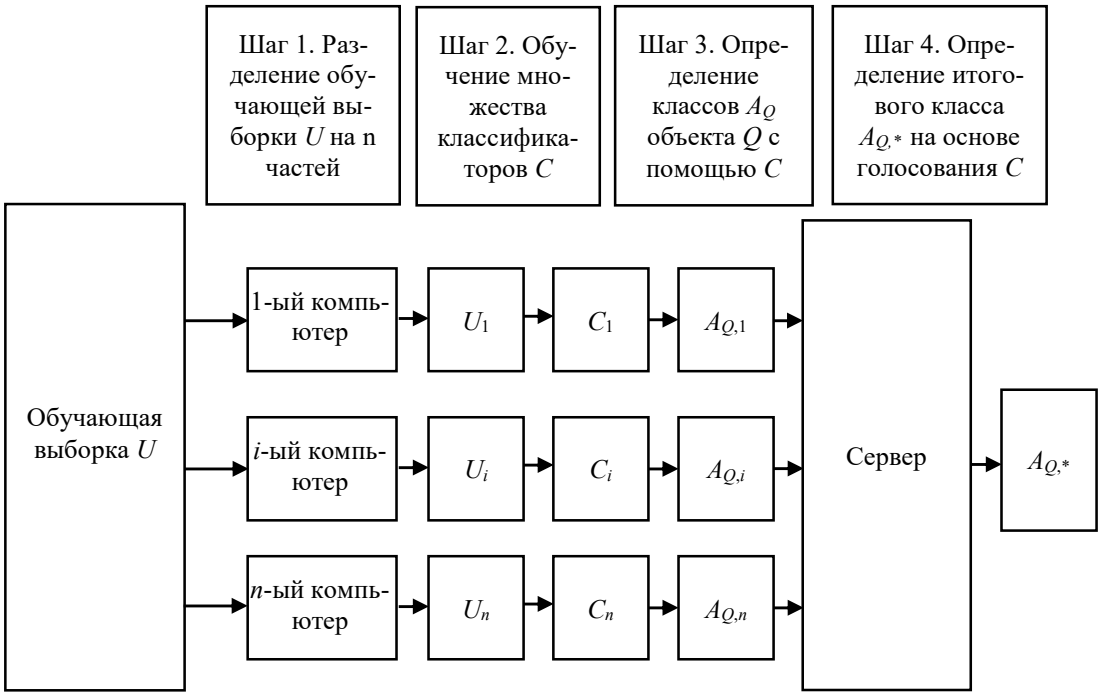


Рис. 1. Параллельная реализация беггинга в Grid системе

В качестве функционального расширения, алгоритм бэггинга был интегрирован в авторскую аналитическую систему распознавания образов на основе Grid-технологии [5].

Проведен эксперимент, исследовавший эффективность классификации данных на основе методов решающих функций и технологии беггинга, со следующими параметрами:

1. Для оценки эффективности классификации объектов были выбраны метрики точности (*precision*) и полноты (*recall*). Точность в пределах класса – это доля объектов, действительно принадлежащих данному классу, относительно всех объектов, причисленных классификатором к этому классу. Полнота системы – отношение числа найденных классификатором объектов, принадлежащих классу, к числу всех объектов этого класса в тестовой коллекции.

2. В качестве методов решающих функций тестировались следующие алгоритмы:

1) метод K ближайших соседей (KNN);
2) метод потенциальных функций (МПФ);
3) метод эталонов (МЭ);
4) метод коррекционных приращений (МКП);
5) метод наименьших среднеквадратических ошибок (МНСКО);
6) метод наивный Байесовский (МНБ).

Концептуально, методы решающих функций одинаковы, однако особенности метрической оценки позволяют учитывать нюансы исходной выборки и делать выбор с позиции точности для частных задач в пользу того или иного метода.

3. В рамках технологии беггинга был сформирован ансамбль из всех вышеуказанных методов решающих функций с единичным весом «компетентности» для каждого алгоритма.

4. Классификация данных производилась по двум классам (наличие/отсутствие диабета) на различных частях задачи «*Diabetes* (UCI_*diabetes_dataset*)» [6]. Для исследования были отобраны обучающая (теоретическая точность) и тестовая (экспериментальная точность) подборки, в которых содержалось одинаковое количество входных данных – 350 записей, каждая из которых имела по 8 признаков.

Результаты эксперимента представлены на рис. 2.

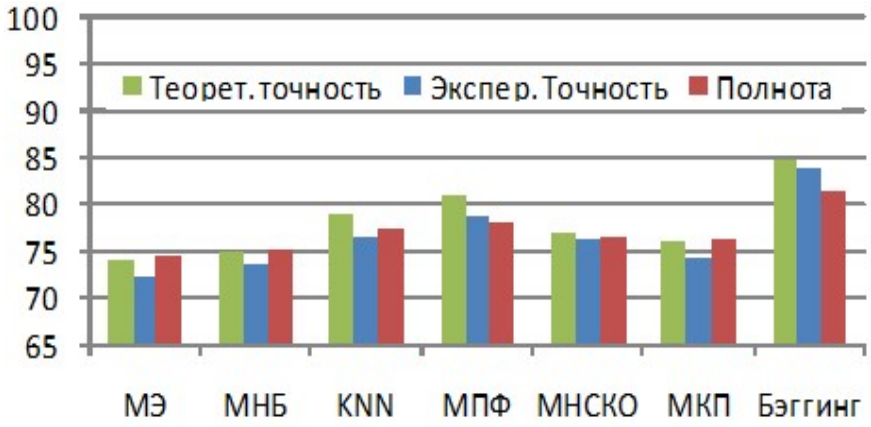


Рис. 2. Сводный график точности и полноты методов

На основе анализа полученных результатов сделаны следующие выводы:

– подтверждено соответствие тенденции зависимостей точности от метода, как при классификации обучающей выборки (теоретическая точность), так и при распознавании классифицируемой выборки (экспериментальная точность);

– полученные точности в пределах одного алгоритма не позволили достигнуть требуемой эффективности результатов в рамках практического применения;

– объединение частных методов в ансамбль позволило повысить точность классификации в среднем на 10 % для рассматриваемой задачи.

Таким образом, экспериментальным путем была доказана целесообразность интегрирования частных метрических методов в ансамбль для повышения точности классификации.

Список используемых источников

1. Ту Д., Гонсалес Р. Принципы распознавания образов. М. : Мир, 1978. 416 с.

2. Bishop C. Pattern Recognition and Machine Learning / C. Bishop: Springer Press, 2006. P. 738.

3. Сикулер Д. В., Фомин В. В. Проектные решения web-ресурса интеллектуального анализа данных и поддержки принятия решений на основе унифицированного класса методов решающих функций. СПб. : РГПУ им. А. И. Герцена. 2016. 102 с.

4. Strobl, C. An Introduction to Recursive Partitioning: Rationale, Application and Characteristics of Classification and Regression Trees, Bagging and Random Forests // Psychological Methods. 2009. Vol. 14, no. 4. P. 323–348.

5. Fomin V., Duke V., Aleksandrov I. The use of machine learning methods for the determination of the fuel consumption of a gas turbine frigate // Marine intellectual technologies. 2019. Vol. 1 (43). PP. 156–160.

6. Diabetes (UCI_diabetes_dataset). URL: https://datahub.io/machine-learning/diabetes (дата обращения: 22.01.2022).

УДК 004.273
ГРНТИ 50.41.01

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ ЗАПИСИ ИНФОРМАЦИИ НА УЗЛЫ РАСПРЕДЕЛЕННОЙ СИСТЕМЫ ХРАНЕНИЯ ДАННЫХ

Н. Н. Алексеева, Н. М. Редругина, А. А. Савельева, И. Ф. Тарабанов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В данной статье описывается процесс построения функциональной модели распределенной системы хранения данных в части процесса записи блоков данных на диски системы. Процедура записи данных на диски в распределительной системе хранения данных отличается необходимостью репликации данных. Произведен сравнительный анализ синхронного и асинхронного подхода к репликации данных и их влияние на QoS

и QoE. Оперирование входными данными позволило предсказать поведение системы и проанализировать подходы к решению возможных проблем.

система хранения данных, распределенная СХД, аналитическое моделирование, система массового обслуживания.

Модель сети массового обслуживания (СеМО) с репликацией входящих блоков данных, состоит из четырех основных элементов как показано на схеме (рис. 1).

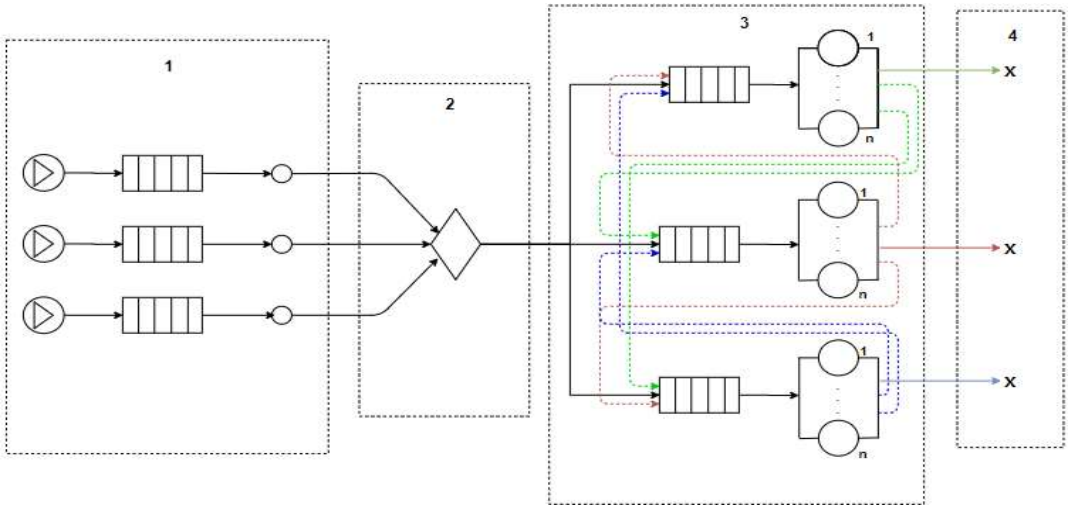


Рис. 1. Схема комплексной модели, рассматриваемой СеМО

Модель сети систем массового обслуживания (СеМО) [1, 2] с репликацией входящих блоков данных состоит из четырех основных элементов:

1. *Сторона клиента,* совокупность клиентов каждый из которых генерирует входящий поток блоков данных на запись в распределенной системе хранения данных. На каждом клиенте есть очередь, которая копит заявки до получения разрешения на обслуживания. Так же данный блок включает компонент обратной связи всё системы, который при получении разрешения от системы, разрешает запись блока данных, пришедшего в очередь раньше всех.

2. *Блок, распределяющий входящие запросы* работает как маршрутизатор, распределяя блоки данных на запись в узлы с какой-либо вероятностью.

3. *Блок обработки входящих запросов.* В каждом узле возможна реализация *n*-го количества дисков. Данный блок представляет собой систему хранения и обработки блоков данных, также на данном блоке происходит репликация записанных данных (блоками) и их дальнейшая обработка другими узлами;

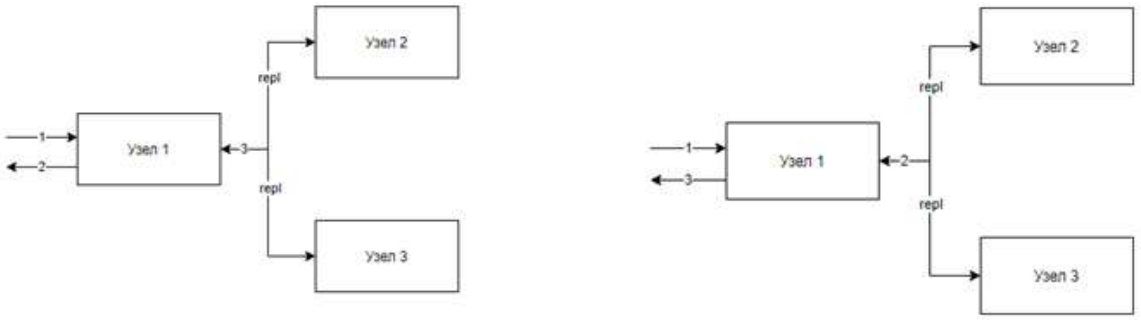
В системе не допускается повторная запись на первоначально выбранный узел, из чего следует необходимость распределения реплицированных данных на конкретные узлы.

4. Выход из системы и *обратная связь,* обеспечивающие безошибочную запись на диски блоков данных.

Обратная связь является отличительная особенностью данной функциональной модели. Организация обратной связи весьма трудозатрата для моделирования как аналитического, так и имитационного. Её главным назначением является сохранение безошибочной работы системы. Это значит, что она контролирует запись оригинального требования и его реплик для полного доступа к любым данным, записанным на дисках, при выходе из строя одного или нескольких узлов.

Далее необходимо рассмотреть возможные варианты реализации обратной связи с обоснованием выбора наиболее подходящей [3].

Первым вариантом реализации обратной связи является разрешение записи следующего блока данных после записи оригинала. Один из существующих и рассматриваемых подходов к распространению обновлений в системе – асинхронный. Асинхронный подход подразумевает запись блока данных на диск, не изменяя все реплики в контексте одной транзакции. Начальная запись на диск производится и фиксируется как можно быстрее, а затем обновления происходят на всех репликах, как показано на схеме (рис. 2а).



а) б)

Рис. 2. Реализация обратной связи: а) асинхронный подход;
б) синхронный подход к репликации данных

Данный подход повысит производительность системы за счет того, что исключает необходимость в ожидании записи реплик данных на все узлы. Однако есть вероятность, что одна из реплик не будет записана и данные будут утеряны. В случае выхода из строя остальных узлов, у клиента не будет возможности получить доступ к этому блоку данных, что сказывается на качестве обслуживания и лишает систему отказоустойчивости. Однако стоит отметить, что очередь на стороне клиентов при таком подходе будет гораздо меньше, что влияет на качество восприятия и скорость работы всей схемы хранения данных (СХД).

Второй вариант реализации обратной связи – разрешение записи после записи последней реплики запроса. Такой подход к распространению обновлений в системе называется синхронный. Синхронный подход к распространению обновлений применяет изменения ко всем репликам в контакте одной транзакции инициализации обновления, что показано на схеме (рис. 2б). Таким

образом, когда транзакция фиксируется, все реплики имеют одинаковое состояние, что достигается путем использования двухфазной блокировки (2PL), либо двухфазной фиксации (2PC) для обеспечения атомарности. Из чего понятно, что синхронное распространение обеспечивает полную согласованность между репликами.

Данный подход в сравнении с предыдущим значительней нагружает систему уменьшая её производительность. Качество обслуживания, которое вычисляется количеством потерянных данных, что при этом подходе сводится к нулевому значению. Однако если принимать во внимание качество восприятия, то на клиентской стороне загруженность очередей заметно больше, чем в других подходах.

На графике (рис. 3) отображены зависимости времени нахождения требования в очереди на стороне клиента от интенсивности входного потока при двух подходах к реализации обратной связи: после записи оригинала данных и после записи последней реплики. Исходя из данных результатов можно сделать вывод, что время в очереди начинает бесконечно расти при синхронной репликации раньше асинхронной репликации, что негативно влияет на качество обслуживания со стороны клиента. На основании данного заключения видится целесообразным реализация синхронного метода записи данных в СХД. Далее при рассмотрении следующей зависимости (рис. 4, см. ниже) возможно сравнить поведение длинны очереди на дисковом устройстве при использовании данных подходов.

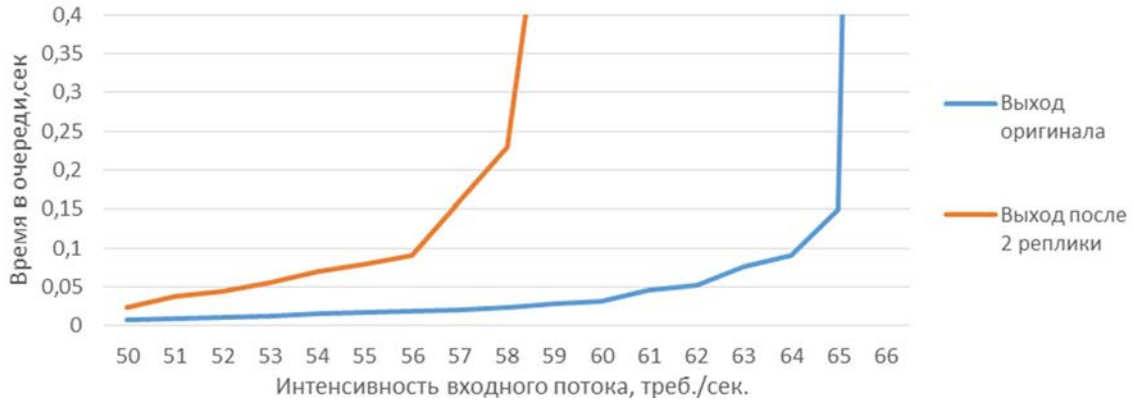


Рис. 3. Зависимость времени нахождения в очереди на клиентской стороне от подхода записи данных

График зависимости длинны очереди на узлах от интенсивности входного потока позволяет заключить, что синхронный подход записи данных помимо обеспечения доступности данных, регулирует входящую нагрузку и не позволяет перегружать систему. Очевидно, что загруженность системы напрямую зависит только от количества клиентов.

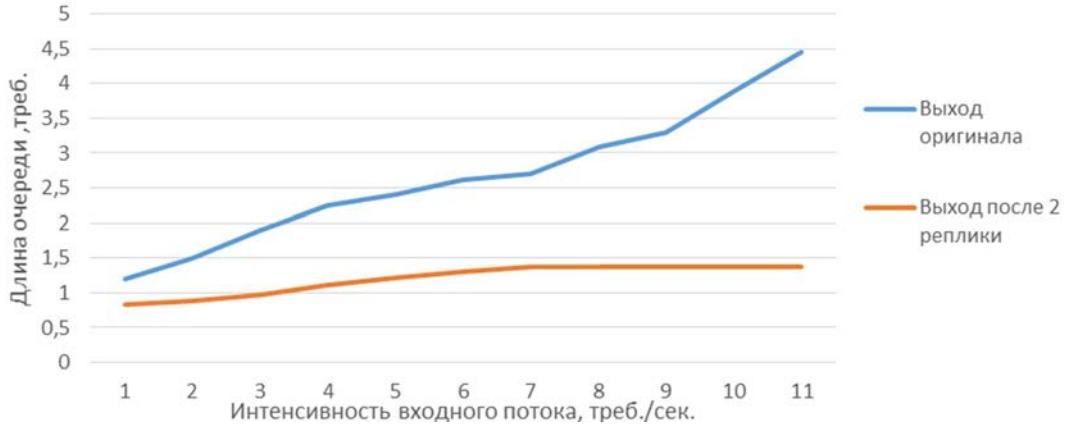


Рис. 4. Зависимость длины очереди на узлах от подхода записи данных

Третьим вариантом реализации обратной связи является разрешение записи после записи первой реплики запроса. Данный вариант реализации обратной связи не дает гарантии к безошибочной работе системы, однако в случае выхода из строя одного узла, данные, записанные клиентом больше чем в 50 %, будут доступны для чтения. Затраты на операции записи при этом меньше, чем в синхронном подходе.

Следующей задачей, рассмотренной в данной статье выбрано определение максимально допустимого количества клиентов при ограниченной очереди ожидания записи на дисковое пространство. В результате проведенного анализа системы было сделан вывод о том, что загруженность очередей на узлах распределенной системы хранения данных напрямую зависит от количества клиентов, обращающихся к нему.

Результатом аналитического моделирования стала формула расчета максимально допустимого количества клиентов, при котором система будет работать исправно:

$$K = \left(\frac{L * Y}{R}\right) + D,$$

где K – допустимое количество клиентов; L – вместимость очереди; Y – количество узлов в системе; R – количество реплик; D – количество дисков.

Для оценки результата моделирования и обоснованность использования данной формулы для расчета необходимого параметра представлен график зависимости длинны очереди на узле от количества допущенных клиентов при μ = const, λ = const и постоянном количестве дисков (рис. 5, см. ниже). Вместимость буфера определена равной 100 требований.

Из расчета при максимальной вместимости очереди равной 100, допустимое количество клиентов равно 151. Это схоже с расчетом имитационного моделирования, следовательно, для дальнейших проверок при более высоких значениях целесообразно использовать аналитическую формулу расчета.

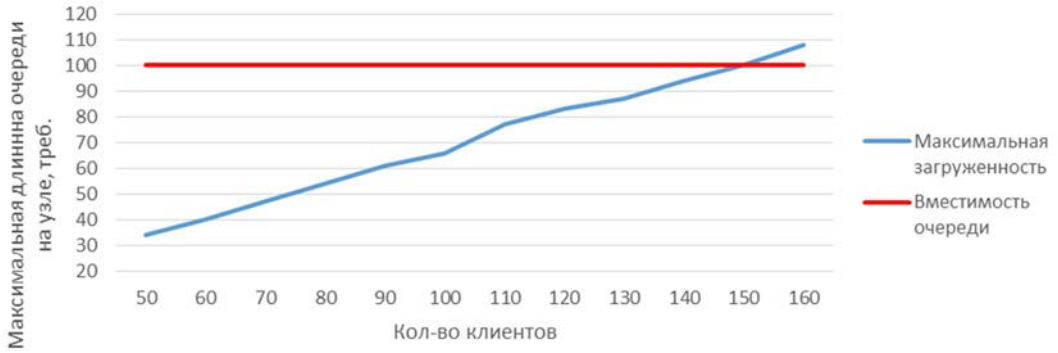


Рис. 5. Зависимость длинны очереди от количества клиентов

Список используемых источников

1. Иверсен Вилли Б. Разработка телетрафика и планирование сетей : пер. с англ. / Под ред. А. Н. Берлина. М. : Нац. Открытый Ун-т «ИНТУИТ» : БИНОМ. Лаб. знаний, 2011. 526 с.

2. Клейнрок Л. Вычислительные системы с очередями :пер. с англ. / Под ред. Б. С. Цыбакова. М. : Мир, 1979. 600 с.

3. Кирносов В. Ю., Куржангулов Н. М. Сравнительный анализ механизмов репликаций данных в различных СУБД // Фундаментальные и прикладные исследования в современном мире. 2017. № 18–1. С. 84–91.

Статья представлена научным руководителем,
кандидатом технических наук, доцентом А. А. Зарубиным.

УДК 004.75
ГРНТИ 20.53.33

ОБЛАЧНЫЕ СЕРВИСЫ. ПРИНЦИП РАБОТЫ, КЛАССИФИКАЦИЯ И МОДЕЛИ ОБСЛУЖИВАНИЯ

Р. В. Алехин, А. В. Красов, А. Д. Макарова, Г. А. Орлов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В наши дни с увеличением объемов передаваемой, принимаемой и хранящейся информации возрастают требования к методам хранения этих данных в центрах обработки данных. Возрастает спрос на использование облачных сервисов. В данной статье представлена основная информация по принципам работы центров обработки данных, а также рассмотрены виды облачных инфраструктур, характеристики и классификация моделей обслуживания со стороны операторов облачных сервисов.

облачные сервисы, облачная инфраструктура, SaaS, PaaS, DaaS, IaaS, оператор облачных сервисов, центры обработки данных.

Процесс организации облачных вычислений базируется на развертывании одного или нескольких, связанных между собой, центров обработки данных. Основной целью является решение задачи, которая заключается в невозможности для стандартного пользователя отличить виртуальную инфраструктуру от физической [1]. Благодаря облачной системе конечный пользователь работает напрямую с вычислительными ресурсами, без мыслей о её технических способностях. Эта особенность позволяет клиенту просто оплачивать определенную услугу, а вся техническая составляющая обслуживания сервиса – задача оператора облачного сервиса [2]. Само взаимодействие пользователя с оператором строится следующим образом:

1. Пользователь заключает договор аренды с оператором облачного сервиса (например, с *Yandex.Cloud*), получая в пользование удалённый сервер.

2. Арендованный сервер конфигурируется: на него устанавливается и настраивается необходимое для выполнения поставленной задачи программное обеспечение.

Существует несколько типов моделей развертывания облачных систем.

Частное облако – инфраструктура, подразумевающая под собой приватное облако, которое функционирует внутри одной организации, включающая в своё пользование некоторых потребителей, иногда – клиентов и подрядчиков организации. Данная инфраструктура может находиться в собственности, управлении и эксплуатации либо в самой организации, либо у третьей стороны, которая является поставщиком услуги, то есть можно зафиксировать, что частное облако может физически находиться как внутри, так и не вне юрисдикции владельца.

Публичное облако – инфраструктура, развернутая для публичного пользования широким кругом лиц. Оно может находиться в собственности, управлении и эксплуатации у различных организаций, но стоит отметить, что в отличии от частного облака, физически публичное находится под юрисдикцией владельца, то есть – под поставщиком услуг.

Общественное облако – инфраструктура, предназначенная для пользования определенных потребителей из организации, имеющих схожий ряд задач и требований, что подразумевает под собой требования безопасности, политики и прочее. Данный вид инфраструктуры находится в управлении организации сообщества, либо у третьих лиц и физически может быть внутри юрисдикции как поставщика услуг, так и вне его.

Гибридное облако – это вид инфраструктуры, являющийся уникальной и стандартизированной по некоторым критериям, таким как технология передачи данных, сборкой различных других, то есть частных, публичных или общественных облаков.

С помощью формирования определенных пакетов услуг, процесс конфигурации сервера часто автоматизируют. В большинстве своем, небольшая стандартизация видов услуг помогает клиентам подобрать тот вид сервиса, который ему необходим по критериям масштабируемости и реализации рабочего процесса [3]. Рассмотрим часть из них:

SaaS ("*Software as a Service*") – аренда конкретного программного обеспечения.

PaaS ("*Platform as a Servic*e") – использование облачного сервиса для разработки нового программного обеспечения.

DaaS ("*Desktop as a Service*") – аренда «рабочего места», сконфигурированного для прямого использования пользователями.

IaaS ("*Infrastructure as a Service*") – аренда информационной инфраструктуры.

Рассмотрим характеристики отдельных моделей обслуживания. Аренда конкретного ПО (*SaaS*) зачастую подразумевает полное отсутствие установки пакета программ. Нет никакой нужды в том, чтобы устанавливать, обновлять и обслуживать конкретный продукт, работающий на этом оборудовании. Стоит отметить, что работа с продуктом возможна мультипользовательская. Пользователь никакого отношения к обслуживанию продукта не имеет, всем занимается поставщик услуг. Стандартная плата за услугу является абонентской платой, что выходит, обычно, дешевле, чем покупка лицензии на софт.

PaaS – является способом предоставления клиенту заранее готовой программной среды и инструментов для её настройки. Элементами PaaS является аппаратное обеспечение, операционная система, СУБД, промежуточное ПО, инструменты тестирования и разработки [4]. В большей степени PaaS предоставляет пользователю возможность для развертывания типовой среды для разработки и теста продуктов. Аналогично, в типовой среде можно разместить резервные площадки и перенести часть рабочих нагрузок из приватного облака в общее и наоборот [5]. Зачастую, PaaS используется программистами, которые работают над различными проектами. В этом случае все или часть разработчиков удаленный получают доступ к общей среде разработки. Соответственно, все они нуждаются в достаточном количестве системных ресурсов, а также в инструментах совместной работы. PaaS без особых проблем позволяет распределить задания, работать с ошибками и с различными версиями проекта. Подобная среда позволяет настроить коммуникацию между программистами, которые внутри среды могут обмениваться информацией друг с другом.

DaaS представляет собой комплекс программного обеспечения, который дается клиенту в пользование для работы. Единственное отличие от физического рабочего стола пользователя является то, что вся инфраструктура

является виртуальной. Клиентский десктоп предоставляется для конкретного предприятия или его отдельного подразделения. В разных случаях для работы предоставляется различный набор программного обеспечения, необходимого клиенту для решения той или иной задачи, то есть набор характеристик является плавающим и разнообразным. Клиент, которому предоставляется доступ к удаленному серверу, получает на дисплее результаты своей работы, которые обрабатываются на стороне провайдера. Дисплей при этом играет роль рабочего стола, который размещен в виртуальной среде. В стандартный комплект DaaS, как правило, включена определенная операционная система, интернет-браузер для доступа к сети, текстовый редактор, приложение для чтения определенных типов файлов и архиватор, но этот набор может отличаться в зависимости от оператора.

IaaS помогает очень сильно снизить финансовые нагрузки компании путем минимизации затрат на локальные центры обработки данных и оборудование. Решения IaaS позволяют гибко масштабировать ИТ-ресурсы в соответствии с увеличением и уменьшением спроса. Повышение надёжности базовой инфраструктуры и быстрая подготовка новых приложений к работе тоже является основным преимуществом использования IaaS [6]. Каждый ресурс предоставляется как отдельный компонент службы, а клиент платите за конкретный ресурс, только на момент нужды в нем. Оператор облачной инфраструктуры полностью ответственен за её работоспособность, а клиент уже отвечает за установленное на инфраструктуру программное обеспечение [7].

Одной из отличительных характеристик рассмотренных моделей является граница ответственности, которая сдвигается от оператора (провайдера) до пользователей (заказчиков), что кратко представлено на рис.

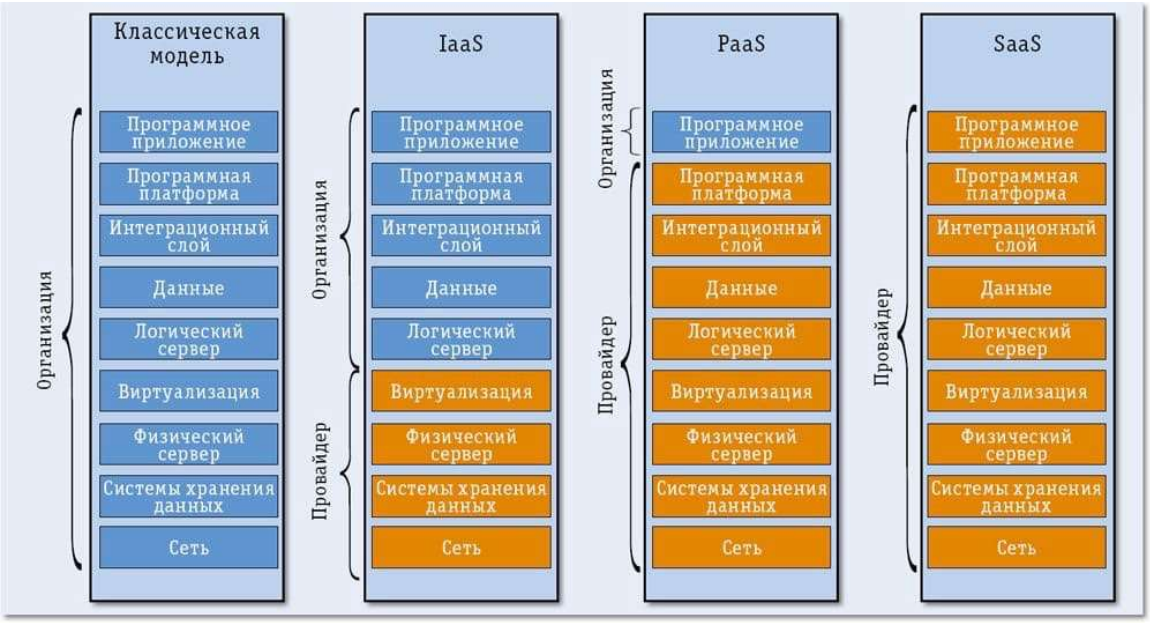


Рисунок. Границы ответственности

Анализируя информацию, представленную на рис. можно уточнить, что ответственность за обслуживание может полностью лежать на провайдере, который предоставляет услуги, либо ответственность делится между оператором и заказчиком.

Подводя итоги разбора принципов работы и моделей обслуживания, можно сказать, что облачные сервисы на протяжении последних лет становятся неотъемлемой частью информационного общества и что в ближайшие года мы увидим их дальнейшее развитие, так как пользование различными услугами и хранение информации в центрах обработки данных значительно влияет на физическую инфраструктуру, позволяя минимизировать хранящееся в организации оборудование [8].

Список используемых источников

1. Меркушев Е. С., Котенко И. В. Механизмы обеспечения целостности облачных вычислений // Региональная информатика «РИ-2018» : материалы конференции. Санкт-Петербург, 2018. С. 158–159.

2. Чмутов М. В., Ковцур М. М., Ушаков И. А., Пестов И. Е. Исследование действующей ИТ-инфраструктуры организации для последующего перехода к облачной архитектуре // Информационная безопасность регионов России (ИБРР-2017) : материалы конференции. 2017. С. 535–537.

3. Котенко И. В., Меркушев Е. С. Механизмы обеспечения целостности данных и вычислительной целостности в облачных системах // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VII Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4-х т. Санкт-Петербург. 2018. С. 493–498.

4. Пестов И. Е. Методика разработки управляющего воздействия на инстансы облачной инфраструктуры // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2020. № 4. С. 72–76.

5. Шемякин С. Н., Пестов И. Е., Федоров П. О., Кошелева С. А. Использование теории графов для моделирования безопасности облачных систем // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2021. № 2. С. 31–35.

6. Krasov A., Vitkova L., Pestov I. Behavioral analysis of resource allocation systems in cloud infrastructure // 2019 International Russian Automation Conference (RusAutoCon). IEEE, 2019. PP. 1–5.

7. Гельфанд А. М., Косов Н. А., Красов А. В., Орлов Г. А. Защита для распределенных отказов в обслуживании в облачных вычислениях // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VIII Международная научно-техническая и научно-методическая конференция : сб. науч. ст. и : в 4 т. Санкт-Петербург. 2019. С. 329–334.

8. Десницкий В. А., Сахаров Д. В., Чечулин А. А., Ушаков И. А., Захарова Т. Е. Защита информации в центрах обработки данных, СПб. Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, 2019. 92 с.

УДК 004.77
ГРНТИ 49.33.29

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ТЕХНОЛОГИЙ C-V2X И DSRC

А. М. Аль-Свейти Малик, А. С. А. Мутханна

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В этой статье исследуется влияние скорости транспортного средства на характеристики режима C-V2X-4 на основе симулятор с открытым исходным кодом. Влияние скоростей на функции окна обнаружения и вероятности сохранения ресурсов также проанализированы соответственно. В результате выполнения исследования установлено, что низкая скорость негативно влияет на производительность C-V2X при этом и производительность снижается стабильнее на высоких скоростях. Более быстрые транспортные средства могут выдерживать более высокие частоты пакетов, поскольку влияние скорости может компенсироваться. Также, были собраны данные для сравнений радиотехнологий DSRC и Cellular V2X (C-V2X) для их применения с целью доставки широковещательных сообщений безопасности V2X.

моделирование, миграция, мультимедийные задачи, сети V2X, DSRC.

Введение

Сегодня две основные тенденции побуждают индустрию беспроводной связи развивать сети сотовой связи пятого поколения: стремительное увеличение спроса на беспроводные широкополосные услуги, требующие значительно больших скоростей передачи данных и сети значительно большей емкости, которые могут предоставлять видео и другие ресурсоемкие услуги, а также услуги Интернета Вещей (IoT), побуждающие к необходимости массового подключения устройств, а также к необходимости сверхнадежной связи со сверхнизкой задержкой [1]. Впервые технология V2X была продемонстрирована на выставке потребительской электроники в Лас-Вегасе (CES) тремя автомобильными компаниями: Ducati, Audi и Ford [2]. Технология V2X, а точнее C-V2X позволяет транспортным средствам автоматически взаимодействовать с разными участниками дорожного движения. Ducati продолжает развивать свою программу «Дорожная карта безопасности 2025», ориентированную на безопасность мотоциклистов. Эта программа предусматривает постепенное внедрение новых технологических модулей систем безопасности в производимом серийном оборудовании. Все началось с внедрения улучшенной работы ABS, с целью помощи при прохождении поворотов, а следующим шагом будет появление у машин

со встроенными передними и задними радарами, работающими с интеллектуальным круиз-контролем, использующим технологию V2X [3].

Постановка задачи

В современной цифровой экономике можно определить ряд различных областей применения, где будут использоваться сети сотовой связи пятого поколения [4]:

– V2X коммуникация (коммуникация транспортных средств между собой и с другими объектами инфраструктуры);

– промышленная автоматизация и коммунальные программы;

– беспроводные медицинские услуги;

– потребительские и бизнес-услуги виртуальной и дополненной реальности; некоторые приложения разумного города;

– умные дома и большое количество применений мобильной широкополосной связи.

Исходя из вышесказанного, можно утверждать, что развитие сотовых сетей пятого поколения и повышение их эффективности является задачей актуальной и перспективной [5]. При этом с развитием сотовых сетей появляются новые более совершенные сетевые архитектуры для передачи данных и управления. Тем не менее, остается ряд нерешенных задач и проблемных мест, которые необходимо решать и устранять соответственно. Так, например, в последние десятилетия модель облачных мощностей и вычислений получила широкое применение в области Информационных Технологий (ИТ) [6].

Анализ технологии V2X и C-V2X

V2x – это технология быстро развивающегося будущего. Сейчас данная разработка только начинает свое использование. Применение V2X будет определяться разными факторами, от одного принятия нормативов и стандартов, до реализации и контроля использования. Хотя эта технология еще совсем новая и малоизвестная, ее внедрением занимаются известные гиганты разработки в технологической сфере и машиностроительной [7]. Кроме всего, технология проявила себя довольно эффективной, полезной и вообще удачной во время предыдущих тестов, а это значит, что компании производители транспортных средств продолжат работу над глобальным внедрением V2X.

C-V2X – это синхронная система, опирающаяся на распределенный механизм планирования передачи пакетов. Этот механизм обеспечивает очень эффективное распределение ресурсов на устройстве C-V2X. «Бюджет задержки пакетов» или PDB – это окно времени, в течение которого пакетам из потока SPS назначаются ресурсы, когда они запланированы впервые.

PDB определяет время задержки пакетов из определенного потока полуустойчивого планирования (SPS) [3].

В различных условиях радиосреды (LOS, NLOS и препятствия) полевые испытания показали, что Cellular-V2X имеет преимущество в диапазоне от 1,3 до 2,9 раза по сравнению с DSRC. Преимущество LOS было в 1,7 раза больше диапазона, однако, после улучшения выросло до 2,2 раза преимущества в некоторых условиях NLOS, включающих помеху сигнала. С учетом помех в непосредственной близости улучшение дальности действия помехи U-NII-3 составило 1,7 раза, тогда как улучшение соседней помехи DSRC составило 2,9 раза (табл. 1, 2).

ТАБЛИЦА 1. Сравнение дальности связи DSRC и C-V2X при эффективной мощности передатчика 5 дБм

Процедура испытания	Дальность связи, м (при 90 % надежности)	
	DSRC	C-V2X
Диапазон прямой видимости (LOS)	625	1050
Нелинейный блокировщик зрения (5GAA)	250/350	450
Блокировка нелинейного зрения (NLOS) (CAMP)	175/250	550 53

ТАБЛИЦА 2. Сравнение дальности связи DSRC и C-V2X при эффективной мощности передатчика 11 дБм

Процедура испытания	Дальность связи, м (при 90 % надежности)	
	DSRC	C-V2X
Диапазон прямой видимости (LOS)	925	>1350
Нелинейный блокировщик прямой видимости (NLOS и 5GAA)	425	625/725
Перекрещение нелинейного зрения (NLOS)	90/400	600/80
Сосуществование с Wi-Fi (полоса пропускания 80 МГц)	550	950
Сосуществование V2X с соседней носительной DSRC	100/325	950

Заключение

Благодаря комбинации различных взаимодействий V2X между транспортными средствами, инфраструктурой и другими участниками дорожного движения (такими как пешеходы и велосипедисты) результаты испытаний показали, что у C-V2X достаточно потенциала для обеспечения безопасности дорожного движения, повышения эффективности дорожного движения и обеспечения информационно-развлекательных сервисов. Кроме того,

тесты также показали сильные стороны технологии в части обеспечения надежности передачи данных и низких задержек связи, что очень важно для критически важных сообщений. По результатам теста C-V2X значительно превзошел DSRC в разных тестах. Надежность и высокая спектральная эффективность связи V2X – это то, что в первую очередь требуют производители транспортных средств, владельцы дорожной инфраструктуры, органы стандартизации и регулирующие органы. Это важно для критических приложений безопасности автомобиля. Проведено много тестов данной технологии с помощью разных сценариев в разных частях света. И хотя технология V2X может работать с помощью DSRC или C-V2X, большинство производителей выбирают технологию C-V2X для использования V2X по причине наличия у нее ряда преимуществ, которые были определены при сравнительном тесте этих систем при одинаковых условиях.

В этой статье исследуется влияние скорости транспортного средства на характеристики режима C-V2X-4 на основе симулятор с открытым исходным кодом. Влияние скоростей на функции окна обнаружения и вероятности сохранения ресурсов также проанализированы соответственно [8].

Список используемых источников

1. Ибрагимов Б. Г., Гумбатов Р. Т., Ибрагимов Р. Ф. Производительность мультисервисных телекоммуникационных сетей на базе архитектурной концепции fn с использованием технологии SD // T-Comm. 2018. № 12. URL: https://cyberleninka.ru/article/n/proizvoditelnost-multiservisnyh-telekommunikatsionnyh-setey-na-baze-arhitekturnoy-kontseptsii-fn-s-ispolzovaniem-tehnologii-sd (дата обращения: 22.01.2022).

2. Ефимушкин В. А., Ледоковских Т. В., Иванов А. Б., Шалагинов В. А. Роль технологий SDN/NFV в инфраструктуре цифровой экономики. Опыт тестирования и внедрения // Электросвязь. 2018. № 3. С. 27–36.

3. R. Molina-Masegosa, J. Gozalvez, and M. Sepulcre. Configuration of the C-V2X Mode 4 Sidelink PC5 Interface for Vehicular Communication // In Proceedings 14th International Conference on Mobile Ad-Hoc and Sensor Networks, MSN 2018, pages 43–48. Institute of Electrical and Electronics Engineers Inc., jul. 2018.

4. Мутханна А. С. Интеллектуальная распределенная архитектура сети связи для поддержки беспилотных автомобилей // Электросвязь. 2020. № 7. С. 29–34.

5. A. Vladyko, A. Khakimov, A. Muthanna, A. A. Ateya, A. Koucheryavy, Distributed edge computing to assist ultra-low-latency vanet applications // Future Internet 11 (6) (2019) 128.

6. A. Vladyko, A. Khakimov, A. Muthanna et al. Distributed Edge Computing to Assist Ultra-Low-Latency VANET Applications // Future Internet. 2019. Vol. 11, Issue 6. P. 128.

7. McCarthy and A. O'Driscoll. OpenCV2X mode 4: A simulation extension for cellular vehicular communication networks // In IEEE International Workshop on Computer Aided Modeling and Design of Communication Links and Networks, CAMAD, volume 2019-September. Institute of Electrical and Electronics Engineers Inc., sep. 2019.

8. F. Eckermann, M. Kahlert, and C. Wietfeld. Performance Analysis of C-V2X Mode 4 Communication Introducing an Open-Source C-V2X Simulator // In IEEE Vehicular Technology Conference, volume 2019-September. Institute of Electrical and Electronics Engineers Inc., sep. 2019.

УДК 004.77
ГРНТИ 49.33.29

СЦЕНАРИИ И МЕТОДЫ ПРИМЕНЕНИЯ БПЛА В КОНЦЕПЦИИ АВТОНОМНОГО УПРАВЛЯЕМОГО ТРАНСПОРТА

А. М. Аль-Свейти Малик, А. С. А. Мутханна

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

БПЛА представляют собой сетевой узел инфраструктуры VANET, так же, как и другие узлы. БПЛА создают каналы связи как с транспортными средствами, так и с сервисами и приложениями ITS. Во время полета БПЛА могут длительное время обеспечивать связь для большинства транспортных средств в связи с тем, что они находятся высоко и взаимодействуют с транспортными средствами в пределах прямой видимости. Использование БПЛА также позволяет значительно увеличить расстояние взаимодействия между сетевыми узлами. Расстояние увеличивается, потому что БПЛА намного выше земли и строений, чем оборудование OBU, поэтому сигналы исчезают и поглощаются окружающими объектами и ландшафтом в меньшей степени.

БПЛА, БА, VANET, DSRC.

Введение

В современном обществе все большее значение приобретают сетевые инфраструктуры, такие как электросети, интернет, трубопроводы и авиационные сети. Эти сети являются линиями нашей повседневной жизни, и безопасность этих сетей серьезно влияет на экологономическое развитие, поэтому мы должны уделять больше внимания безопасности сетевых инфраструктур. Сетевая инфраструктура является ветвью сложных сетей, и соответствующие исследования исходят из сложных сетей, которые привлекают все больше внимания в последние десятилетия.

Операторы мобильных сетей выбирают концепцию самоорганизующейся сети (SON) как экономически эффективный метод развертывания сетей LTE/4G и удовлетворения ожиданий пользователей в отношении высокого качества обслуживания и пропускной способности. Основной целью

SON является внедрение автоматизации в деятельность по управлению сетью и сокращение вмешательства человека. Сети LTE с поддержкой SON в значительной степени полагаются на информацию, полученную от мобильных телефонов, для обеспечения функций самоконфигурации, самооптимизации и самовосстановления. Однако мобильные телефоны могут быть атакованы по воздуху с помощью неавторизованных базовых станций [1].

В реальном мире существует несколько самоорганизующихся сетей, которые оказывают серьезное влияние на развитие современного общества. ниже исследуется уязвимость самоорганизующихся сетей.

За последние два года значительно возросло число призывов к разработке синергетических связей между двумя мирами – (VANET) и автономными транспортными средствами – для достижения дальнейшей безопасности на дорогах и выгоды для конечных пользователей [2]. Автомобильная сеть ad hoc (VANET) состоит из групп, движущихся или неподвижных транспортных средств, соединенных беспроводной сетью. До недавнего времени основное применение VANET было связано с обеспечением безопасности и комфорта водителей в автомобильной среде [3].

Одним из вариантов, который можно использовать для решения проблем слабости информационной безопасности самоорганизующихся сетей, является возможность использования дронов, которые могут быть интегрированы в сеть VANET и обеспечивать требуемую поддержку работы всех необходимых сервисов, организуя стабильное соединение между узлами сети (рис.).

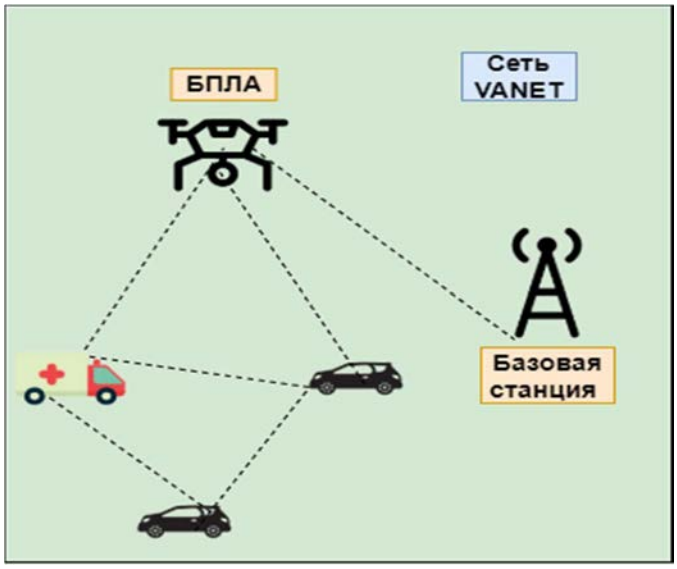


Рисунок. Модель сети VANET с использованием БПЛА

В данной модели, БПЛА выступает в качестве сетевого узла, также как других участников дорожного движения, обеспечивая связь между автомо-

билями и базовой станцией. Использование БПЛА в сетях VANET увеличивает радиус взаимодействия между узлами сети, а также регламентирует подключение автомобилей и устройств к придорожным станциям, где прямое подключение к базовой станции транспортного средства невозможно. Наличие БПЛА над землей намного выше, чем оборудование, встроенное в транспортное средство, увеличивает дальность взаимодействия, делая сигнал менее ослабленным и не поглощаемым окружающей средой.

Помощь БПЛА транспортным средствам способна обеспечить высокие коэффициенты доставки и низкие задержки при эффективном расширении сети связи [4].

Сценарии использования БПЛА

Использование технология радиосвязь ближнего радиуса действия (DSRC) – это технология беспроводной связи, разработанная для обеспечения связи автомобилей в интеллектуальной транспортной системе (ITS) с другими автомобилями или инфраструктурными технологиями. Технология DSRC работает в диапазоне 5,9 ГГц радиочастотного спектра и эффективна на коротких и средних расстояниях. DSRC имеет низкую задержку и высокую надежность, является безопасным и поддерживает оперативную совместимость. Она получает очень мало помех, даже в экстремальных погодных условиях, из-за малого радиуса действия. Это делает его идеальным для связи с и от быстро движущихся транспортных средств.

Технология DSRC может использоваться в формате «автомобиль – автомобиль» (V2V) или «автомобиль – инфраструктура» (V2I), а связь осуществляется с помощью транспондеров, известных как бортовые устройства (OBU) или придорожные устройства (RSU). В формате V2V, DSRC используется для того, чтобы транспортные средства могли общаться друг с другом через бортовые устройства [5]. Такая связь обычно осуществляется в целях безопасности, например, для предупреждения водителя одного автомобиля о том, что автомобиль перед ним собирается снизить скорость. В режиме V2I OBU в автомобиле или на нем связывается с окружающей инфраструктурой, оснащенной RSU. Это также может предупреждать водителя о рисках безопасности, например, о том, что он слишком быстро приближается к повороту, или может использоваться для сбора платы за проезд и парковку.

Используя обработку изображений, можно извлечь полезную информацию о дорогах и транспортных средствах, движущихся по дорогах [6].

Система видеонаблюдения с использованием БПЛА требует технологии высокоскоростной беспроводной передачи данных для получения видеоизображения высокого разрешения в реальном времени в условиях плохого эфирного канала, технологии точного отслеживания местоположения

для определения фактического положения зоны съемки и технологии дистанционного управления для безопасного полета БПЛА.

Цель получения видеоинформации для БПЛА:

1. Оценка дорожной обстановки на дороге с целью своевременного вызова аварийно-спасательных служб и контроля текущих ремонтных работ на дороге.

2. Обнаружение посягательств на дорогу автотранспортом.

3. Оценка состояния дорожной инфраструктуры.

IEEE 802.11p – это обновленная версия стандарта IEEE 802.11b, которая работает на канальном и физическом уровнях и обеспечивает связь между высокоскоростными транспортными средствами.

Так как IEEE802.11p, поддерживает скорость передачи данных от 3 до 27 Мбит/с, что достаточно для HD-видео, БПЛА отлично подходят для данной задачи [4].

Заключение

БПЛА является сетевым узлом в инфраструктуре VANET, а также другими узлами. БПЛА создают каналы связи как с транспортными средствами, так и с ИТС-сервисами и приложениями. Во время полета БПЛА могут обеспечить долгосрочную связь для большинства транспортных средств, поскольку они находятся высоко и взаимодействуют с транспортными средствами в пределах прямой видимости.

Использование БПЛА также позволяет значительно увеличить дистанцию взаимодействия между узлами сети. Расстояние увеличивается, потому что БПЛА находятся намного выше над землей и конструкциями, чем аппаратура бортового устройства, поэтому сигналы исчезают и в меньшей степени поглощаются окружающими предметами и ландшафтом.

Список используемых источников

1. N. Bizanis, and F. A. Kuipers, “SDN and virtualization solutions for the Internet of Things: A survey,” IEEE Access, vol. 4, pp. 5591–5606, 2016.

2. A. Vladyko, A. Khakimov, A. Muthanna et al. Distributed Edge Computing to Assist Ultra-Low-Latency VANET Applications // Future Internet. 2019. Vol. 11, Issue 6. P. 128.

3. A. Vladyko, A. Khakimov, A. Muthanna, A. A. Ateya, A. Koucheryavy, Distributed edge computing to assist ultra-low-latency VANET applications // Future Internet 11 (6) (2019) 128.

4. Мутханна А. С. Интеллектуальная распределенная архитектура сети связи для поддержки беспилотных автомобилей // Электросвязь. 2020. № 7. С. 29–34.

5. Ateya, A. A.; Muthanna, A.; Gudkova, I.; Vybornova, A.; Koucheryavy, A. Intelligent core network for Tactile Internet system // In Proceedings of the International Conference on Future Networks and Distributed Systems, July 2017, (p. 15). ACM.

6. Makolkina M., Koucheryavy A., Paramonov A. The Models of Moving Users and IoT Devices Density Investigation For Augmented Reality Applications // Lecture Notes in Computer Science. 2017. V. 10531. PP. 671–682.

УДК 621.39, 530.182
ГРНТИ 49.29.14

ОСОБЕННОСТИ ИЗМЕРЕНИЯ ПАРАМЕТРОВ СВЕРХКОРОТКИХ ОПТИЧЕСКИХ ИМПУЛЬСОВ ДЛЯ ВЫСОКОСКОРОСТНЫХ ВОЛОКОННО-ОПТИЧЕСКИХ СИСТЕМ ПЕРЕДАЧИ ДАННЫХ

Е. И. Андреева

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Исследованы методы измерения сверхкоротких оптических импульсов, применяемых в высокоскоростных волоконно-оптических системах со спектральным уплотнением. Показана необходимость точного измерения комплекса параметров сверхкоротких оптических импульсов, включая их частотно-временные и энергетические характеристики.

волоконно-оптические системы, волоконный световод, сверхкороткие оптические импульсы, лазеры, нелинейные эффекты.

Для высокоскоростных систем связи необходимо использовать оптические символьные импульсы сверхкороткой длительности. Сверхкороткие оптические импульсы находят все более широкое применение в фотонике, в системах синхронизации, технике, медицине и других областях. Для широкого применения необходимо точное измерение параметров таких импульсов [1–7]. Сверхкороткие импульсы – оптические импульсы длительностью от нескольких десятков пикосекунд и менее. Для характеризации символьной импульсной последовательности требуется определение комплекса частотно-временных и мощностных параметров. В индустрии волоконно-оптических телекоммуникаций основными для систем со спектральным уплотнением являются несущая частота, длительность, оптическая мощность и форма огибающей.

Методы измерений частотных характеристик и методы калибровок и поверок рабочих средств измерений являются предметом деятельности Международной электротехнической комиссии (МЭК). Работа по стандартизации в области волоконно-оптических систем осуществляется Техническим комитетом 86 (ТК86 МЭК). В течение последних лет в Рабочей группе 4 комитета разрабатывался международный стандарт IEC/TS 62129-3:2019 (*Calibration of wavelength/optical frequency measurement instruments. Optical frequency meters using optical frequency combs*). Это уже вторая редакция,

нормативного документа, предыдущая была принята в 2014 году. Эксперименты показали возможность генерации с помощью комб-генератора шкалы частот с нестабильностью, не превышающей 10^{-13} за время более 1000 с [1, 2, 3, 4].

Принцип работы оптического комб-генератора базируется на генерации набора эквидистантных частот с помощью фемтосекундных лазерных импульсов. Уменьшение длительности импульсов до 10^{-13} с приводит к значительному расширению спектра такого излучения. При периодической последовательности импульсов спектр излучения в частотном выражении представляет шкалу узких эквидистантных спектральных линий. Частотный интервал между отдельными линиями равен частоте повторения фемтосекундных импульсов, которая для различных вариантов технической реализации комб-генераторов изменяется от нескольких десятков до нескольких сотен мегагерц и в отдельных случаях может находиться в гигагерцовом диапазоне.

Расширение спектра путем сокращения длительности импульсов недостаточно для перекрытия требуемого частотного диапазона 176,47–272,8 ТГц (1100–1900 нм), поэтому приходится использовать дополнительные устройства, например, нелинейно-оптическую ячейку на основе фотонно-кристаллического волокна, спектральное уширение с помощью фазовой самомодуляции из-за зависимости показателя преломления от интенсивности в оптическом волокне и т. п.

Принцип работы комб-генератора позволяет привязать эквидистантную шкалу частотных линий как к стандартам частоты радиодиапазона, так и к стандартам частоты оптического диапазона в перспективе. В настоящее время стандарты частоты официально связаны с радиодиапазоном. Решение практических задач метрологического обеспечения измерений частоты в высокоскоростных волоконно-оптических системах пока возможно с использованием стандартов частоты только этого типа. В радиодиапазоне наиболее распространены рубидиевые стандарты и водородные мазеры. Для промышленных образцов рубидиевых стандартов нестабильность частоты находится на уровне 10^{-11} за 1000 с. Для калибровки средств измерений с помощью оптического комб-генератора в большей степени подходят водородные стандарты частоты. Отечественные водородные стандарты имеют нестабильность воспроизводимого значения частоты не больше $5 \cdot 10^{-16}$ за 10000 с.

Длительность импульса – носителя информации определяет скорость передачи информации в системе. Изменение длительности импульса, например, вследствие влияния дисперсии в волоконном световоде, должно быть проконтролировано для предотвращения появления ошибок при регистрации информационного потока. Общепринятое определение длительности импульса лазерного излучения дано в международном стандарте

ISO 11554:2006 (ГОСТ Р ИСО 11554-2008). Согласно этому документу, длительность импульса – это максимальный временной интервал между двумя точками по оси времени, в которых мощность достигает половины пиковой мощности.

При скорости передачи данных порядка нескольких Гбит/с длительность оптических импульсов составляет десятки пикосекунд и менее. Большая дальность передачи данных в свою очередь требует высокой мощности оптического импульса на входе линии. При передаче данных такими импульсами в волоконно-оптических системах характер и интенсивность взаимодействия излучения с веществом определяются мгновенной мощностью излучения. Поэтому наряду с энергетическими характеристиками импульсного лазерного излучения, такими как средняя мощность и энергия импульса, большое значение имеют временные характеристики. Это обуславливает необходимость контролировать длительность, форму огибающей и мощность (энергию) сверхкороткого импульса [5, 6].

Измерение длительности сверхкоротких импульсов осуществляется прямыми и корреляционными методами. Прямой метод (метод развертки) измерения длительности оптического импульса пикосекундной длительности, как правило, осуществляется с помощью электронно-оптической камеры. Это наиболее точный метод. Прямой метод регистрации временных параметров используется в составе эталонов высшей точности. Калибровка измерительной системы осуществляется высокоточными интерферометрическими методами с использованием фемтосекундного лазера [6, 7].

Однако область применения этого метода ограничена временем отклика на одиночный сверхкороткий импульс. Для измерения временных параметров импульсов меньшей длительности, чем время отклика электрооптической камеры, применяются корреляционные методы. Наибольшую точность измерения временных параметров субпикосекундных импульсов обеспечивают корреляционные методы, дающие фемтосекундное разрешение. Разработаны методы, позволяющие на основе корреляционных измерений однозначно восстановить огибающую импульса.

Для регистрации излучения малой средней энергии излучения, типичных для волоконно-оптических систем, применяются фотоэлектрические приемники. Для расширения диапазона калибровки средств измерений используется принцип изменения длительности импульса в известное число раз при фиксированной выходной мощности [7]. Необходимое условие – мощный высокостабильный источник.

Таким образом можно сделать вывод, что разработана и постоянно совершенствуется приборная база для измерения комплекса параметров сверхкоротких оптических импульсов, включая их частотно-временные и энергетические характеристики.

Список используемых источников

1. Бакланов Е. В., Покасов П. В. Оптические стандарты частоты и фемтосекундные лазеры // Квантовая электроника. 2003. Т. 33, № 5. С. 383–400.
2. Тан Дж. Н., Стайн Б., Спренджер Б., Хакер Б. Фемтосекундные волоконные лазеры для различных аспектов квантовых технологий // Фотоника. 2018. Т. 12, № 5 (73). С. 502–506.
3. B. R. Washburn, S. A. Diddams, N. R. Newbury. Phase-locked, erbium-fiber-laser-based frequency comb in the near infrared // Optics Lett., v. 29, n. 3, p. 259–252, 2004.
4. Жукова М. О., Ромашова В. Б., Буров Н. В., Болт С. А. Оптические частотные гребенки для метрологических применений – беспрецедентная точность измерений // Фотон-Экспресс. 2018. № 6 (150). С. 14–18.
5. Крутиков В. Н., Канзюба М. В., Берлизов А. Б., Фельдман Г. Г. Комплекс технических средств для воспроизведения, хранения и передачи единицы длительности импульса лазерного излучения в диапазоне $5 \bullet 10^{-11}$ – $1 \bullet 10^{-9}$ с в составе государственного первичного специального эталона // Измерительная техника. 2018. № 11. С. 11–14.
6. Канзюба М. В. Метрологическое обеспечение измерений временных характеристик импульсного лазерного излучения в пикосекундном диапазоне // Фотоника. 2019. Т. 13, № 7. С. 670–75.
7. Кувалдин Э. В. Калибровка источников излучения и приёмных устройств в широком диапазоне измерения энергии оптического излучения // Метрология. 2018. № 4. С. 3–16.

УДК 621.39, 530.182
ГРНТИ 49.29.14

МЕТОДЫ ФОРМИРОВАНИЯ СВЕРХКОРОТКИХ ОПТИЧЕСКИХ ИМПУЛЬСОВ ВЫСОКОЙ МОЩНОСТИ С УЧЕТОМ ЛИНЕЙНЫХ И НЕЛИНЕЙНЫХ СВОЙСТВ ВОЛОКОННЫХ СВЕТОВОДОВ

Е. И. Андреева, А. А. Ермолаев, П. А. Хитров

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Исследованы методы формирования сверхкоротких оптических импульсов высокой мощности в волоконных световодах. Показано, что процесс самосжатия оптического чирпованного импульса может быть использован в линейном режиме распространения. Наибольший эффект достигается в случае нелинейного «многосолитонного» самосжатия оптического импульса. Приведены численные оценки для такого случая.

волоконно-оптические сети, волоконный световод, сверхкороткие оптические импульсы, лазеры, синхронизация мод, оптические солитоны.

Оптические символьные импульсы сверхкороткой длительности находят все более широкое использование [1, 2]. Основные области применения: высокоскоростные системы волоконно-оптической связи; системы синхронизации; измерительные системы; медицина, техника и т. п.

Сверхкороткие импульсы – оптические импульсы длительностью менее 100 пс. Солитоно-образующие импульсы – это спектрально-ограниченные сверхкороткие импульсы высокой мощности. Короткий световой импульс можно получить, модулируя интенсивность излучения непрерывного источника. В современных лазерных системах достигается пикосекундная электрооптическая модуляция. Однако в экспериментах с оптическими солитонами она играет скорее вспомогательную роль - пиковая мощность генерируемых таким образом импульсов не превышает пиковую мощность исходного квазинепрерывного излучения и недостаточна для формирования солитонных импульсов в волоконном световоде. Альтернативный подход основывается на фазировке (синхронизации) различных спектральных компонент источника. Синхронизация различных спектральных компонент широкого спектра позволяет одновременно укоротить импульс и резко увеличить его пиковую мощность. Для фазировки можно использовать внешнюю синхронизацию мод на межмодовой частоте источника – режим активной синхронизации мод, или их нелинейное взаимодействие – самосинхронизация мод. Типичным примером лазера с самосинхронизацией мод является лазер с нелинейным поглотителем: совместное действие усилителя и нелинейного поглотителя обеспечивает формирование сверхкороткого импульса в процессе, известном как пассивная синхронизация мод. Кроме того, самофазировка спектральных компонент используется при генерации коротких импульсов в пассивных системах, использующих самовоздействие или взаимодействие широкополосных волновых пакетов в нелинейной среде.

Для получения солитоно-образующих импульсов наиболее часто применяются источники на полупроводниковых структурах, генерирующие, как правило, импульсы пикосекундной длительности с частотами следования от сотен мегагерц до единиц гигагерц. Генерация импульсов несколько меньшей длительности с большей частотой повторения осуществляется волоконными лазерами. И, наконец, фемтосекундные импульсы с предельно высокими частотами следования (до нескольких терагерц) могут быть получены с использованием нелинейных эффектов в волоконных световодах.

Таким образом, для получения сверхкороткого импульса высокой мощности можно выделить:

– метод компрессии чирпированного импульса в среде с дисперсией другого знака;

– самосжатие мощного сверхкороткого импульса в нелинейной среде (метод многосолитонного сжатия).

Возможность генерации полупроводниковыми структурами пикосекундных импульсов обусловлена широкой, около 10^{13} Гц, линией усиления, и может быть реализована как при прямой модуляции тока накачки, так и в режиме синхронизации мод, причем в последнем случае достигается существенно большая мощность при меньшей величине частотной модуляции (чирпа) генерируемых импульсов и обеспечивается высокая стабильность параметров излучения, что расширяет возможности применения метода синхронизации мод для получения солитоно-образующих импульсов.

Метод компрессии чирпированного импульса в среде с дисперсией другого знака

Для формирования солитона в волоконном световоде входной импульс должен быть спектрально ограничен. Для импульса с гауссовским профилем это означает:

$$\Delta\omega T_o = 1,$$

где $\Delta\omega$ – полуширина спектра импульса (по уровню e^{-1}), а T_o – полуширина импульса (по уровню e^{-1}). Заметим, что длительность импульса по уровню половины максимальной интенсивности: $T_{FWHM} = 1{,}665T_o$.

В случае линейной частотной модуляции спектра импульса ширина спектра импульса увеличивается в $(1 + C^2)^{1/2}$ раз, где C – параметр частотной модуляции. Если $C > 0$, частота линейно увеличивается от переднего фронта к заднему, и уменьшается, если $C < 0$. В волоконном световоде с дисперсией β_2 противоположного знака ($\beta_2 C < 0$) такой импульс испытывает самосжатие до минимального значения длительности:

$$T_1^{min} = \frac{T_o}{\sqrt{(1 + C^2)}}.$$

В этот момент импульс становится спектрально ограничен. Это справедливо при распространении импульса в линейном режиме. Точка максимального самосжатия удалена на расстояние (рис. 1):

$$z_{\min} = \frac{C}{1 + C^2} L_D,$$

где L_D – дисперсионная длина: $L_D = \frac{T_o^2}{\beta_2}$.

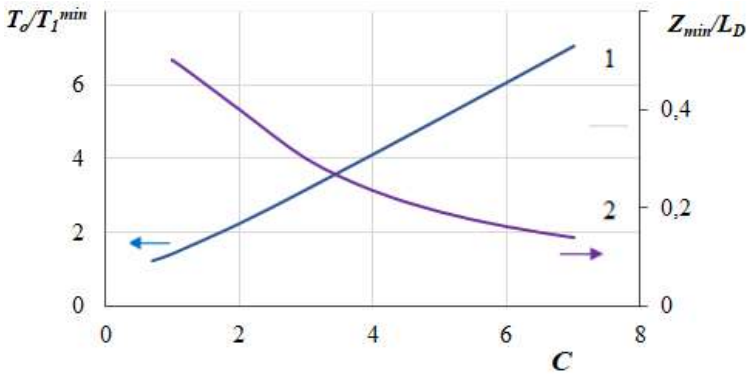


Рис. 1. Зависимость степени самосжатия (1) и положение точки максимального самосжатия $Z_{\min}/L_D$ (2) чирпованного импульса от величины начального чирпа C_o

Самосжатие мощного сверхкороткого импульса в нелинейной среде (метод многосолитонного сжатия)

В среде с аномальной дисперсией можно добиться самосжатия спектрально ограниченного импульса высокой мощности. Для описания распространения сверхкоротких лазерных импульсов в волоконном световоде в области аномальной дисперсии групповых скоростей применяется нелинейное уравнение Шредингера. В общем случае данное уравнение описывает совместное существование как дисперсионных волн, так и солитонных импульсов. Солитонный импульс – волновой пакет, пространственная эволюция которого носит периодический характер. В частности, изменение фазы солитона происходит с пространственным периодом, Z_{SP}.

Солитонное решение уравнения Шредингера:

$$i\frac{\partial u}{\partial \xi}+\frac{1}{2}\frac{\partial^2 u}{2\,\partial \tau^2}+|u|^2u=0,$$

где пространственная координата ξ нормирована на дисперсионную длину L_D, $\xi=\frac{z}{L_D}$, а временная координата τ – на длительность импульса T_o, $\tau=\frac{t}{T_o}$.

Величина пиковой мощности P_0 солитона первого порядка $N = 1$ (фундаментального солитона):

$$P_0=\frac{\beta_2 A_{ef}}{2gT_0^2}=\frac{\beta_2}{\gamma T_0^2},$$

где A_{ef} – эффективная площадь модового пятна световода, γ – нелинейный параметр. Для солитона N-го порядка:

$$P_N=N^2P_o.$$

Энергия E_s фундаментального солитона:

$$E_S=2T_0P_0=\frac{2\beta_2}{\gamma T_0}.$$

Для солитона N-го порядка: $E_N=N^2E_s$

Период солитона Z_{SP} связан с дисперсионной длиной L_D соотношением:

$$Z_{SP}=\frac{\pi}{2}L_D.$$

Важной особенностью солитонов высокого порядка является наличие фазы самосжатия, обусловленной частной модуляцией вследствие эффекта нелинейной фазовой самомодуляции импульса. Для солитона второго порядка точке максимального самосжатия соответствует $z=\frac{Z_{SP}}{2}$.

Коэффициент самосжатия K_s солитонного импульса порядка N можно оценить как (рис. 2):

$$K_S = 4{,}1N.$$

Оптимальное отношение длины волокна L_s к периоду солитона Z_{sp}:

$$\frac{L_S}{Z_{sp}} = \frac{0{,}32}{N} + \frac{1{,}1}{N^2}.$$

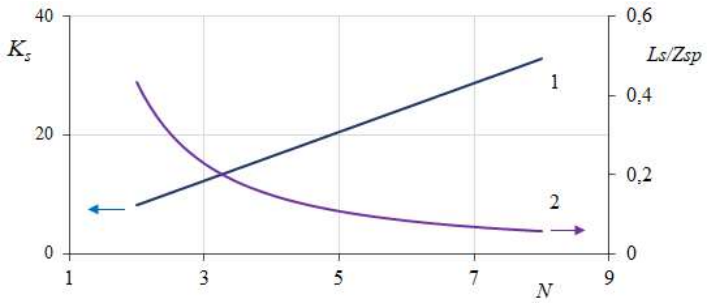
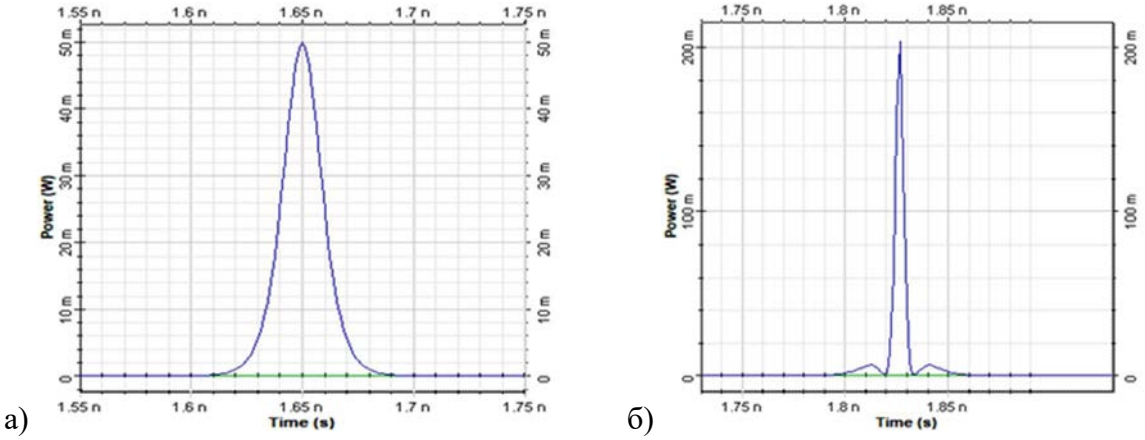


Рис. 2. Зависимость коэффициента самосжатия K_s (1) и положения (2) точки самосжатия, отнесенной к периоду солитона, L_s/Z_{sp} от порядка солитона N

Если пиковая мощность оптическо-го импульса $P_p = N^2P_{fs}$, при $N = 2, 3$, он испытывает самосжатие по мере распространения по волоконному световоду, что может использоваться для формирования сверхкороткого импульса высокой мощности. Моделирование самосжатия импульса в волоконном световоде проводилось в программе OptiSystem. На рис. 3 представлен случай $N = 2$.



а) б)

Рис. 3. Импульс на входе волоконного световода (а) и в точке самосжатия (б)

Таким образом, для получения сверхкоротких импульсов высокой мощности могут использоваться линейные и нелинейные методы самосжатия в волоконных световодах. Импульсы, генерируемые волоконными лазерами, как правило, характеризуются значительным чирпом. При прохождении по световоду с дисперсией другого знака такие импульсы испытывают самосжатие с увеличением пиковой мощности.

Импульсы на выходе полупроводниковых лазеров, как правило, имеют малый чирп и могут использоваться для формирования оптических солитонов. Для формирования сверхкоротких импульсов высокой мощности может использоваться нелинейный эффект многосолитонного самосжатия.

Список используемых источников

1. Агравал Г. Нелинейная волоконная оптика. М. : Мир, 1996. 323 с.
2. Кившарь Ю. С., Агравал Г. П. Оптические солитоны. От волоконных световодов до фотонных кристаллов. М. : Физматлит, 2005. 648 с.

УДК 535.015
ГРНТИ 29.31.27

ИССЛЕДОВАНИЕ ВЛИЯНИЯ ЭФФЕКТА ЧЕТЫРЕХВОЛНОВОГО СМЕШЕНИЯ НА КАЧЕСТВО ПЕРЕДАЧИ В СИСТЕМАХ DWDM И СПОСОБЫ ЕГО ОСЛАБЛЕНИЯ

Е. И. Андреева, Н. В. Яковлев

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Одним из основных направлений современного научно-технического прогресса является всестороннее развитие систем связи, в частности волоконно-оптических линий связи. Сегодня ВОЛС обладают большой информационной емкостью с длиной регенерационных участков до 200 км и более. Это стало возможно, в частности, благодаря технологии спектрального уплотнения WDM. При использовании данной технологии приходиться сталкиваться с нелинейными оптическими эффектами, возникающими в волоконном световоде. Одним из таких эффектов является эффект четырехволнового смешения, оказывающий влияние на качество передачи данных в WDM-системах.

оптические системы связи, волоконные световоды, четырехволновое смешение, нелинейные оптические эффекты.

Суть эффекта четырехволнового смешения (ЧВС) в том, что при взаимодействии трёх и более линейно поляризованных оптических волн с частотами ω_1, ω_2, и ω_3 с достаточно высоким уровнем мощности может наблюдаться уничтожение фотонов одной частоты и рождение фотонов других частот ω_4, являющихся комбинацией частот трёх других частот, с сохранением энергии и импульса.

Общий вид взаимодействия трех линейно поляризованных волн ω_i, ω_j, ω_k можно описать следующим выражением:

$$\omega_{ijl} = \omega_i + \omega_j \pm \omega_k. \quad (1)$$

Так как в результате эффекта ЧВС наблюдается генерация паразитных гармоник в спектре передаваемого сигнала, данный нелинейный эффект

представляет помеху в системах передачи данных со спектральным уплотнением [1, 2, 3, 4]. Этот эффект наиболее заметно проявляется в системах, построенных на волоконных световодах со смещенной дисперсией. Увеличение числа спектральных каналов приводит к значительному возрастанию негативного влияния ЧВС.

Несмотря на энергетическую природу данного эффекта, разрабатыва способов ослабления негативного воздействия ЧВС на качество передачи в системах со спектральным уплотнением служит метод выделенной пассивной спектральной полосы. Данный метод заключается в создании пассивной спектральной полосы между группами рабочих каналов с целью исключения попадания продуктов ЧВС в рабочие полосы пропускания других каналов или канальных групп.

Для иллюстрации метода пассивной спектральной полосы необходимо исследовать распределение комбинационных частот (1), которые можно разделить на:

$$\omega_{ijl} = \omega_i + \omega_j - \omega_k, \;\; i \neq k, j \neq k,$$
$$\omega_{ijl} = 2\omega_i - \omega_k, \;\; i \neq k.$$

Число генерируемых паразитных продуктов ЧВС в зависимости от общего числа рабочих спектральных каналов *N* можно оценить по формуле [2]:

$$N_{(\omega_i+\omega_j-\omega_k)}(m,N) = \frac{m*(N-m+1)}{2} + \frac{[(N-3)^2-5]}{4} - \\ - \frac{[1-(-1)^N*(-1)^{N+m}]}{8}, \quad (2)$$

$$N_{(2\omega_i-\omega_k)}(m,N) = [N-2-0{,}5*(N-2-0{,}5(1-(-1)^N)*(-1)^m], \quad (3)$$

где *m* – индекс спектрального канала от 1 до *N*.

Из данных аналитических представлений (2) и (3) можно сделать вывод, что количество комбинационных спектральных составляющих вида $\omega_{ijl} = 2\omega_i - \omega_k$ намного меньше, чем $\omega_{ijl} = \omega_i + \omega_j - \omega_k$, поэтому их вклад не учитывается. При этом видно, что при увеличении числа рабочих спектральных каналов *N*, число создаваемых помех вида $\omega_i + \omega_j - \omega_k$ значительно увеличивается (рис. 1).

Как видно из результатов моделирования, при увеличении числа каналов в рабочей спектральной группе генерируется бо̀льшее количество помех в области центральных каналов. К тому же наблюдается общее расширение области распределения комбинационных гармоник. Поэтому для реализации 16-канальной системы передачи следует использовать 2 набора по 8 рабочих спектральных каналов с пассивной полосой между ними для уменьшения влияния эффекта ЧВС (рис. 2).

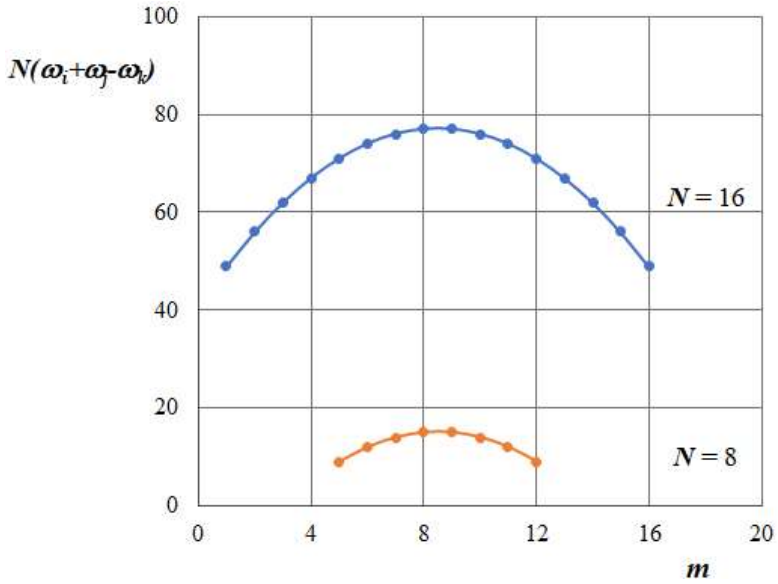


Рис. 1. Поканальное распределение количества продуктов ЧВС в зависимости от общего числа *N* спектральных каналов в системе

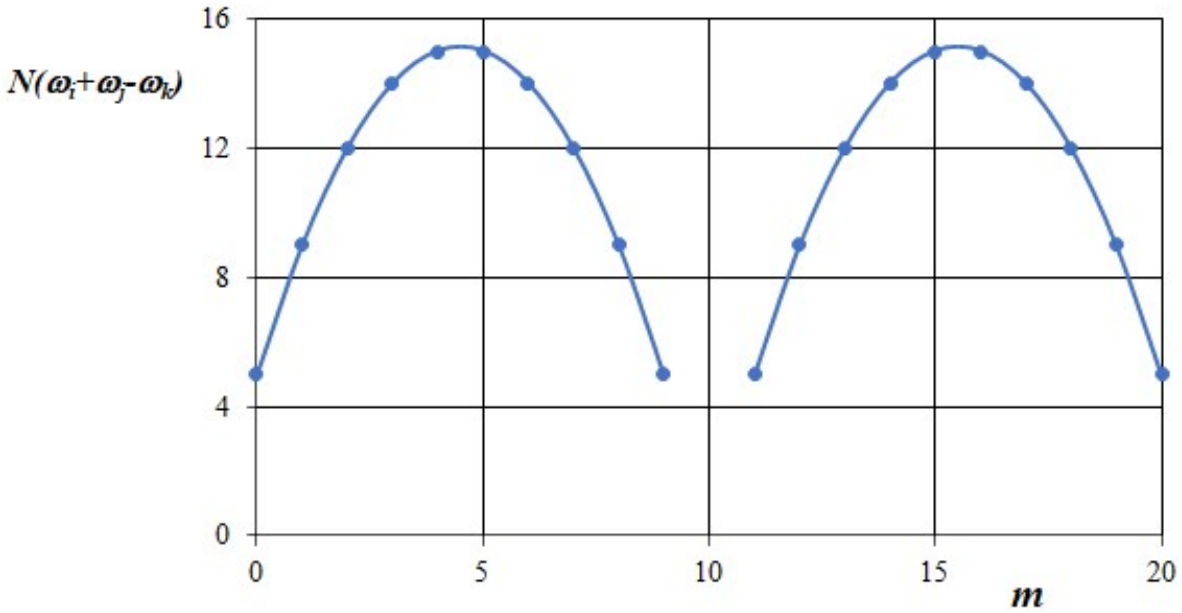


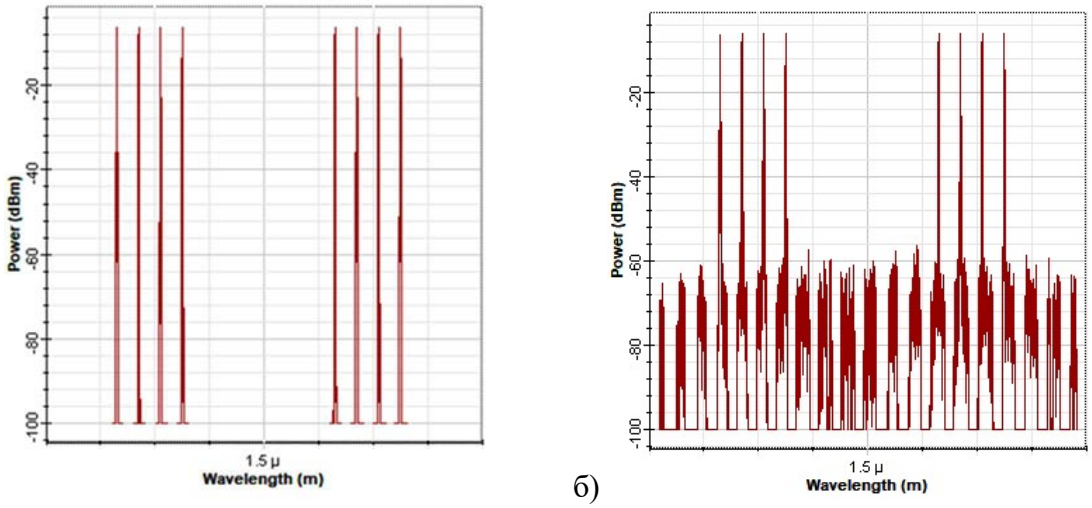
Рис. 3. Распределение продуктов ЧВС с пассивной полосой

Такое решение позволит как уменьшить разброс продуктов ЧВС вне полосы передачи, что уменьшит ширину пассивной полосы, так и снизить их количество на частотах центральных каналов и повысить качество передачи данных в системе (рис. 3).

По данным аналитическим представлениям о распределении продуктов ЧВС вне канальных полос пропускания можно оценить ширину пассивной полосы, кратной межканальному спектральному интервалу.

Моделирование эффекта четырехволнового смешения проводилось в программе OptiSystem. Как и ожидалось, количество продуктов четырехволнового смешения быстро возрастает с ростом числа каналов в системе.

Для демонстрации распределения комбинационных частот – продуктов четырехволнового смешения показан пример использования пассивной полосы (рис. 4). Видно, что общий вклад комбинационных частот снижается при удалении от рабочей спектральной полосы. Таким способом удается существенно снизить помеху от эффекта четырехволнового смешения, в особенности в центральных каналах рабочей спектральной полосы.



а) б)

Рис. 4. Последовательности спектральных каналов, разделенные пассивной спектральной полосой.

Выводы

1. Для снижения влияния эффекта четырехволнового смешения достаточно использовать метод выделения пассивной спектральной полосы между рабочими спектральными каналами.

2. Преимущество метода в том, что он прост в реализации, не требует дополнительного активного оборудования.

3. Эффективность метода возрастает с уменьшением числа каналов в канальной группе.

Список используемых источников

1. Агравал Г. П. Нелинейная волоконная оптика. – М. : Мир, 1996.

2. Варданян В. А. Исследование распределения продуктов четырёхволнового смешивания в ВОСП с ЧРК // Вестн. СибГУТИ. 2016. № 2. С. 78–84.

3. Ferreira M.: "Nonlinear Effects in Optical Fibers", John Wiley & Sons, Inc., Hoboken, New Jersey, USA (2011).

4. Листвин В. Н., Трещиков В. Н. DWDM-системы. – М. : Техносфера. 2017.

УДК 535.14, 372.862
ГРНТИ 29.05.15, 29.01.45

ВИРТУАЛЬНАЯ ЛАБОРАТОРНАЯ УСТАНОВКА ДЛЯ ИЗУЧЕНИЯ ЭФФЕКТА КВАНТОВОГО ЛАСТИКА

А. И. Андрюнин, М. С. Былина

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В настоящее время особое значение приобрели квантовые технологии – современные технологии, основанные на явлениях квантовой физики. Сейчас это одно из наиболее перспективных направлений науки и техники, относящееся к сквозным цифровым технологиям. Выпускники направлений «Инфокоммуникационные технологии и системы связи» и «Фотоника и оптоинформатика» должны получать базовые знания и навыки в этой перспективной области, поэтому в СПбГУТ ведется активная работа по внедрению в учебные планы дисциплин, относящихся к квантовым технологиям. Эти дисциплины предполагают обязательное наличие лабораторного практикума. В данной работе представлена виртуальная лабораторная установка для изучения эффекта квантового ластика, симулирующая интерференционный эксперимент, который демонстрирует квантовую запутанность и принцип дополнительности.

интерференция, одиночный фотон, квантовое состояние, вектор состояния, интерферометр Маха-Цендера, квантовый ластик, виртуальная лабораторная работа.

Предлагаемая в работе виртуальная лабораторная установка Single photon experiments with polarizers: the quantum eraser (эксперименты с одиночными фотонами и поляризаторами: квантовый ластик) [1], показанная на рис. 1, содержит источник одиночных фотонов, интерферометр Маха-Цендера (ИМЦ), состоящий из двух полупрозрачных (BS1 и BS2) и двух непрозрачных (M1 и M2) зеркал, два детектора одиночных фотонов D1 и D2, а также фазовращатель и набор поляризаторов (вертикальный V, горизонтальный H и 45^0), которые можно устанавливать на пути распространяющихся фотонов.

Источник испускает одиночный фотон, который проходит через ИМЦ и регистрируется одним из двух детекторов. Эксперимент можно повторять многократно, при этом виртуальная установка подсчитывает числа срабатываний N_1 и N_2 каждого детектора и вычисляет наблюдаемые вероятности срабатывания P_{1o} и P_{2o} по выражениям:

$$P_{1o} = N_1 / N_{tot}\ , \quad P_{2o} = N_2 / N_{tot}\ , \quad N_{tot} = N_1 + N_2\ .$$

Если измерение траектории фотона не производится (схема 1, нет установленных поляризаторов), между двумя полупрозрачными зеркалами

фотон находится в суперпозиции состояний, соответствующих двум возможным траекториям, и ИМЦ позволяет наблюдать квантовый эффект интерференции одиночных фотонов. При этом на одном из детекторов (D1) наблюдается конструктивная интерференция ($P_{1o} = 1$), а на втором – деструктивная ($P_{2o} = 0$), то есть срабатывать будет только D1.

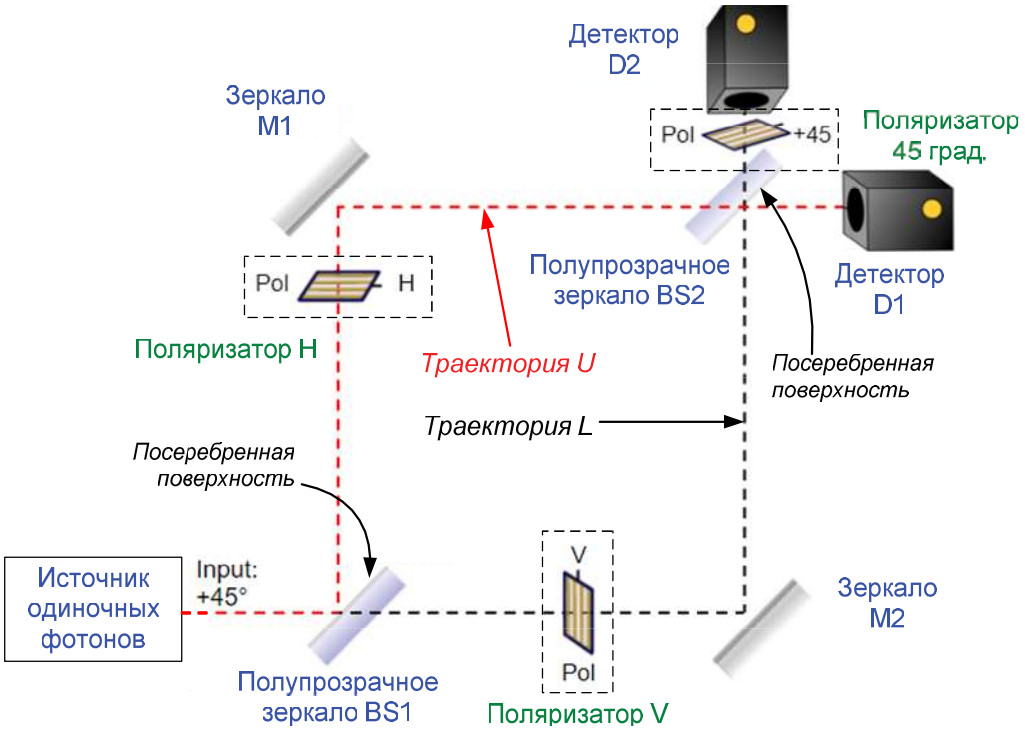


Рис. 1. Виртуальная установка для изучения эффекта квантового ластика

Установка в одно плечо ИМЦ горизонтального, а в другое – вертикального поляризатора (схема 2) эквивалентна измерению траектории фотона, разрушающему суперпозицию состояний и интерференцию. Вероятности срабатывания детекторов становятся одинаковыми.

Если дополнительно поместить перед одним из детекторов – поляризатор 45^0 (схема 3), то можно «стереть» информацию о траектории и восстановить интерференцию. Этот эффект называют эффектом квантового ластика.

Фотон внутри лабораторной установки характеризуется траекторией распространения (L – через нижнее плечо ИМЦ или U – через верхнее плечо ИМЦ) и поляризацией (H – горизонтальной или V – вертикальной).

Математически состояние фотона описывается вектором в четырехмерном пространстве, образованном базисными векторами:

$$|UV\rangle = \begin{pmatrix}1\\0\\0\\0\end{pmatrix}, |UH\rangle = \begin{pmatrix}0\\1\\0\\0\end{pmatrix}, |LV\rangle = \begin{pmatrix}0\\0\\1\\0\end{pmatrix}, |LH\rangle = \begin{pmatrix}0\\0\\1\\0\end{pmatrix}.$$

Любое возможное состояние фотона в лабораторной установке может быть представлено суперпозицией базисных векторов.

Компоненты лабораторной установки (зеркала и поляризаторы) изменяют состояние фотона. Математически действие компонента можно описать матрицей 4×4. Вектор состояния $|q_{out}\rangle$ фотона на выходе компонента можно получить, умножив матрицу этого компонента на вектор $|q_{in}\rangle$ входного состояния фотона [2, 3].

Полупрозрачное зеркало изменяет на π фазу света, отраженного от границы раздела между воздухом и посеребренной поверхностью. Например, для зеркала BS1 это свет, распространяющийся по траектории *U*, поэтому матрица **BS1** будет иметь вид:

$$\mathbf{BS1} = \frac{1}{\sqrt{2}} \cdot \begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix} \otimes \mathbf{I} = \frac{1}{\sqrt{2}} \cdot \begin{pmatrix} -1 & 0 & 1 & 0 \\ 0 & -1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix},$$

где **I** – единичная матрица 2×2, ⊗ означает тензорное умножение.

Зеркала M1 и M2 изменяют на π фазу отраженного света, независимо от его траектории, то есть их действие описывается матрицей:

$$\mathbf{M} = \mathbf{M1} = \mathbf{M2} = \begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}.$$

Вид матрицы поляризатора будет зависеть от того, в каком плече ИМЦ он установлен. Например, матрицы $\mathbf{P_{HU}}$ и $\mathbf{P_{VL}}$ – поляризаторов *H* в плече *U* и *V* в плече *L*, показанных на рис. 1, будут иметь вид:

$$\mathbf{P_{HU}} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \mathbf{P_{VL}} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

Студентам предлагается провести многократные измерения в трех описанных выше схемах, исследовать изменения наблюдаемых вероятностей срабатывания детекторов и подтвердить свои наблюдения теоретическими расчетами.

Состояние фотона $|q_0\rangle$ на входе лабораторной установки представляет собой суперпозицию базисных векторов $|UV\rangle$ и $|UH\rangle$:

$$|q_0\rangle = \frac{1}{\sqrt{2}} \cdot (|UV\rangle + |UH\rangle) = \frac{1}{\sqrt{2}} \cdot \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix}.$$

Рассмотрим изменения состояния фотона при его распространении внутри установки в схеме 1:

после BS1: $$|q_1\rangle = \mathbf{BS1} \cdot |q_0\rangle = 0{,}5 \cdot \begin{pmatrix} -1 \\ -1 \\ 1 \\ 1 \end{pmatrix},$$

после M1 (M2): $$|q_2\rangle = \mathbf{M} \cdot |q_1\rangle = 0{,}5 \cdot \begin{pmatrix} 1 \\ 1 \\ -1 \\ -1 \end{pmatrix},$$

после BS2: $$|q_3\rangle = \mathbf{BS2} \cdot |q_2\rangle = \frac{1}{\sqrt{2}} \cdot \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix}.$$

На детекторы фотон приходит в состоянии $|q_3\rangle$. Рассчитаем теоретическую вероятность детектирования фотона детекторами D1 и D2:

$$\text{детектор D1: } P_1 = ||UV\rangle^T \cdot q_3|^2 + ||UH\rangle^T \cdot q_3|^2 = 1, \quad (1)$$

$$\text{детектор D2: } P_2 = ||LV\rangle^T \cdot q_3|^2 + ||LH\rangle^T \cdot q_3|^2 = 0. \quad (2)$$

Из (1) и (2) видно, что в результате интерференции будет срабатывать только один детектор.

Схема 2 включает поляризаторы *H* в плече *U* и *V* в плече *L*. Можно показать, что вектор состояния фотона на входах детекторов имеет вид:

$$|q_4\rangle = \frac{1}{2\sqrt{2}} \cdot \begin{pmatrix} 1 \\ 1 \\ -1 \\ -1 \end{pmatrix}.$$

Расчет показывает, что срабатывание детекторов D1 и D2 в этой схеме равновероятно:

$$\text{детектор D1: } P_1 = ||UV\rangle^T \cdot q_4|^2 + ||UH\rangle^T \cdot q_4|^2 = 0{,}25,$$

$$\text{детектор D2: } P_2 = ||LV\rangle^T \cdot q_4|^2 + ||LH\rangle^T \cdot q_4|^2 = 0{,}25.$$

Таким образом, в схеме 2 наблюдается эффект разрушения интерференции.

Отметим, что сумма вероятностей P_1 и P_2 равна 0,5, так как с вероятностью $P_3 = 0{,}5$ фотон будет поглощен одним из поляризаторов.

Схема 3, демонстрирующая эффект квантового ластика, включает три поляризатора *H* в плече *U*, *V* в плече *L* и 45^0 перед детектором D2. Вектор состояния фотона на входах детекторов имеет вид:

$$|q_4\rangle = \frac{1}{2\sqrt{2}} \cdot \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix}.$$

Расчет теоретической вероятности детектирования фотона детекторами D1 и D2 показывает, что интерференция восстановилась, и снова срабатывает только детектор D1:

$$\text{детектор D1:} \quad P_1 = ||UV\rangle^T \cdot q_5|^2 + ||UH\rangle^T \cdot q_5|^2 = 0{,}25,$$

$$\text{детектор D2:} \quad P_2 = ||LV\rangle^T \cdot q_5|^2 + ||LH\rangle^T \cdot q_5|^2 = 0.$$

Сумма вероятностей P_1 и P_2 равна 0.25, так как с вероятностью $P_3 = 0{,}75$ фотон будет поглощен одним из поляризаторов.

Результаты теоретических расчетов и экспериментальных исследований в каждой схеме студенты оформляют в виде таблицы.

ТАБЛИЦА. Результаты измерений и расчетов

Количество фотонов, ед.	Наблюдаемое число срабатываний детекторов		Наблюдаемые вероятности срабатывания детекторов		Теоретические вероятности срабатывания детекторов	
	D1	D2	D1	D2	D1	D2
100						
200						
300						
...						
1000						

В результате выполнения работы студенты закрепляют и углубляют свои знания о квантовых объектах и их состояниях, экспериментально убеждаются в наличии интерференции одиночных фотонов, учатся применять математический аппарат квантовой механики.

Возможности лабораторной установки не ограничены тремя проанализированными схемами. Наличие трех поляризаторов и фазовращателя с настраиваемым сдвигом фаз позволяет предлагать студентам различные задания не только учебного, но и исследовательского уровня.

Предлагаемая лабораторная работа будет внедрена в учебный процесс кафедры «Фотоники и линий связи».

Список используемых источников

1. Виртуальная лабораторная установка Single photon experiments with polarizers: the quantum eraser (Open source software) [Электронный ресурс]. URL: https://www.st-andrews.ac.uk/physics/quvis/simulations_html5/sims/QuantumEraser/QuantumEraser.html.

2. Никитин Н. В., Томс, К. С., Фотина О. В. Аксиомы квантовой механики. – М.: Университетская книга, 2015. – 130 с.

3. Чернов П. С. Квантовая механика: конспект лекций (избранные вопросы). – Пенза : Изд-во Пензенского университета, 2013. – 126 с.

УДК 004.732
ГРНТИ 49.43.29

ИССЛЕДОВАНИЕ ЭФФЕКТИВНОСТИ ТЕХНОЛОГИИ ФОРМИРОВАНИЯ ЛУЧА В СЕТЯХ СТАНДАРТА IEEE 802.11AC

А. Д. Антоненко, Я. А. Герасимова, Р. А. Дунайцев

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Технология адаптивного формирования диаграммы направленности передатчика, также известная как технология формирования луча, подразумевает формирование электромагнитного поля антенн передающего устройства в дальней зоне в виде узконаправленного главного лепестка, ориентированного в сторону принимающего устройства, с возможностью изменения направленности по мере необходимости. Данная технология впервые появилась в стандарте IEEE 802.11n и получила дальнейшее развитие в последующих стандартах IEEE 802.11ac и IEEE 802.11ax. В статье представлены результаты экспериментального исследования эффективности технологии формирования луча в сетях стандарта IEEE 802.11ac. Проводится анализ скорости передачи кадров данных, коэффициента повторных передач, а также уровня принимаемого сигнала с использованием и без использования указанной технологии.

IEEE 802.11ac, TxBF, transmit beamforming, формирование луча.

Технология адаптивного формирования диаграммы направленности передатчика, также известная как технология формирования луча (*transmit beamforming*, TxBF), впервые появилась в стандарте IEEE 802.11n, выпущенном в 2009 году [1]. Данная технология позволяет передающему устройству, оборудованному несколькими всенаправленными антеннами, сфокусировать излучаемую энергию в сторону принимающего устройства с целью повышения уровня сигнала на приеме (*received signal strength*), увеличения отношения сигнал/шум (*signal-to-noise ratio*, SNR), снижения количества ошибочных битов и повторных передач кадров, а также обеспечения высокой скорости передачи данных. При этом устройство, фокусирующее передаваемый сигнал в сторону адресата, называется формирователем

луча (*beamformer*), а устройство, в чью сторону формируется луч, – получателем луча (*beamformee*). Wi-Fi роутеры и точки доступа, равно как и всевозможные клиентские устройства (смартфоны, планшеты, ноутбуки, внешние Wi-Fi адаптеры и т.п.) могут выступать как в роли формирователя, так и в роли получателя луча. Однако поскольку данная технология не является обязательной, далеко не все выпускаемые устройства поддерживают ее. Также следует отметить, что формирование луча используется лишь при одноадресной (*unicast*) передаче кадров, а широковещательные (*broadcast*) и многоадресные (*multicast*) рассылки происходят в обычном режиме.

В стандарте IEEE 802.11n были описаны два варианта данной технологии: неявного (*implicit*) и явного (*explicit*) формирования луча. В первом варианте устройство, в чью сторону направляется луч, напрямую не участвует в этом процессе. В результате получателем луча могло быть устройство либо предыдущего поколения Wi-Fi (IEEE 802.11a/b/g), либо этого же поколения (т. е. IEEE 802.11n), но не имеющее соответствующего функционала. Во втором варианте получатель луча активно участвует в процессе, обеспечивая обратную связь с формирователем луча. С одной стороны, это позволяет сформировать луч с большей точностью, а с другой – ограничивает область применения данной технологии, так как в этом случае оба устройства должны ее поддерживать. В стандарте IEEE 802.11ac [2], ратифицированном в 2013 году, отказались от неявного формирования луч в пользу явного. Процесс начинается с отправки формирователем луча получателю специального кадра NDP Announcement. Вслед за ним, спустя короткий межкадровый интервал (*short interframe space*, SIFS), передается так называемый Null Data Packet (NDP), который представляет из себя PLCP-кадр без данных внутри, но содержащий длинные обучающие поля VHT (*VHT long training field*, VHT-LTF) для каждого пространственного потока. В свою очередь, выждав короткий межкадровый интервал, получатель отправляет формирователю в сжатой форме матрицу обратной связи (*compressed beamforming feedback matrix*), в которой содержится информация о состоянии беспроводного канала связи, полученная на основе анализа, принятого NDP. В результате формирователь рассчитывает управляющую матрицу (*steering matrix*), которая определяет настройку антенн передатчика для последующей отправки кадров данных.

Для исследования эффективности технологии формирования луча в сетях стандарта IEEE 802.11ac использовалось следующее оборудование. Wi-Fi роутер TP-Link Archer A6v2 [3] был подключен сетевым кабелем категории 6 к настольному компьютеру, который выступал в качестве сервера. Wi-Fi адаптер TP-Link Archer T9UHv1 [4] через порт USB 3.0 был подключен к ноутбуку, выступавшему в качестве клиента. Для организации двусторонней передачи данных по протоколу TCP между устройствами использовалась утилита TamoSoft Throughput Test. Захват трафика производился на

ноутбуке с помощью программы Savvius Omnipeek и Wi-Fi адаптера NETGEAR A6210. Расстояние между Wi-Fi роутером и ноутбуком составляло 20 метров. Сами устройства находились в двух несмежных аудиториях 508 и 512 первого учебного корпуса СПбГУТ по адресу пр. Большевиков, д. 22 [5]. У всех Wi-Fi устройств был выбран режим IEEE 802.11ac. Ширина канала была установлена равной 20 МГц. Измерения проводились на каналах 36, 40, 44 и 48 диапазона 5 ГГц. Функционал для формирования луча поочередно включался и отключался. Настройки Wi-Fi роутера и Wi-Fi адаптера показаны на рис. 1 и 2.

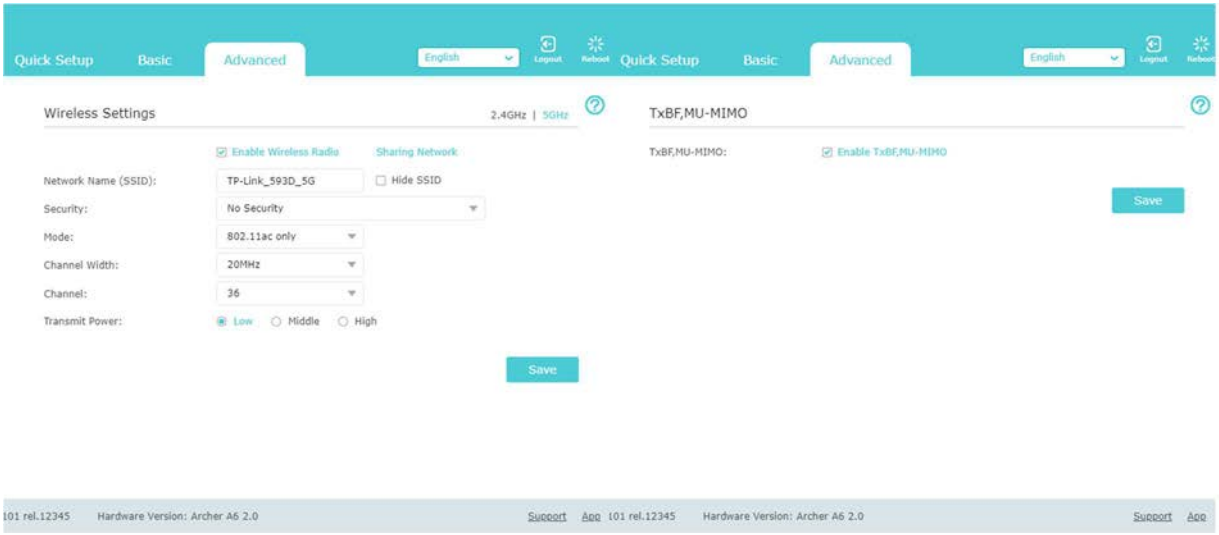


Рис. 1. Настройки Wi-Fi роутера TP-Link Archer A6v2

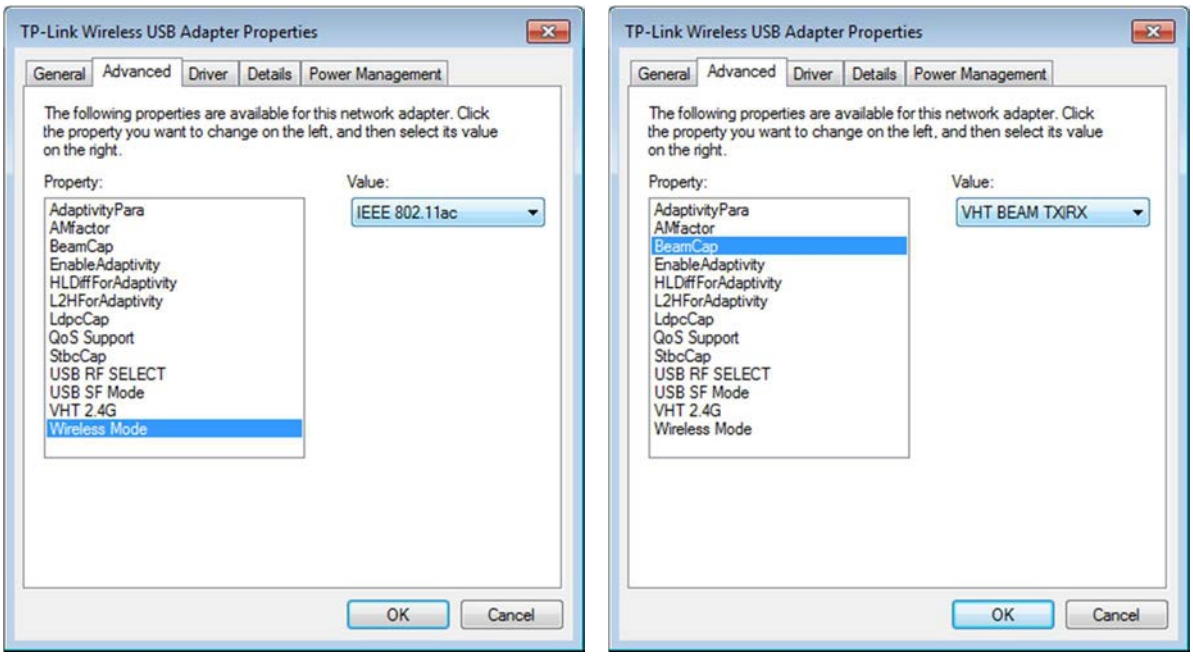
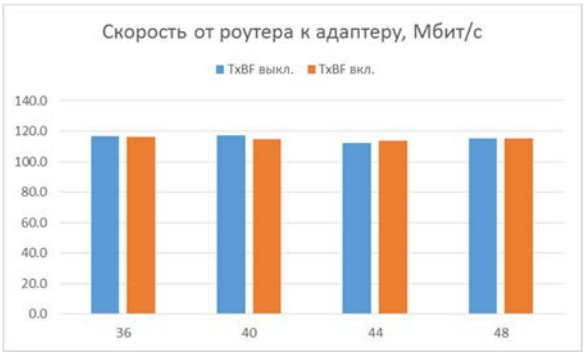
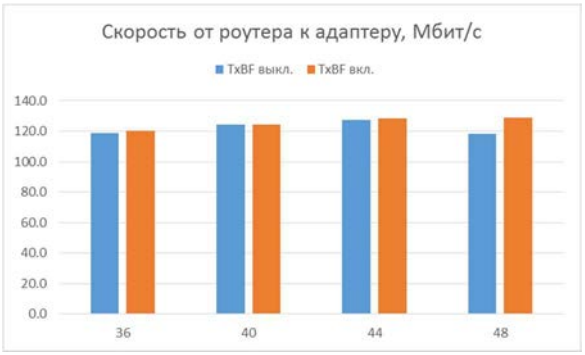


Рис. 2. Настройки Wi-Fi адаптера TP-Link Archer T9UHv1

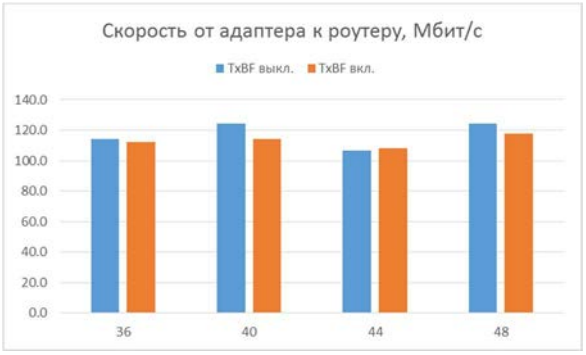
Для передачи данных поочередно использовались каналы 36, 40, 44 и 48 с применением и без применения технологии формирования луча. Всего было произведено три серии таких экспериментов. Для определения эффективной скорости передачи кадров (*effective data rate*) и коэффициента повторных передач кадров (*retry rate*) использовалась программа MetaGeek Eye P.A., а для измерения уровня шума (*noise floor*) и коэффициента загруженности каналов (*utilization*) – программа MetaGeek Chanalyzer. Спектральный анализ радиоэфира показал, что средний уровень шума на момент проведения исследования составлял – 101 дБм, а коэффициент загруженности рассматриваемых каналов был около 0 %. Иными словами, значительной интерференции или помех в каналах не наблюдалось. Для имитации работы Wi-Fi устройств на различном удалении друг от друга мощность передатчика Wi-Fi роутера (см. рис. 1) устанавливалась либо как низкая (*Low*), либо как высокая (*High*), что эквивалентно увеличению или уменьшению расстояния до Wi-Fi адаптера. Усредненные результаты экспериментов представлены на рис. 3–5.



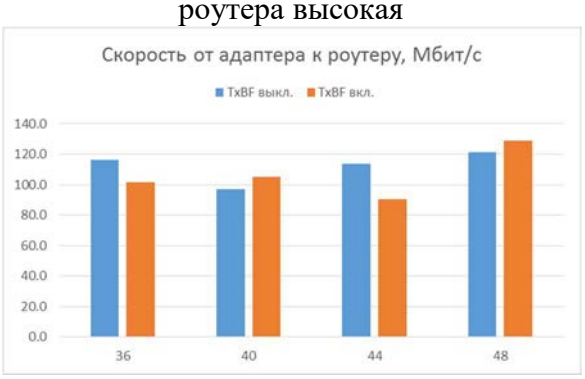
а) Мощность передатчика роутера низкая



б) Мощность передатчика роутера высокая



в) Мощность передатчика роутера низкая

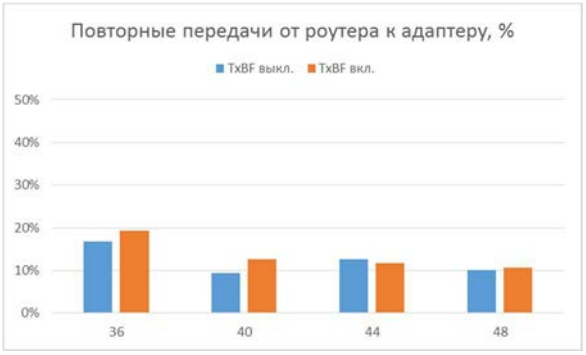


г) Мощность передатчика роутера высокая

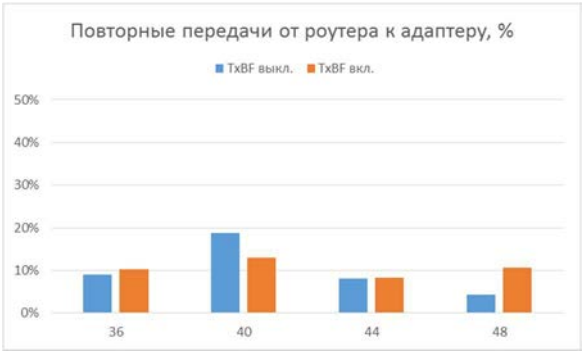
Рис. 3. Эффективная скорость передачи кадров данных между роутером и адаптером

Следует отметить, что в Wi-Fi адаптере TP-Link Archer T9UHv1 используется схема MIMO 4x4:3, а в Wi-Fi роутере TP-Link Archer A6v2 –

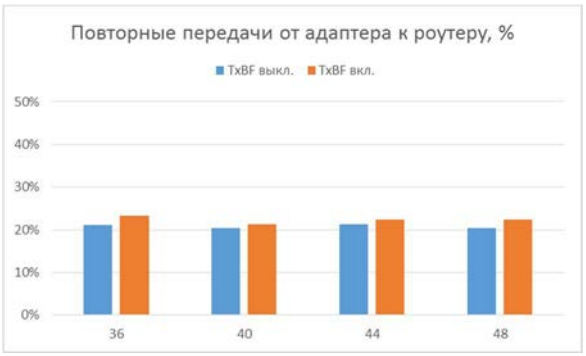
2x2:2, поэтому передача данных между ними возможна лишь в два пространственных потока. Таким образом, максимальная скорость передачи кадров данных оказывается ограничена 173,3 Мбит/с [6].



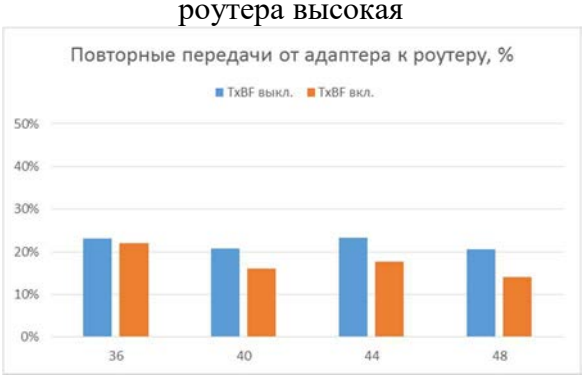
а) Мощность передатчика роутера низкая



б) Мощность передатчика роутера высокая

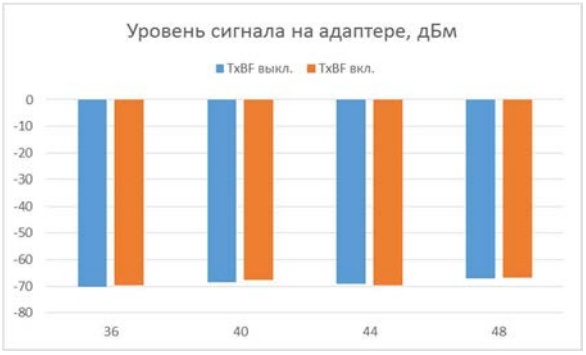


в) Мощность передатчика роутера низкая

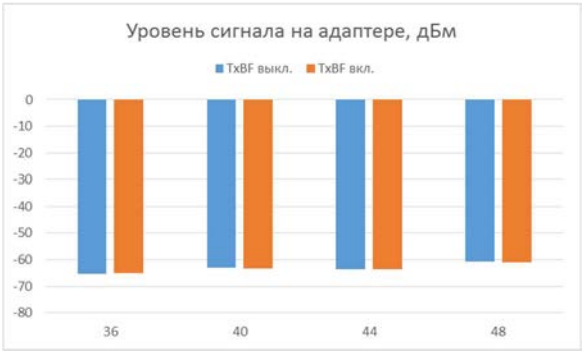


г) Мощность передатчика роутера высокая

Рис. 4. Коэффициент повторных передач кадров данных между роутером и адаптером



а) Мощность передатчика роутера низкая



б) Мощность передатчика роутера высокая

Рис. 5. Уровень принимаемого сигнала от роутера на стороне адаптера

Анализ полученных результатов показывает, что, вопреки ожиданиям, использование технологии явного формирования луча не привело ни к заметному повышению уровня принимаемого сигнала, ни к увеличению скорости передачи кадров данных. В ряде случаев наблюдалась даже обратная

ситуация. Эффективность данной технологии с другим оборудованием и в других условиях требует дальнейшего изучения.

Исследование выполнено в рамках выполнения ПНИ по государственному заданию СПбГУТ на 2022 год.

Список используемых источников

1. "IEEE Standard for Information Technology – Local and Metropolitan Area Networks – Specific Requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 5: Enhancements for Higher Throughput," in IEEE Std 802.11n-2009, doi: 10.1109/IEEESTD.2009.5307322.

2. "IEEE Standard for Information Technology – Telecommunications and Information Exchange between Systems - Local and Metropolitan Area Networks – Specific Requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications – Amendment 4: Enhancements for Very High Throughput for Operation in Bands below 6 GHz," in IEEE Std 802.11ac-2013, doi: 10.1109/IEEESTD.2013.7797535.

3. AC1350 MU-MIMO Wi-Fi гигабитный роутер. URL: https://www.tp-link.com/ru/home-networking/wifi-router/archer-a6/v2/ (дата обращения: 27.03.2022).

4. AC1900 двухдиапазонный Wi‑Fi USB‑адаптер высокого усиления. URL: https://www.tp-link.com/ru/home-networking/high-gain-adapter/archer-t9uh/v1/ (дата обращения: 27.03.2022).

5. ГУТ.Навигатор. URL: https://nav.sut.ru (дата обращения: 27.03.2022).

6. 802.11ac – VHT MCS, SNR, and RSSI. URL: https://d2cpnw0u24fjm4.cloudfront.net/wp-content/uploads/802.11ac-VHT-MCS-SNR-and-RSSI.pdf (дата обращения% 27.03.2022).

УДК 004.056.55
ГРНТИ 81.96

ЭКСПЕРИМЕНТАЛЬНОЕ ИССЛЕДОВАНИЕ ПРОТОКОЛА РАСПРЕДЕЛЕНИЯ КЛЮЧА ПО ПОСТОЯННЫМ КАНАЛАМ С ДОБАВЛЕНИЕМ ИСКУССТВЕННОГО ШУМА

М. Э. Ахметшина, Р. М.-А. Манкаев, В. А. Яковлев

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Проведено экспериментальное исследование протокола распределения ключа по постоянным бесшумным каналам, состоящего из числового протокола распределения бит сырого ключа и протокола преимущественного улучшения основного канала. Разработан комплекс программ, моделирующих формирование бит ключа у легальных

пользователей и нарушителя и позволяющих проводить статистический анализ распределения ошибок в символах ключевой последовательности. Результаты эксперимента хорошо согласуются с теоретическими расчетами.

протоколы распределения ключей, криптографические преобразования, S-блоки.

В [1, 2] предложен протокол формирования бит ключа между двумя пользователями, связанными каналом с постоянными параметрами (типа Интернет) на основе обмена между пользователями случайными действительными гауссовскими числами с добавлением искусственного шума – протокол ЧПРК. Суть этого протокола в следующем. Легальные пользователи А и В обмениваются между собой гауссовскими случайными величинами ($p + n_A$) и ($q + n_B$) соответственно, где p и q гауссовские случайные величины с параметрами (0,1), а n_A, n_B – гауссовские случайные величины с параметрами (0, ϭ). Далее производится вычисление бит «сырого» ключа пользователями А и В по формулам:

$$K_A = rec[p(g + n_B)], K_B = rec[q(p + n_A)]. \quad (1)$$

Нарушитель Е контролирует канал связи, наблюдая случайные величины ($p + n_A$) и ($q + n_B$), и получает бит «сырого» ключа в виде:

$$K_E = rec[(p + n_A)(g + n_B)], \quad (2)$$

где $rec[u]$ – операция квантования u на два уровня по знаку.

Затем выполняется протокол преимущественного улучшения основного канала (ПУОК).

Корреспондент А генерирует случайный бит $V = (0, 1)$. Этот бит V преобразуется в кодовое слово длиной s бит путем повторения бита V s раз. Корреспондент В декодирует принятый двоичный блок следующим образом:

– если все s бит в блоке одинаковые (нули или единицы), блок считается принятым;

– если блок содержит и нули, и единицы блок стирается, об этом сообщается корр. A по *каналу обсуждения,* и он стирает этот бит из буфера памяти.

Нарушитель E контролирует обмен информацией в отводном канале и канале обсуждения и, если корреспонденты стерли блок, он тоже его стирает, если они приняли блок, он его декодирует по мажоритарному правилу. Протокол ПУОК может быть выполнен несколько раз подряд.

В [1] были получены выражения для вероятности несовпадения бит ключа у корреспондентов А и В $P(K_A \neq K_B) = p_m$ и у нарушителя и корреспондента А $P(K_A \neq K_E) = p_e$ для числового протокола, а также аналогичные вероятности $p_{m\text{ПУОК}}$ и $p_{e\text{ПУОК}}$ для протокола ПУОК.

В данной работе приводятся результаты экспериментального исследования протоколов ЧПРК и ПУОК. Экспериментальные исследования были организованы следующим образом. Была разработана программа на языке Python генерации последовательностей случайных величин p, q, n_A, n_B, из которых в соответствии с соотношениями (1) и (2) формировались биты сырого ключа. Далее проводилось сравнение этих последовательностей, и вычислялись экспериментальные вероятности.

Объем сгенерированных последовательностей составлял $3 \cdot 10^5$ бит для протокола ЧПРК и $1{,}2 \cdot 10^7$ бит для протокола ПУОК. Для протокола ПУОК последовательно выполнялись 3 итерации, и на каждой итерации оценивались вероятности совпадения бит в последовательностях у A и B, а также в последовательностях у A и E.

В таблице 1 приведены аналитические и экспериментальные значения перечисленных вероятностей для трех итераций протокола ПУОК.

ТАБЛИЦА 1. Вероятности несовпадения бит ключевой последовательности разных значений шума σ^2

№ итерации ПУОК		$\sigma^2 = 0.1$		$\sigma^2 = 0.2$		$\sigma^2 = 0.5$		$\sigma^2 = 0.7$	
		p_m, $p_{m\text{ПУОК}}$	P_y, $p_{e\text{ПУОК}}$	p_m, $p_{m\text{ПУОК}}$	P_y, $p_{e\text{ПУОК}}$	p_m, $p_{m\text{ПУОК}}$	P_y, $p_{e\text{ПУОК}}$	p_m, $p_{m\text{ПУОК}}$	P_y, $p_{e\text{ПУОК}}$
0	теор.	0,198	0,098	0,2319	0,1338	0,3151	0,1959	0,3452	0,2218
	эксп.	0,1759	0,0975	0,2318	0,1338	0,3149	0,1959	0,3453	0,2218
1	теор.	0,0208	0,0014	0,0082	0,0057	0,0429	0,0035	0,0717	0,0066
	эксп.	0,0021	0,0014	0,0083	0,0058	0,0424	0,0299	0,0721	0,0508
2	теор.	0,0002	0,0029	0,0011	0,0112	4,03e-06	1,54e-10	3,56e-05	1,9e-09
	эксп.	2,1e-11	4,4e-12	5e-09	1,37e-05	6,89e-06	0,0002	4,54e-05	0,0008
3	теор.	2e-05	0,0184	1e-04	0,0611	2,63e-22	5,62e-40	1,6e-18	1,3e-35
	эксп.	2 e-43	4e-46	6e-34	3,5e-20	2,3e-21	3e-15	4,3 e-18	1,81e-05

Анализ таблицы показывает хорошее совпадение результатов расчета вероятностей ошибок по формулам, приведенным в [2], и в результате моделирования. Теоретические расчеты целесообразно использовать в тех случаях, когда вероятности ошибки малы, и в этом случае сложно получить статистические данные нужного объема. Наоборот, экспериментальные результаты проще получить при большом числе итераций, так как расчетные соотношения становятся громоздкими.

Расчеты и эксперимент показывают, что уже при 2-х итерациях вероятности p_m и p_e являются настолько малыми, что становится сложным применение процедуры «усиления секретности» [3]. В связи с этим для формирования ключа предлагается использовать дополнительный протокол,

названный протоколом ухудшения обоих каналов, однако при этом существенно уменьшается скорость формирования ключевой последовательности [2].

В нашем исследовании с этой целью предлагается использовать нелинейные преобразования на основе криптографических *S*-блоков [4]. Для исследования был выбран *S*-блок с четырьмя входами и четырьмя выходами, осуществляющий отображение вход-выход $a(x) \to b(x)$ таким образом, что выполняется условие $a(x)b(x) = 1(\mathrm{mod}\, f(x)$, где $f(x)$ – неприводимый многочлен четвертой степени над полем $GF(2)$.

Также были проверены различные сочетания протокола ПУОК и нелинейного преобразования с использованием *S*-блока. Результаты представлены в таблице 2, где для различных сочетаний протокола ПУОК и нелинейного преобразования использованы следующие обозначения: *sp* – последовательности бит сырого ключа у легальных пользователей и нарушителя преобразуются *s*-блоками, затем выполняется протокол ПУОК; $(sp)^2$ – преобразование *sp* повторяется два раза; $(sp)^i$ – преобразование *sp* повторяется *i* раз; $(sp)^i p$ – преобразование *sp* повторяется *i* раз, после еще раз применяется протокол ПУОК.

ТАБЛИЦА 2. Вероятности несовпадения бит ключевой последовательности у легальных пользователей и нарушителя разных значений дисперсии шума σ^2 для различных сочетаний протокол ПУОК и нелинейного преобразования

№ итерации ПУОК		$\sigma^2 = 0{,}1$		$\sigma^2 = 0{,}2$		$\sigma^2 = 0{,}5$		$\sigma^2 = 0{,}7$	
		p_m, $p_{m\text{ПУОК}}$	P_y, $p_{e\text{ПУОК}}$	p_m, $p_{m\text{ПУОК}}$	P_y, $p_{e\text{ПУОК}}$	p_m, $p_{m\text{ПУОК}}$	P_y, $p_{e\text{ПУОК}}$	p_m, $p_{m\text{ПУОК}}$	P_y, $p_{e\text{ПУОК}}$
0	ЧПРК	0,1759	0,0975	0,2318	0,1338	0,3149	0,1959	0,3453	0,2218
1	SP	0,1074	0,0814	0,1529	0,1288	0,235	0,2236	0,2691	0,2656
2	$(SP)^2$	0,0613	0,1047	0,09	0,1789	0,1576	0,3216	0,1853	0,3764
3	$(SP)^3$	0,0327	0,1965	0,0502	0,3106	0,0929	0,4526	0,1124	0,49
	$(SP)^3P$	3,9e-05	0,0178	0,0002	0,0572	0,001	0,1959	0,0036	0,2689
4	$(SP)^4$	0,0176	0,3517	0,0271	0,4548	0,0554	0,5134	0,0666	0,5
	$(SP)^4P$	1,22e-06	0,089	0,0002	0,2118	0,0005	0,4156	0,0004	0,4506
5	$(SP)^5$	0,0109	0,479	0,0113	0,5033	0,0258	0,4976	0,0192	0,523

Анализ таблицы показывает, что при всех значениях дисперсии дополнительного шума σ^2 увеличение количества итераций *SP* приводит к тому, что вероятность ошибки в битах ключевой последовательности у легальных пользователей становится значительно меньше, чем вероятность ошибки в ключевой последовательности нарушителя. На рис. для примера показано, как изменяются вероятности ошибок в ключевых последовательностях для

каждой итерации протокола $(SP)^3P$. Заметим, что применение дополнительной итерации протокола ПУОК, как показано на рис., может быть целесообразно для получения оптимального соотношения между вероятностями p_e и p_m, необходимого для проведения процедуры усиления секретности.

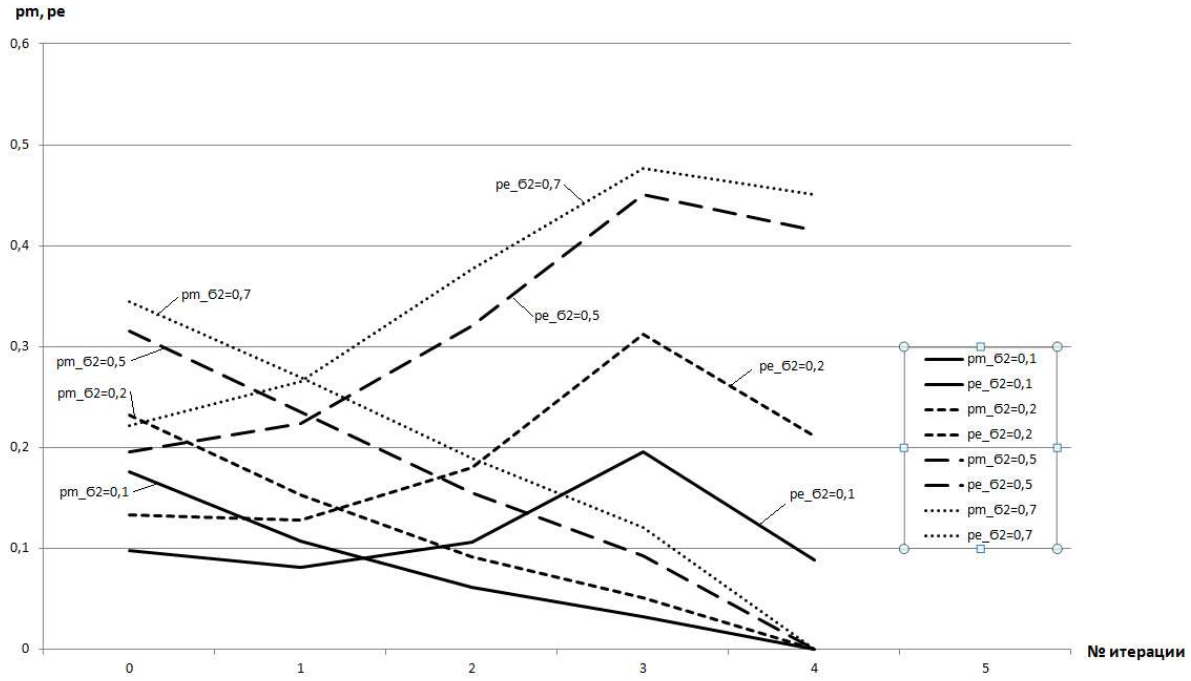


Рисунок. Вероятностей P_m и P_e для протокола $(SP)^3P$ после выполнения промежуточных итераций для различных значений дисперсии шума σ^2

В дальнейшем целесообразно проведение исследований по выбору оптимальной структуры *S*-блока и исследования более сложных сочетаний нелинейных блоков в итерациях протокола ПУОК.

Список используемых источников

1. Коржик В. И., Яковлев В. А. Вероятности ошибок при распределении ключей по бесшумным постоянным каналам с использованем добавления искусственного шума // Актуальные проблемы инфотелекоммуникаций в науке и образовании. X Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2021. Т. 1.С. 516–522.

2. Коржик В. И., Яковлев В. А. Протокол распределения ключей по постоянным каналам на основе совместного применения интерактивных протоколов обмена данным // Актуальные проблемы инфотелекоммуникаций в науке и образовании XI Международная научно-техническая и научно-методическая конференция : сб. науч. ст. СПб.: СПбГУТ, 2022. (в настоящем сборнике).

3. Starostin V., Korzhik V., Kabardov M., Gerasimovich A., Yakovlev V. and Morales-Luna G. Key Generation protocol executing through non-reciprocal fading channels // International Journal of Computer Science and Applications. 2019. Vol. 16. No. 1. pp. 1–16.

4. Коржик В. И., Яковлев В. А. Основы криптографии: учебное пособие. СПб. : ИЦ Интермедия, 2016. 296 с.

УДК 004.056
ГРНТИ 20.53.19

ВОЗМОЖНОСТИ ИСПОЛЬЗОВАНИЯ ЛИНГВИСТИЧЕСКОЙ СТЕГАНОГРАФИИ В ЗАВИСИМОСТИ ОТ ЖАНРА КОМПЬЮТЕРНЫХ ИГР

К. А. Ахрамеева, Е. Ю. Герлинг, И. А. Куликов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В данной статье рассматривается вопрос о возможностях использования лингвистической стеганографии и создания стеганографических систем с помощью лингвистической стеганографии на основе современных компьютерных игр и на основе игровых механик. Современные компьютерные игры делятся на множество различных жанров со своими особенностями, а также игровыми, кооперативными и коммуникативными механиками. В данной статье рассмотрены способы создания стеганографических систем в зависимости от игрового жанра и особенностей игровых механик определенных жанров компьютерных игр. Также в статье рассмотрены способы создания стеганографических систем на основе коммуникативных механик и способов внутриигрового взаимодействия между игроками.

стеганография, стеганография с учетом содержимого, стегоанализ, компьютерные игры.

Введение

Одной из наиболее важных задач для человечества была и остается защита информации. Для ее решения человек разработал много способов защиты, в том числе и стеганографию. Стеганографические системы позволяют вложить необходимое сообщение в некоторый объект, тем самым скрыв сам факт передачи сообщения.

Основной принцип создания стеганографических систем – скрытие информации в «шуме», чтобы она «затерялась» и не была обнаружена. И для такого рода вложений подходят компьютерные игры, которые в последнее время являются довольно распространенным видом развлечений. Для того, чтобы ориентироваться во всём многообразии игр, люди стали разделять игры на различные категории. И наибольшую популярность получил способ разделения на игровые жанры.

Лингвистическая стеганография

Методы лингвистической стеганографии позволяют осуществлять передачу скрытого сообщения с помощью внедрения этого сообщения в некоторый

неприметный текст, который и является покрывающим объектом и сам по себе не содержит «полезной» (имеется в виду – никак не связан с информацией во внедряемом сообщении) для получателя информации. При этом покрывающий объект считается неприметным, если он не вызывает подозрений и выглядит естественно.

Классификация

Основным критерием деления жанров являются действия, наиболее часто совершаемые игроком (рис.). При этом положение камеры (вид из глаз, вид сзади, вид сверху, вид из кабины), движение времени (реальное время или пошаговый режим), количество игроков и прочие факторы и особенности – не являются критериями для жанров, они лишь определяют способ подачи геймплея.

Игры делятся на три большие группы: игры действия, игры информации, игры контроля [1].

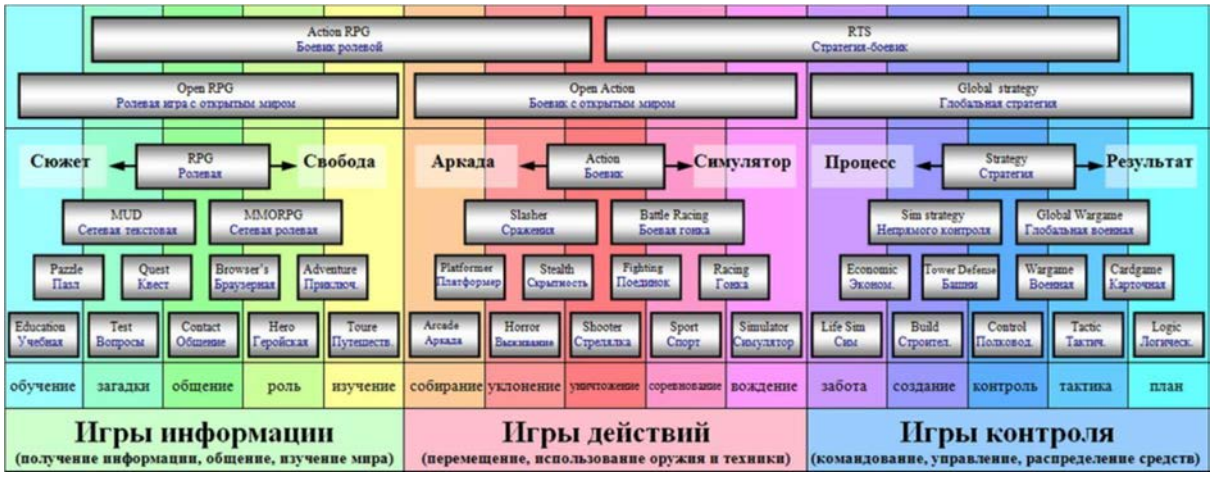


Рисунок. Схема классификации игровых жанров

Выделены 15 основных геймплейных элементов из которых состоит вообще любая игра (в схеме – предпоследняя строчка снизу: обучение, загадки, общение, роль, изучение, собирание, уклонение, уничтожение, соревнование, техника, забота, развитие, контроль, тактика, план) [2].

Возможности создания стеганографических систем

Стоит рассмотреть возможности создания стеганографических систем в контексте основных геймплейных элементов каждой выделенной группы жанров.

Игры информации

1. Обучение

Главное действие – получение новой информации, а точнее – обучение. Самые простейшие из них — изучение цифр, алфавита, названий вещей. Возможно применение семаграмм, жаргонов, решеточных и нулевых шифров.

2. Общение

Главное действие – взаимодействие нескольких субъектов между собой с наличием обратной связи. Это различные новеллы, симуляторы свиданий, может встречаться в квестах, больших ролевых играх. Существует необычная игра на двух игроков «Keep Talking and Nobody Explode», где один пытается разминировать бомбу, а второй читает инструкцию и голосом объясняет саперу, как это нужно сделать. В игре содержится огромное количество модулей для разминирования, с помощью которых игроки в редакторе могут создавать свои сценарии для прохождения другими игроками. Следовательно, игра обладает кооперативной механикой, на основе которой можно построить лингвистическую стегосистему с применением семаграмм и жаргонов.

3. Изучение

Главное действие – изучение окружающего мира. Игровой мир может быть большим, поэтому вероятность случайного извлечения становится ниже, а знающий человек может спокойно извлекать необходимую информацию, выполняя, на первый взгляд, рядовые игровые действия. Покрывающим объектом в данном случае может выступать как текст, найденный игроком, так и объекты, несущие в себе какую-либо текстовую информацию – игровые записки, камни с символами и так далее. Возможно применение семаграмм и решеточных шифров.

Игры действий

Собирание

Главная задача - собрать все особые объекты на уровне. Довольно часто игры бывают бесконечны, а целью игры является набор наибольшего количества очков. В играх этой группы можно вкладывать информацию в разнообразие игровых предметов. Возможно применение семаграмм.

Игры контроля

Создание

Главное действие – распределение доступных ресурсов для развития. В подчинении игрока находятся ресурсы (деньги, стройматериалы, строители, свободная для застройки земля), их нужно с умом использовать для развития (обычно, постройка города). Такие игры еще называют «песочницами» (“*Sandbox*”). Данный жанр обладает большим количеством возможностей создания лингвистических систем. Почти все игры этого жанра имеют конструктор, который позволяет менять окружающий мир, а онлайн-игры этого жанра позволяют делиться игрокам собственными построенными мирами в сети Интернет [4]. Таким образом получается целая система передачи стеговложений. На примере игры “Minecraft” – игрок создал игровую карту с городом, в котором по определенным координатам спрятал сундук с письмом или разместил табличку с важной информацией. Игрок выложил эту карту в свободный доступ. Другие игроки могут играть на этой карте и модифицировать ее, а знающий человек может провести извлечение информации, так как местоположение сундука или таблички с текстом ему было известно заранее. При создании

стегосистем возможно применение семмаграмм, жаргонов, нулевых и решеточных шифров.

Сравнение возможностей создания стеганографических систем

Наименее подходящими для построения стеганографических систем являются жанры группы «Игры действий». Игры данного жанра, в первую очередь, направлены на быстрое совершение манипуляций с игровыми объектами, а не работу со статичной информацией.

Игры группы жанров «Игры информации» прямо нацелены на работу с информацией и в таких играх зачастую присутствуют коммуникативные механики, которые позволяют игрокам обмениваться игровой информацией в онлайн-режиме.

«Игры контроля» и, в особенности, жанр «Строительство» обладают большим потенциалом и наибольшей эффективностью создания стеганографических систем. В таких играх нет необходимости что-то менять и дополнять, чтобы создать новую стегостистему взамен старой, так как внутриигровой конструктор чаще всего содержит все необходимое для удобного редактирования игрового уровня. При этом многие игры этого жанра предлагают игрокам возможность обмена своими творениями по сети, что упрощает передачу стеговложений.

Заключение

Современные игры делятся на огромное количество жанров, каждый из которых обладает своими уникальными чертами и особенностями. При этом не только каждый жанр, но и группы жанров отличаются по способам и эффективности создания стеганографических систем.

Список используемых источников

1. Киризлеев А. А. Жанры компьютерных игр (общая схема) [Электронный ресурс]. URL: https://gamesisart.ru/TableJanr.html, свободный.

2. Ахрамеева К. А., Герлинг Е. Ю., Куликов И. А. Обзор жанров компьютерных игр для создания стеганографических систем // Актуальные проблемы инфотелекоммуникаций в науке и образовании. X Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2021.

3. Коржик В. И., Небаева К. А., Герлинг Е. Ю., Догиль П. С., Федянин И. А. Цифровая стеганография и цифровые водяные знаки / Под общей редакцией профессора В. И. Коржика. Ч. 1. Цифровая стеганография. – СПб. : СПбГУТ, 2016. – 226 с. ISBN 978-5-89160-125-3.

4. Воробьев Д. Б., Шабалкин Л. Э., Музыкантов М. А. Симуляторы строительства и управления. История развития и особенности жанра // Молодой исследователь Дона [Электронный ресурс]. URL: https://cyberleninka.ru/article/n/simulyatory-stroitelstva-i-upravleniya-istoriya-razvitiya-i-osobennosti-zhanra, свободный

Статья докладывалась на Юбилейной X Международной научно-технической и научно-методической конференции «Актуальные проблемы инфотелекоммуникаций в науке и образовании» (АПИНО-2021).

УДК 004.056
ГРНТИ 20.53.01

РЕАЛИЗАЦИЯ АВТОСБОРКИ HONEYPOT НА ОС СЕМЕЙСТВА LINUX ПРИ ПОМОЩИ ПО VAGRANT

К. А. Ахрамеева, С. А. Кузнецов, И. А. Куликов, А. А. Фоминых

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В данной статье рассматривается проблемный вопрос реализации автосборки технологии honeypot на операционных системах семейства Linux при помощи программного обеспечения Vagrant. Существующие готовые сборки образов часто построены на устаревших версиях ОС и, в сущности, пригодны лишь для образовательных целей. В данной статье рассмотрена установка honeypot на современные операционные системы семейства Linux и адаптация пакета безопасности PenTBox для обеспечения его стабильной работы на новейших ОС. Также в статье рассмотрена возможность автоматической установки на «пустую» ОС необходимых пакетов безопасности и автосборки ОС с использованием ПО Vagrant для создания готового образа ОС с предустановленным honeypot.

honeypot, vagrant, linux, pentbox.

Введение

В настоящее время остро стоит вопрос борьбы с угрозами информационной безопасности (далее – УБИ). Для борьбы с киберугрозами разрабатываются новые средства защиты информации (далее – СрЗИ), которые помогают компаниям защищаться от кибератак. Для отслеживания атаки и поимки преступника необходимы различные средства, которые будут предупреждать и отслеживать действия злоумышленника в системе. Также все еще используются устаревшие операционные системы (далее – ОС), на которых функционируют СрЗИ и сервисы компаний. Использование такого рода ОС позволяет злоумышленнику эксплуатировать известные уязвимости, которые не были устранены из-за окончания поддержки данных ОС и выпуском производителем обновлений безопасности [1]. Существует множество эффективных СрЗИ, которые были разработаны для устаревших версий ОС, но которые являются актуальными и в настоящее время. С авторской точки зрения, востребованным в данном вопросе должно стать решение задачи использования существующих СрЗИ на новейших ОС, при этом имея такую же стабильность и эффективность.

Реализация honeypot на новейших ОС

Honeypot представляет собой ресурс, который без какого-либо воздействия на него ничего не делает. *Honeypot* собирает небольшое количество информации, после анализа которой строится статистика методов, которыми пользуются взломщики, а также определяется наличие каких-либо новых решений, которые впоследствии будут применяться в борьбе с ними [2]. В данной работе был использован *honeypot*, который входит в пакет безопасности *PenTBox*.

Развертывание Vagrant

Начало работы с данным проектом началось с установки на ОС *Linux* версии 20 программного обеспечения (далее – ПО) *Vagrant*.

Vargant это свободное и открытое программное обеспечение для создания и конфигурирования виртуальной среды разработки. Является обёрткой для ПО виртуализации, например *VirtualBox*. Также необходимо было установить среду виртуализации. В данной работе была использована среда *Virtual Box*. В основной ОС необходимо было создать директорию, из которой будет происходить сборка. В созданную директорию необходимо клонировать файлы для работы проекта. Список файлов необходимых для работы проекта представлен на рис. 1.

Рис. 1. Список файлов для работы проекта

Основными файлами для работы являются:

- «*Vagrantfile*», в котором представлена конфигурация операционных систем для автоматической сборки;
- Директория «*configs*», в которой представлены исполняемые скрипт файлы для загрузки таких ОС как:
- *Ubuntu* 20;
- *Centos* 7;
- Fedora 34;

- *Centos Stream* 8.

В «*Vagrantfile»* содержатся конфигурационные параметры виртуальных машин (далее – ВМ). Пример конфигурации ВМ «*centos-honey*» представлен на рис. 2.

```
  config.vm.define "centos7" do |box|
  box.vm.box = "centos/7"
  box.vm.hostname = "centos-honeypot"
  box.vm.box_check_update = false
  box.vm.define "centos-honey"

  box.vm.provider "virtualbox" do |vb|
  vb.name = "centos-honeypot"
  #   vb.memory = "1024"
  #   # Display the VirtualBox GUI when booting the machine
  #   vb.gui = true
  #
  #   # Customize the amount of memory on the VM:
  end

  box.vm.provision "shell", path: "./configs/setup_centos.sh"
end
```

Рис. 2. Пример конфигурации ВМ «*centos-honey*»

В директории «configs» находится исполняемые скрипт файлы для установки ОС. Пример скрипта для настройки ОС *Centos* 7 и установки пакета безопасности *PenTBox* представлен на рис. 3.

```
set -e

sudo yum -y install git
sudo yum -y install ruby

git clone https://github.com/technicaldada/pentbox

cd pentbox

tar -zxvf pentbox.tar.gz

cd ..

echo "cd pentbox/pentbox-1.8 && sudo ruby pentbox.rb" >> pentbox_start.sh

chmod +x pentbox_start.sh
```

Рис. 3. Скрипт для настройки ОС *Centos* 7 и установки пакета безопасности *PenTBox*

Для запуска автосборки ОС с предустановленным Honeypot необходимо в созданной директории запустить ВМ. Для работы с ВМ на базе ПО Vagrant были выделены следующие команды:

- *vagrant up* – запуск и конфигурация всех ВМ. Так как в данной работе рассматривались 4 ОС, то после ввода данной команды запустятся все 4 ВМ с предустановленным honeypot;
- *vagrant up "name"* – запуск и конфигурация конкретной ВМ.

После успешного запуска ВМ можно выполнять следующие команды:

- *vagrant ssh "name"* – подключение к конкретной ВМ;
- *vagrant status* – вывод состояния всех ВМ;
- *vagrant destroy "name"* – удаление конкретной ВМ;
- *vagrant halt "name"* – остановка конкретной ВМ.

После подключения к ВМ с honeypot необходимо запустить пакет безопасности *PenTBox*. Для запуска используется команда *pentbox_start.sh/pentbox_launch.sh.*

После запуска пакета безопасности откроется интерфейс *PenTBox*, представленный на рис. 4.

Рис. 4. Интерфейс *PenTBox*

Необходимо запустить ловушку и сконфигурировать её параметры. Конфигурация происходит через консоль ОС. После конфигурации *honeypot*

становится активным и ожидает ввода действий злоумышленника. На рис. 5 представлен пример успешного перехвата команды *http*-запроса *get*: «*culr localhost*:80».

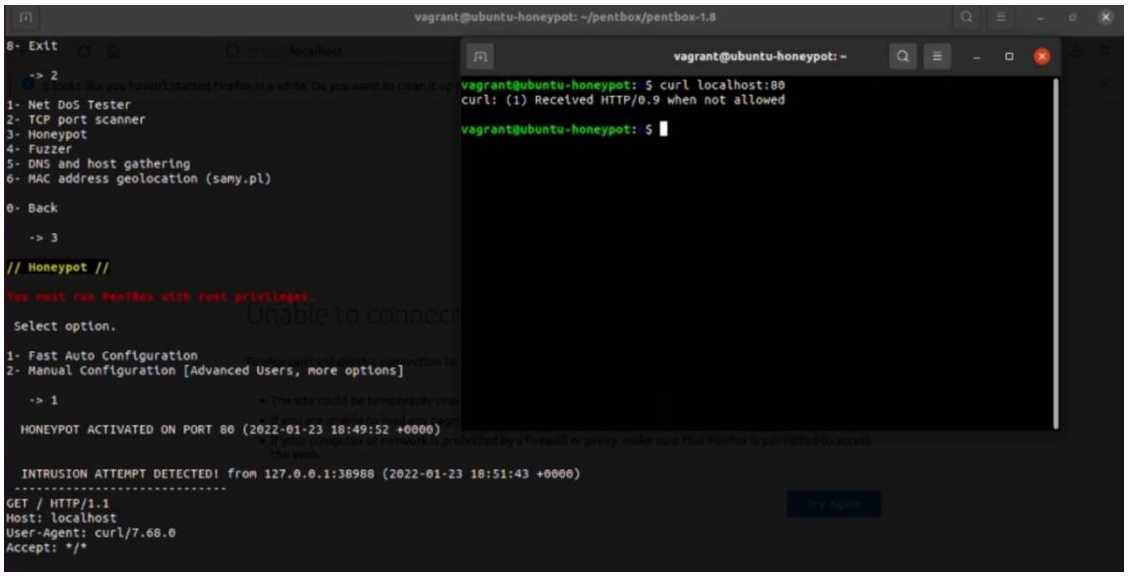


Рис. 5. Пример успешного перехвата команды *http*-запроса *get*: «*culr localhost*:80»

Список используемых источников

1. Красов А. В., Петрив Р. Б., Сахаров Д. В., Сторожук Н. Л., Ушаков И. А. Масштабируемое *HONEYPOT*-решение для обеспечения безопасности в корпоративных сетях // Труды учебных заведений связи. 2019. Т. 5. № 3. С. 86-97.

2. *Honeypot*: [Электронный ресурс] // Википедия. URL: *https://ru.wikipedia.org/wiki/Honeypot*. (дата обращения: 10.02.2022).

УДК 681.7
ГРНТИ 49.44.31

АНАЛИЗ МЕТОДОВ И СРЕДСТВА ПОВЫШЕНИЯ ПОМЕХОУСТОЙЧИВОСТИ ВОЛОКОННО-ОПТИЧЕСКИХ СИСТЕМ ПЕРЕДАЧИ НА БАЗЕ СПЕКТРАЛЬНЫХ ТЕХНОЛОГИЙ

А. Б. Бабаев[2], Э. М. Джафарова[1], Б. Г. Ибрагимов[1], С. Р. Исмайлова[1]

[1]Азербайджанский Технический Университет

[2]Бакинский инженерный университет

Проанализированы методы и средства повышения достоверности передачи оптических сигналов в волоконно-оптических системах передачи (ВОСП) с использованием

спектральных технологий WDM (Wavelength Division Multiplexing) и DWDM (Dense WDM) в мультисервисных телекоммуникационных сетях. На основе исследования предложен новый подход к построению методов расчета показателей помехоустойчивости приема потоков оптических сигналов, функционирующих в условиях воздействия непреднамеренных источников помех. Получены важные аналитические выражения, оценивающие характеристики помехоустойчивости приема оптических сигналов с учетом передаточных характеристик.

помехоустойчивость, вероятность битовой ошибки, WDM непреднамеренные помехи, отношения сигнал/помехи, DWDM, оптический сигнал, ВОСП.

Проблема повышения помехоустойчивости и эффективного использования оптических каналов потенциальной связи, средств волоконно-оптических систем передачи мультисервисных телекоммуникационных сетей для совместной передачи информационных потоков, при преобразовании, объединении и мультиплексировании мультимедийного трафика – речи, данных и видео трафика представляет, несомненно, большой интерес в системах связи [1–3].

Проведенные исследования и анализ показывают [1–5], что совместная передача мультимедийного трафика по волоконно-оптической линий связи (ВОЛС) требует, естественно, преобразования последней в цифровую форму.

Однако, совместная передача по оптическому каналу связи потоков речевых, видео и данных с помощью оптических абонентских и сетевых терминалов, модемов, шлюза, интерфейса ввода и вывода, мультиплексоров и демультиплексоров всегда сопровождается большими ошибками. Эти последствия оказывают существенное влияние на потенциальную помехоустойчивость функционирования волоконно-оптических систем передачи (ВОСП) на базе спектральных технологий таких как, WDM (*Wavelength Division Multiplexing)*, SONET (*Synchronous Optical Network*), SDH *(Synchronous Digital Hierarchy*), CWDM (*Coarse Wavelength Division Multiplexing*) и DWDM (*Dense WDM*) с длиной оптических волн $\lambda_i = 1.31,...,1.55$ *mkm* .

Следует отметить, что внедрение оптических спектральных технологий WDM, CWDM, DWDM и HDWDM *(Higher DWDM)* в ВОСП позволяет на несколько порядков увеличить число спектральных каналов и скорость передачи в каждом канале связи, что противоречит задаче повышения достоверности функционирования системы передачи потоков оптических сигналов.

Поэтому задача исследования показателей достоверности функционирования оптических телекоммуникационных систем таких как, помехоустойчивость ВОСП на базе перспективных оптических спектральных технологий с учетом вероятности битовых ошибок $P_{BER}(\lambda_i)$, битовых

скоростных характеристик $V_b(\lambda_i)$ и оптических средств ВОЛС, которые состоят из приемных оптических модулей (ПРОМ), волоконно-оптических кабелей (*ВОК)* и передающих оптических модулей (ПОМ) при оказании мультимедийных услуг является наиболее актуальной.

Теоретически вопросы потенциальной помехоустойчивости приема потоков цифровой информации хорошо изучены [2, 3, 5], но бурное развитие мультисервисных ВОСП с применением спектральных технологии WDM, DWDM и средств DSP *(Digital Signal Processing)* стимулирует дальнейшее их исследование и анализ показателей их достоверности. Установлено в работе [2–8], что при увеличении битовой скорости передачи данных по спектральному каналу связи все большую роль на качество их приема оказывает межсимвольная интерференция, которая приводит к ухудшению качества связи ВОСП.

Использование нескольких длин волны в ВОСП на базе спектральных технологии WDM и DWDM, является по сути общим подходом для увеличения пропускной способности ВОЛС. Преимущество этого подхода состоит в том, что модули компенсации дисперсии ВОК и оптические усилители являются общими для всех спектральных оптических каналов.

В работах [2–5, 8] проанализированы методы улучшения качества функционирования волоконно-оптических систем передачи на базе WDM&DWDM и CWDM технологий, определены передаточные характеристики волоконно-оптических линий связи с использованием ПРОМ, ВОК и ПОМ.

В данной работе рассматривается анализа показателей качества связи и помехоустойчивости ВОСП на базе ВОЛС, использующих эффективные технологии спектрального разделения оптического канала WDM и DWDM.

Создание помехоустойчивых ВОСП с повышенной пропускной способностью, работающих по цифровым оптическим каналам связи с внедрением спектральных технологий, будет способствовать повышению достоверности приема $D_{\text{ф}}(\lambda_i)$ цифровой информации. В современных ВОСП с использованием спектральных технологий в основном определяется достоверность передачи цифровых оптических сигналов и вероятность битовой ошибки при заданной помехе $N_n(t)$, которые в виде целевых функций описываются следующим образом:

$$Z(\lambda_i) = W[D_{\Phi}(\lambda_i), P_{BER}(\lambda_i)] \to \max(\min) \tag{1}$$

при следующих ограничениях

$$V_b(\lambda_i) \geq V_{b.доп.}(\lambda_i),\ \alpha_{кз}(\lambda_i, L_{\max}) \leq \alpha_{кз.доп.}(\lambda_i, L_{ma}), \tag{2}$$

$$OSNR(\lambda_i) \geq OSNR_{\text{доп.}}(\lambda_i), C_{\text{ап.}}(\lambda_i) \leq C_{\text{ап.дп.д}}(\lambda_i), \quad (3)$$

где $V_b(\lambda_i)$ – битовая скорость передачи оптических сигналов по ВОЛС; $L_{\max}$ – максимальная длина между операционных усилителей; $\alpha_{кз}(\lambda_i, L_{\max})$ – коэффициент затухания ВОЛС с учетом максимальной длины $L_{\max}$ между оптическими усилителями; $C_{ап}(\lambda_i)$ – стоимость линий передачи оптических сигналов и программно-аппаратных средств ВОЛС с использованием ПРОМ, ВОК и ПОМ; $SNR(E_b, \lambda_i, N_0)$ – отношение оптического сигнал-шума $OSNR$ (*Optical Siqnal to Noise Rate*) на входе приемника с учетом энергии битового сигнала E_b и спектральная плотность мощности шума N_0, которые характеризуют комплексные показатели качества связи при использовании длины волны λ_i, $i = \overline{1,n}$.

Выражения (1), (2) и (3) описывают сущность рассматриваемого нового подхода с учетом комплексных показателей ВОСП, на основе которого предлагается метод расчета помехоустойчивости приема оптических сигналов. Кроме того, выражения (1), (2) и (3) определяют возможности метода расчета показателей помехоустойчивости ВОСП с учетом передаточных характеристик ВОЛС на базе спектральных технологий и являются простой аналитической записью функции достоверности ВОСП при оценке их качества функционирования.

С целью выполнения целевой функции (1) для помехоустойчивости функцинирования ВОСП и их заданные ограничения (2) и (3) необходимо исследовать:

– методы приема оптических сигналов мультимедийного трафика;

– способы реализации оптических сигнально-кодовых конструкций;

– методы повышения отношения оптического сигнал-шума $SNR(E_b, \lambda_i, N_0)$ на входе приемника;

– эффективные алгоритмы декодирования с исправлением ошибок и схемные решения приемных оптических модулей.

Проведенный анализ показал [1–4], что улучшения помехоустойчивости функционирования современных цифровых оптических локальных и транспортных кольцевых сетей на базе ВОСП определяется интегральной характеристикой – ВОЛС, передающего и приемного оптоэлектронного модуля оптических каналов связи с внедрением технологии WDM и DWDM.

Под улучшением помехоустойчивости функционирования ВОСП с внедрением новейших технологий WDM и DWDM будем понимать процедуры, в ходе которых при заданной структуре оптической сети определяется эффективность использования системы $E_{эи}(\lambda_i)$ и достоверность передачи оптических сигналов $D_n(\lambda_i)$ при минимальной суммарной стоимости $C_{ап}(\lambda_i)$. Заданной считается кольцевая структура ВОЛС в локальных

и транспортных сетях передачи данных SDH/WDM/DWDM, которая описывается следующим графом:

$$E = [T_k, N_k],\ \dot{O}_{\grave{e}} = \{1,2,..., N\},\ N_k = \{N_{i,j}\},\ i, j = 1,2,..., n, \quad (4)$$

где T_k – множество вершин, отображающих узлы ВОСП, какими являются оптические устройства ВОЛС; N_k – множество ребер, соответствующих межузловым оптическим линиям связи, составляющие спектральные КС.

Согласно предложенному подходу и ориентированному графу (4) улучшение помехоустойчивости функционирования ВОСП на базе волоконно-оптических сетей связи учитывает алгоритм работы ВОЛС, достоверность приема, управление передачей и коммутацией цифровых оптических сигналов.

На основе исследования установлено [2, 3, 4, 9], что для проведения инженерных расчетов необходимо изучить следующие важные и интегральные параметры ВОЛС:

– средняя мощность P_{cp} передаваемого оптического сигнала ПОМ;

– внутрисистемная помеха N_{bp} и $N_{bp} = [P_c,\ \Delta F, N_a]$, где ΔF – полосы пропускания оптического приемника; N_a – число активного оптического терминала и мультиплексированного канала связи;

– предельное отношение сигнал-шум $SNR(E_b, \lambda_i, N_0)$ на входе ПРОМ;

– спектральная плотность аддитивного белого гауссовского шума N_0

– $V_b(\lambda_i)$ – битовая скорость передачи оптических сигналов по спектральному каналу связи;

Вышеперечисленные интегральные параметры ВОЛС, способствуют эффективному выбору более точной величины среднего значения порога $\Pi_{ср}(\lambda_i)$ из условия минимума P_{BER} приема оптического сигнала при заданной вероятности ложной тревоги $P(u_1 / u_0)$, характеристики передаваемого сигнала и спектрального канала связи, которые находятся выражением [3]:

$$\Pi_{ср}(\lambda_i) = 0.25[N_0 + N_{bp}] \cdot \{F_L^{-1}[1 - P(u_1 / u_0)] \cdot V_b(\lambda_i), \quad (5)$$

где F_L^{-1} – обратное функции Лапласа.

Допустим, оптические сигналы, поступающие на вход приемника терминала блока принятия решения с таймером имеют прямоугольную форму посылки при $P(u_0) = P(u_1) = 0{,}5$ и среднее напряжение оптического сигнала выполняет следующие условия

$$u_c \geq 2u_{ø}, \quad U(\lambda_i, t, b_i) = u_c[u_1, u_0], \quad (6)$$

где u_1, u_0 – амплитуды сигналов высокого «1» и низкого «0» уровня оптического сигнала.

Для принятия решения в блоке принятия решения с таймером использован метод оптимального когерентного приема оптических сигналов на базе теории статистических решений [3–5], с учетом априорной информации $f(\mathrm{s_i})$ и статистики случайных сигналов $U(\lambda_i, t, b_i)$, согласно которому формируется алгоритм различения отношения функций максимального правдоподобия и сравнения его с средним порогом:

$$\Lambda_{1,0}(\lambda_i) = \frac{f(s/1)}{f(s/0)} \begin{matrix} > u_1 \\ < u_0 \end{matrix} \Pi_{\text{ср}}(\lambda_i), \tag{7}$$

Из (7) следует, что в ПРОМ ошибка может возникнуть в том случае, когда шумы и помехи (флуктационные, дробовые, межсимвольные и переходные) окажутся выше первого $\Pi_1(\lambda_i)$ и второго $\Pi_0(\lambda_i)$ порога.

Одной из основных задач математической теории связи является определение наиболее существенных характеристик системы передачи информации [3, 4, 5, 6]. Одним из важных количественных показателей оптической системы является вероятность ошибочного приема в различных каналах связи.

С учетом (5), вероятность битовой ошибки приема, характеризующей достоверность передачи оптических сигналов ВОЛС примет следующий вид [7, 8]:

$$P_{BER}[\Pi_{ср}(\lambda_i)] = \frac{4\sigma_{\text{ш}}}{5u_{c\max}} \cdot \exp\left[-0{,}5\frac{Q_0(\lambda_i)}{u_{\text{ш}}} \cdot \Pi_{\text{ср}}(\lambda_i)\right], \tag{8}$$

где $\sigma_{\text{ш}}$ – среднеквадратическое отклонение напряжения шума $u_{\text{ш}}$ на входе приемника оптического ПРОМ; $Q_0(\lambda_i)$ – коэффициент ошибок ВОЛС.

Из выражения (8) видно, что введение приемника блока принятия решения с таймером и эффективный выбор параметров $\sigma_{\text{ш}}$, $Q_0(\lambda_i)$ и $\Pi_{\text{ср}}(\lambda_i)$, весьма существенно минимизирует P_{BER} оптического ПРОМ волоконно-оптических линий связи. Здесь, величина среднего значения порога учитывает при приеме порогового уровня двоичного 0 и 1 оптического сигнала, соответственно $\Pi_0(\lambda_i)$ и $\Pi_1(\lambda_i)$.

Таким образом, комплексное исследование интегральных характеристик ВОЛС открывает новые возможности для повышения помехоустойчивости ВОСП на базе спектральных WDW и DWDM технологии, которые

позволяют их использование в высокоскоростных оптических транспортных сетях нового поколения – NGN&FN мультисервисных телекоммуникационных сетях.

Список используемых источников

1. Гордиенко В. Н., Крухмалев В. В., Моченов А. Д., Шарафутдинов Р. М. Оптические телекоммуникационные системы. М. : Горячая линия – Телеком, 2011. 368 с.

2. Ибрагимов Б. Г., Исмайлова С. Р., Джафарова Э. М. Исследование производительности линий волоконно-оптических систем передачи на базе WDM и DWDM технологий // Актуальные проблемы инфотелекоммуникаций в науке и образовании. X Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2021. Т. 1. С.406–410.

3. Зюко А. Г., Кловский Д. Д., Коржик В. И., Назаров М. В. Теория электрической связи: учебник для вузов / под ред. Д. Д. Кловского. М.: Радио и связь, 1998. 432 с.

4. Ibrahimov B. G., Orujov A. O., Hasanov A. H., Tahirova K. M. (2021) Research and analysis efficiency fiber optical communication lines using quantum technology // *T-Comm*, vol. 15, no.10. pp. 50–54. (*in Russian*).

5. Скляр Б. Цифровая связь. Теоретические основы и практическое применение: пер. с англ. М.: Вильямс, 2003. 1104 с.

6. Ibrahimov B. G., Hasanov M. H. Research and analysis of indicators optical telecommunication networks based on PON, WDM and DWDM technology // 2020 International Conference «Engineering Management of Communication and Technology» IEEE Conference Record #49634, Vienna, Austria - Springer Schloessl. October 20–22, 2020. pp. 1–4.

7. Ибрагимов Б. Г., Джафарова Э.М. Показатели волоконно-оптических систем передачи с использованием перспективных технологий // Технологии Информационного Общества. XIV Международный отраслевой научно-технической конференции: сб. тр. Москва: ИД Медиа Паблишер, 2020. Т. 1. С. 43–44.

8. Листвин В. Н., Трещиков В. Н. DWDM – системы. Москва.: Техносфера, 2015. 256 с.

9. Gringeri S., Bitar N., and Xia T. J.. Extending software defined network principles to include optical transport // IEEE Communications Magazine, March, 2013. pp. 32–40.

УДК 004.056
ГРНТИ 19.31

ОПРЕДЕЛЕНИЕ ПОКАЗАТЕЛЕЙ ЭФФЕКТИВНОСТИ СИСТЕМ МОНИТОРИНГА И КОРРЕЛЯЦИИ СОБЫТИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

И. Н. Бабков, Н. И. Казаков, П. В. Карельский, А. А. Миняев

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Управление событиями информационной безопасности (ИБ), от анализа атак и угроз до выбора соответствующих контрмер, стало серьезной проблемой для специалистов по ИБ и ИТ-администраторов. Для своевременного устранения данной проблемы и минимизации наступления рисков ИБ многие компании создают центры мониторинга и управления информационной безопасностью. Одним из важнейших компонентов таких центров являются системы мониторинга и корреляции событий ИБ (SIEM), которые позволяют агрегировать события и выявлять из них инциденты ИБ. В статье определяются показатели эффективности SIEM систем.

security operations center, SIEM, информационная безопасность, инцидент ИБ.

В настоящее время для обеспечения бесперебойного функционирования компании, необходим эффективный контроль и своевременное реагирование на возникающие угрозы, и инциденты ИБ.

Для выполнения данных функций многие компании создают центры мониторинга и управления информационной безопасностью (security operation center, SOC) [1, 2]. Такие центры в совокупности включают технологии, процессы и персонал (аудит, сбор, фильтрация, корреляция событий; выявление инцидентов; формирование отчетов по событиям и т. д.).

Одним из важнейших инструментов SOC являются системы мониторинга и корреляции событий информационной безопасности (SIEM-системы) [3], которые позволяют собирать данные при помощи серверов, сетевых средств защиты информации (ССЗИ), средств криптографической защиты информации (СКЗИ) и т. п., предварительно обрабатывать, хранить и анализировать данные. Функциональная модель системы SIEM представлена на рис. 1.

На существующем в текущий момент рынке, присутствует множество SIEM систем от различных производителей, включая как отечественные, так и зарубежные компании. На рис. 2 представлен мировой рынок SIEM по версии Gartner от 04.2021 года [4]. Из основных необходимо отметить следующие программные продукты: RuSIEM, MaxPatrol SIEM, Micro Focus (HP) ArcSight, IBM Qradar, McAfee ESM, RSA NetWitness, Splunk.

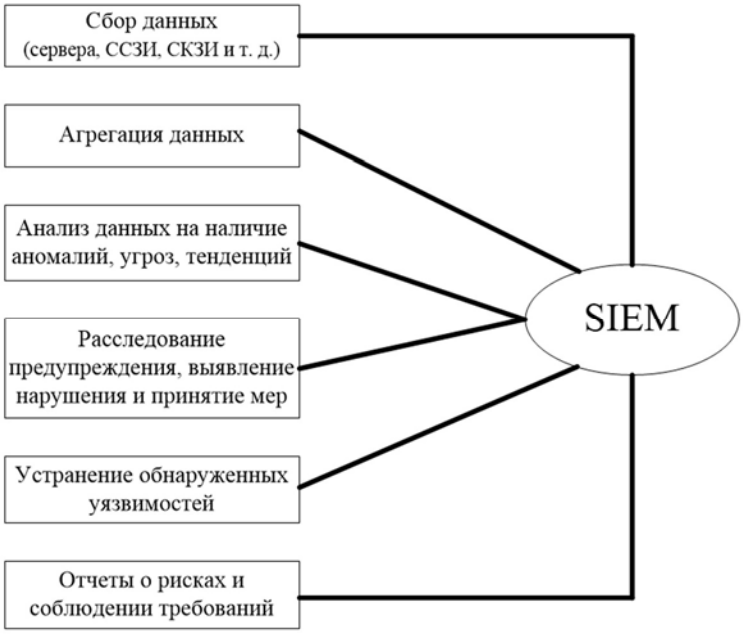


Рис. 1. Функциональная модель системы SIEM

Рис. 2. Мировой рынок SIEM по версии Gartner

Представленные системы имеют как множество плюсов, так и ряд недостатков. Главной целью любой сферы применения таких программных продуктов является выбор наиболее функционального и в то же время соответствующего по цене решения [5].

Для того чтобы центр мониторинга и управления информационной безопасностью работал максимально оперативно и продуктивно, необходимо задать метрики и оценивать по показателям работы SIEM системы.

По результатам изучения и анализа функционирования различных SIEM систем были определены следующие показатели их эффективности.

1) Выделение ложных срабатываний.

- Уровень точности определения инцидента. Из потока событий ИБ надо выбрать «действительно» инцидент, который может привести к рискам ИБ, %.
- Коэффициент принятия решения. Отношение количества всех инцидентов к устраненным инцидентам. (Отношение всех событий ИБ к реальным инцидентам).
- Корректное оповещение и выбор контрмер.

2) Наличие модулей прогнозирования.

- Процент инцидентов, произошедших по причине известных уязвимостей.
- Процент повторения ранее устранённых инцидентов.

3) Корреляция данных.

- Процент событий ИБ, соответствующих ранее созданным правилам (rule based).
- Число сопоставления событий ИБ, определенному инциденту. (Событие – link down; инцидент – lost connection).
- Количество предустановленных правил корреляции.
- Количество используемых методов корреляции.

4) Ресурсы под SIEM системы [6].

- Метрики нагрузки на корреляционное ядро.
- Метрики нагрузки на агрегационное ядро.
- Метрики работы внутренних ресурсов базы данных.
- Метрики работы базы данных.
- Метрики поступающего потока событий.
- Метрики состояния работы операционной системы.
- Метрики состояния работы дисковых накопителей.
- Метрики утилизации процессорного времени.

Современная IT-инфраструктура обязана быть динамичной, в ней постоянно обновляется программное обеспечение, загружаются новые приложения, заменяется устаревшее или вышедшее из строя оборудование. Чтобы SIEM-система работала в условиях постоянных изменений нужно поддерживать её в актуальном состоянии: подключать новые источники, следить за работоспособностью правил корреляции. При внедрении SIEM, модерни-

зации информационной структуры (ИС) зачастую не учитывается дополнительная нагрузка на пропускную способность сети, забивающая трафиком каналы связи. Следует отметить недостатки SIEM [7]:

- Функционирование SIEM-системы направлено на констатацию фактов состояния ИС, а не на реализацию защитных функций.
- Отсутствие масштабируемости. SIEM не подстраиваются под изменения в инфраструктуре. Отсюда некорректность/неэффективность работы правил корреляций.

Для того чтобы функционировать более эффективно SIEM должна включать:

– способность обнаруживать актуальные на текущий момент угрозы;
– гибкость к изменениям в инфраструктуре.

Согласно исследованиям [8], лучшие результаты, с точки зрения эффективности обнаружения инцидентов, показывают приложения Micro Focus (HP), ArcSight и Splunk.

Таким образом, необходимо отметить, что существующие алгоритмы, методики и методы на данный момент не позволяют в полной мере оценивать эффективность SIEM систем и требуют дополнительных пояснений и модернизации [9, 10]. В статье были определены показатели эффективности SIEM систем. В дальнейшем планируется проработка модели оптимальной системы мониторинга и корреляции событий информационной безопасности, разработка метода оценки эффективности SIEM систем.

Список используемых источников

1. Миняев А. А., Красов А. В., Сахаров Д. В. Метод оценки эффективности системы защиты информации территориально-распределенных информационных систем персональных данных // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2020. № 1. С. 29–33.

2. Карельский П. В., Ковцур М. М., Миняев А. А. Особенности развертывания Security Operations Center при организации удаленного доступа к инфраструктуре компании // Актуальные проблемы инфотелекоммуникаций в науке и образовании. X Юбилейная Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2021. Т. 1. С. 433–437.

3. Бабков И. Н. Анализ эффективности SIEM-системы в организации // Актуальные проблемы инфотелекоммуникаций в науке и образовании. X Юбилейная Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб: СПб ГУТ, 2021. Т.1. С. 72–77.

4. Обзор мирового и российского рынков SIEM-систем 2022. URL: https://www.anti-malware.ru/analytics/Market_Analysis/SIEM-2022

5. Карельский П. В., Зуев И. П., Ковцур М. М., Миняев А. А. Разработка методики тестирования IPS модуля // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2021. № 1. С. 25–31.

6. Система под контролем. Автоматизация контроля работоспособности SIEM-систем. URL: https://ib-bank.ru/bisjournal/post/1341

7. Королев И. Д., Попов В. И., Ларионов В. А. Анализ проблематики системы управления информацией и событиями безопасности в информационных системах // Журнал «Инновации в науке». 2018. № 12 (88). С. 19–26.

8. Очередько А. Р., Герасименко В. С., Путято М. М., Макарян А. С. Исследование SIEM-систем на основе анализа механизмов выявления кибератак // Вестник АГУ. 2020. Вып. 2 (261). С. 25–30.

9. Ковцур М. М., Казаков Н. И., Ушаков И. А., Коновалова В. В. Автоматизированная система оповещения пользователей с применением мессенджера. Свидетельство о регистрации программы для ЭВМ 2021619708, 15.06.2021. Заявка № 2021618697 от 03.06.2021.

10. Ковцур М. М., Миняев А. А., Петров В. А., Таргонская А. И. Методика организации распределенной разработки безопасного программного обеспечения // Актуальные проблемы инфотелекоммуникаций в науке и образовании. X Юбилейная Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2021. Т. 1. С. 493–497.

УДК 004
ГРНТИ 20.15.05

СОЗДАНИЕ ДЕЦЕНТРАЛИЗОВАННОГО МЕССЕНДЖЕРА С ПРИМЕНЕНИЕМ БЛОКЧЕЙН ТЕХНОЛОГИЙ

В. Н. Бакатов, А. А. Мартынюк, Н. А. Мурашкин, А. В. Помогалова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевич

Технология Blockchain считается наиболее инновационной и перспективной технологией нашего времени. В наше время эта технология набирает обороты в самых разных сферах. Одна из которых - сфера делового общения. Актуальность применения технологии обоснована необходимостью в безопасном и удобном способе коммуникаций и заключении сделок в корпоративной среде. Данная работа посвящена разработке децентрализованной платформы, выполняющей функции мессенджера с интегрированными смарт-контрактами. В рамках данного проекта предлагается децентрализованное решение, разработанное на базе блокчейн-платформы Ethereum.

блокчейн, Ethereum, смарт-контракт, децентрализованные приложения, matrix.

Предприятия и организации, функциональность которых связана с конфиденциальными данными, требующая локальных корпоративных версий площадок обмена сообщениями и задачами, ищут новые возможности в отрасли информационных технологий, чтобы улучшить свои процессы и операции. Данный проект призван помочь им в этом внедрением технологии блокчейн в мессенджер, через который проходит вся связь сотрудников

в компании, с возможностью совершения цифровых сделок – безопасно и бесшовно.

Поскольку сделки осуществляются без посредников, то есть напрямую между заказчиком и исполнителем, блокчейн гарантирует неизменность данных, отсутствие комиссий, мгновенное заключение сделок и договоров, позволяя экономить средства и время обеих сторон. Данное решение возможно масштабировать, как расширение частного, корпоративного мессенджера до публичного в блокчейн-сети *Ethereum*. При этом все блокчейн функции будут работать так же.

Все сделки и договоренности в мессенджере воплощены в виде смарт-контрактов на блокчейне, что гарантирует безопасность и прозрачность операций. Это обусловлено тем, что смарт-контракт – это программный код, который нельзя изменить после загрузки в сеть. Таким образом, обеспечиваются исполнение обязательств двух сторон, а также автоматизированное и простое совершение сделки, без комиссий и посредников.

Мессенджер позволяет объединить в себе важнейшие для корпораций функции не только обмена сообщениями, но также средства заключения сделок и договоренностей в виде смарт-контрактов на блокчейне, и помимо этого, распределение рабочих задач и их оценку в виде токенов, что позволит также оценить КПД сотрудников с точки зрения количества реализованных задач и их стоимости.

Основой передачи сообщений в данном сервисе является протокол *Matrix* [1], имеющий федеративный характер. Это значит, что пользователи разных серверов могут общаться между собой, а серверы могут связываться между собой, образуя федерацию.

На данный момент в сети *Matrix* порядка 75 тысяч узлов и 40 миллионов пользователей, данная технология позволяет создавать ботов для удобной работы с информацией, дает возможность организовать собственный сервер (как открытый, так и закрытый) даже на непроизводительных компьютерах, и микрокомпьютерах в том числе.

Основными преимуществами его использования являются:

– репликация, ведущая к отсутствию единой точки контроля или отказа;

– синхронизация ключей в зашифрованных комнатах, позволяющая добиться кроссплатформенности;

– мосты(*bridges*), дающие возможность общаться через *Matrix* с пользователями других мессенджеров, в которых у желающего есть аккаунт;

– виджеты для интеграции сторонних приложений в комнаты (чаты);

– разнообразие клиентских приложений и возможность собственной кастомизации.

Основными проблемами разработанного мессенджера является сложность архитектуры приложения (рис.), поскольку проект задействует большой стек языков программирования и сервисов: *Docker* – как контейнер для быстрого запуска и размещения программного продукта, приватный блокчейн из 3 нод (узлов) для осуществления децентрализации задач и возможности безопасных сделок , базы данных *PostgreSQL* для хранения информации о пользователях, необходимой для регистрации и последующего входа, *Backend* – часть на языке программирования *Go*, отвечающая за работоспособность всей архитектуры вместе, Solidity [2] – язык для написания смарт-контрактов, *Frontend* – часть приложения на *Javascript*, работающая поверх протокола открытого стандарта *Matrix*, используемого для передачи сообщений, и позволяющая пользователю удобно контактировать с *Web*-приложением.

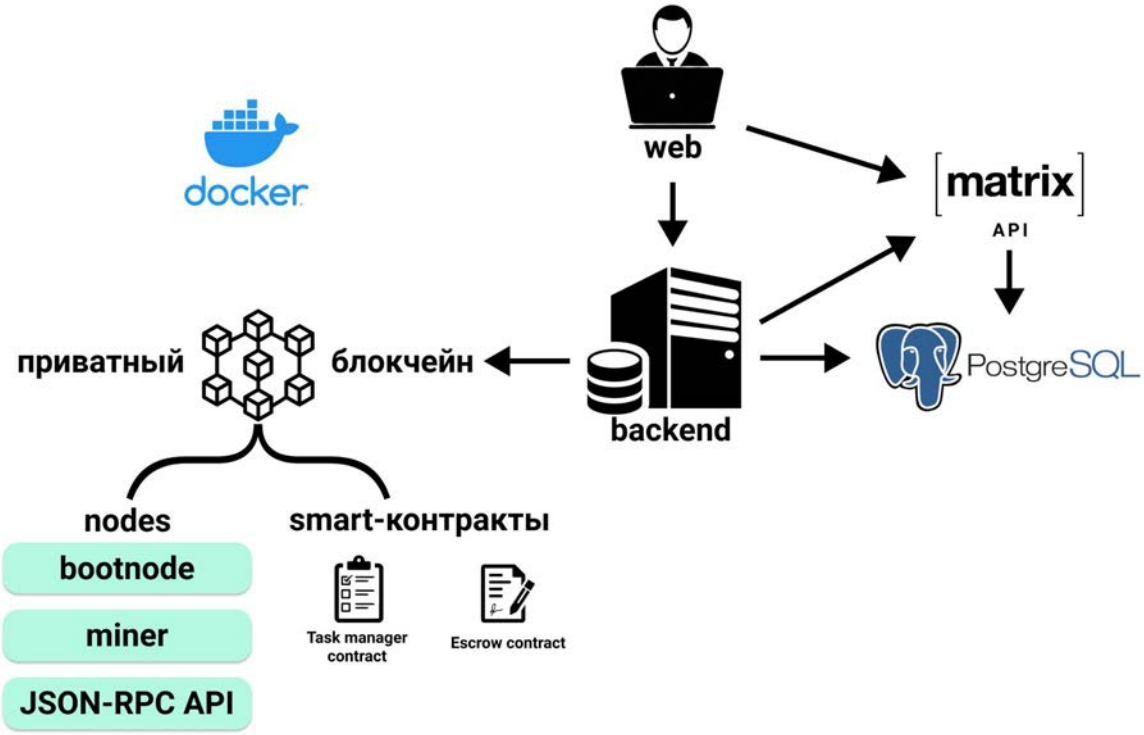


Рисунок. Архитектура приложения

В связи с количеством вышеперечисленных технологий, для поддержания работы мессенджера требуются немалые характеристики: не менее 10 Гб оперативной памяти, процессор с не менее, чем 5 ядрами и 30 Гб пространства памяти.

Помимо затрат на поддержание работоспособности данного сервиса существуют и другие трудности в виде недостатков отдельных технологий, используемых в работе приложения, а также обновления связанных с ним стандартов языков программирования и протокола передачи сообщений, что ведет за собой дополнительные затраты на поддержку программного

обеспечения уже на стадии использования компанией и выпуска в публичный доступ.

Список используемых источников

1. Matrix Specification. URL: https://spec.matrix.org/latest/ (дата обращения: 17.11.2021)

2. The Solidity Contract-Oriented Programming Language documentation. URL: https://docs.soliditylang.org/en/v0.8.13/ (дата обращения: 10.11.2021)

Статья представлена директором научно-исследовательского института «Технологии связи», кандидатом технических наук, доцентом кафедры ИКС СПбГУТ В. С. Елагиным.

УДК 621.391.883
ГРНТИ 49.01.81

ОЦЕНКА ОБЩИХ ПОКАЗАТЕЛЕЙ КАЧЕСТВА АНАЛОГОВЫХ ОКОНЧАНИЙ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ

К. А. Батенков

Академия Федеральной службы охраны Российской Федерации

Рассматриваются общие показатели качества аналоговых окончаний: полоса эффективно передаваемых частот, остаточное затухание, затухание асимметрии, симметричное напряжение и общее несимметричное напряжение. Отмечается, что для каналов тональной частоты, образованных цифровыми системами передач, и смешанных каналов необходимо следить, чтобы частота измерительного сигнала не была субгармоникой частоты дискретизации 8 кГц во избежание дополнительной погрешности или биений.

сеть связи, телекоммуникационная сеть, показатель качества, аналоговое окончание, канал тональной частоты.

К общим показателям качества аналоговых окончаний относят следующие характеристики: полоса эффективно передаваемых частот, остаточное затухание, затухание асимметрии, симметричное напряжение и общее несимметричное напряжение.

Эталонная (опорная) точка передачи (*TRP – transmission reference point*) – гипотетическая точка на передающем конце канала или вблизи него

(предшествующая виртуальной точке переключения), используемая в качестве "точки нулевого относительного уровня" при вычислении номинальных относительных уровней [1, 2].

Полоса эффективно передаваемых частот составного канала тональной частоты: 300–3 400 Гц.

При определении уровней передачи за условную точку номинального нулевого относительного уровня канала тональной частоты (начало канала) принимают его условный двухпроводный вход [3, 4]. Номинальное значение относительного уровня передачи на частоте 1 020 Гц в этой точке равно 0 дБо, а на приеме −7 дБо (рис. 1). Используются транзитные удлинители с затуханием −3,5 дБ [5, 6].

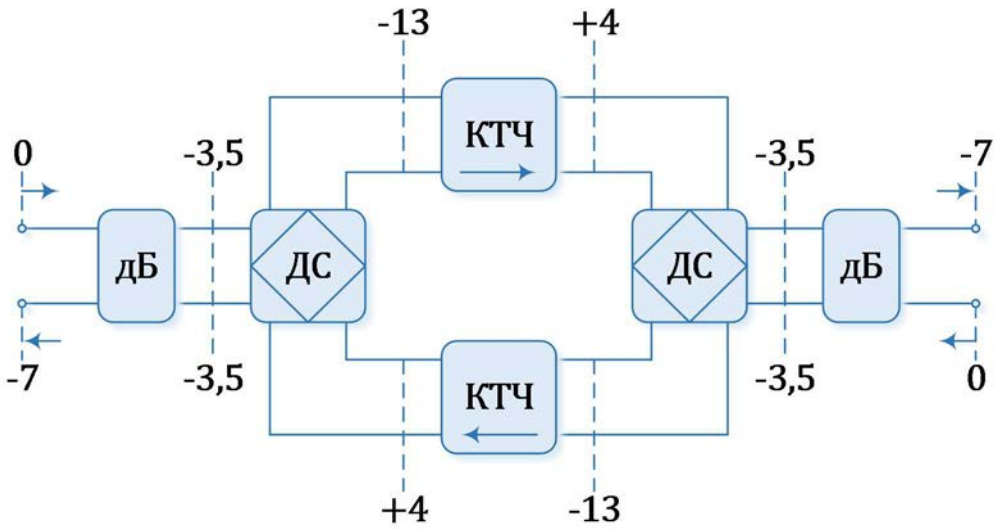


Рис. 1. Уровни передачи и приема двух- и четырехпроводного канала

В четырехпроводной части простого канала тональной частоты номинальный относительный уровень на входе должен быть равен $L_i = 13$ дБо, а на выходе – $L_o = 4$ дБо. В этих точках при использовании канала в четырехпроводном режиме осуществляется передача его потребителям по соединительным линиям, а также постоянный транзит каналов. Погрешность установки значения остаточного затухания канала относительно его номинального значения должна быть не более 0,5 дБ.

На вход передающей части в точку с номинальным относительным уровнем $L_i = 13$ дБо от измерительного генератора подается сигнал частотой 1020 Гц с уровнем $L_i = 23$ дБм, то есть на 10 дБ ниже номинального ($L_r = -10$ дБм0). На выходе приемной части канала в точке с номинальным относительным уровнем $L_o = 4$ дБо устанавливается уровень $L_o = -6$ дБм.

Для каналов тональной частоты, образованных цифровыми системами передач, и смешанных каналов необходимо следить, чтобы частота измерительного сигнала не была субгармоникой частоты дискретизации 8 кГц во избежание дополнительной погрешности или биений.

В подобных условиях (частота дискретизации 8 кГц, 8-битное кодирование) появляются вариации уровней сигналов ± 0,15 дБ при 800 Гц и ± 0,20 дБ при 1 000 Гц [7]. К тому же дрожание других параметров, например, общее искажение, оказываются еще более значительными. Рекомендовано использовать эталонные тестовые частоты, смещенные от 800 Гц или 1 000 Гц на различную величину, но в пределах 804–860 Гц или 1 004–1 020 Гц. В целом эталонная частота 1 020 Гц имеет допуск от +2 до -7 Гц, то есть ее диапазон от 1 013 до 1 022 Гц. Номинальный уровень измерительного сигнала не должен превышать −10 дБм0 ± 0,1 дБ.

Остаточное затухание a – разность между суммой затуханий и усилений в канале [6, 8, 9]:

$$a = L_i - L_o.$$

Входное Z_i и выходное Z_o сопротивления (impedance) канала тональной частоты определяются на основе следующего соотношения [10, 11] (рис. 2):

$$Z_i = \frac{U_1 Z_1}{U_G - U_1}.$$

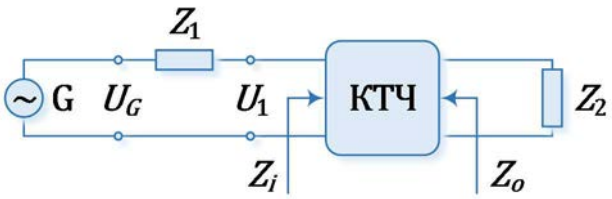


Рис. 2. Несогласованность сопротивлений на передаче Z_i и приеме Z_o

Номинальное значение входного и выходного сопротивлений четырехпроводного (транзитного) окончания канала тональной частоты – 600 Ом [12, 13].

Коэффициент отражения ρ и затухание несогласованности a (return loss) являются мерами отличия входного Z_i и выходного Z_o сопротивлений канала (в общем случае комплексных) от номинальных значений (рис. 2). В общем случае как коэффициент отражения, так и затухание несогласованности на передаче и приеме различны [10, 12, 14]:

$$\rho_i = \left|\frac{Z_1 - Z_i}{Z_1 + Z_i}\right|, \rho_o = \left|\frac{Z_2 - Z_o}{Z_2 + Z_o}\right|,$$

$$a_i = -20\lg\rho_i, a_o = -20\lg\rho_o.$$

Затухание асимметрии (*LCL – longitudinal conversion loss*, продольные потери на преобразования) – это мера (отношение, выраженное в дБ) степени нежелательного поперечного сигнала (симметричного напряжения), возникающего на интерфейсах подключения из-за наличия продольного сигнала (несимметричного напряжения) на соединительных выводах [15–20].

Симметричное напряжение – напряжение между любыми двумя проводниками из заданной группы активных проводников [15, 21].

Общее несимметричное напряжение – среднее значение фазных напряжений между каждым из проводников и регламентированным эталоном, обычно землей или пластиной заземления [15, 22].

Вычисление затухания асимметрии выполняется на основе схемы (рис. 3):

$$a = 20\lg\left|\frac{U_G}{U_1}\right|.$$

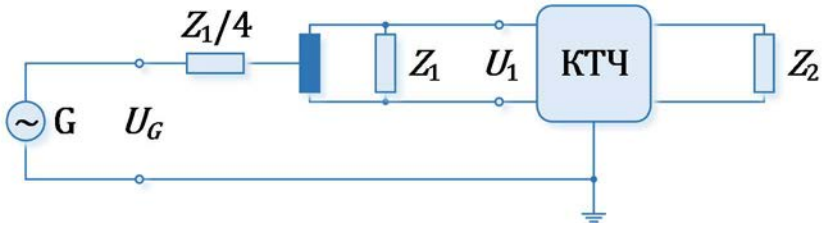


Рис. 3. Схема измерения затухания асимметрии

Список используемых источников

1. Rec. G.101. The transmission plan. – 2003–11. – Geneva : ITU-T, 2003. 34 p.

2. Батенков А. А., Батенков К. А., Фокин А. Б. Методы формирования множеств состояний телекоммуникационных сетей для различных мер связности // Труды СПИИРАН. 2020. Т. 19. № 3. С. 644–673.

3. Нормы на электрические параметры каналов тональной частоты магистральной и внутризоновых первичных сетей : Утв. М-вом связи РФ 15.04.96. –М. : МК-Полиграф, 1996. 96 с.

4. Батенков К. А. Технический эффект оптимальных линейных модуляции и демодуляции в беспроводных системах связи // Известия Института инженерной физики. 2015. № 1 (35). С. 24–28.

5. Rec. G.100.1. The use of the decibel and of relative levels in speechband telecommunications. – 2015–06. – Geneva : ITU-T, 2015. 36 p.

6. Цифровые и аналоговые системы передачи : учебник для вузов / В. И. Иванов, В. Н. Гордиенко, Г. Н. Попов и др. ; Под ред. В. И. Иванова. 2-е изд. М. : Горячая линия – Телеком, 2003. 232 с.

7. Rec. 0.6. 1020 Hz reference test frequency. – 1993. – Geneva : ITU-T, 1996. 3 p.

8. Батенков К. А., Гусев В. В., Илюшин М. В., Катков О. Н., Мельников А. А., Стремоухов М. В. Границы вероятности символьной ошибки для канала связи с логнормальными замираниями при использовании предыскажений и помехоустойчивого кодирования // Телекоммуникации. 2018. № 2. С. 45–48.

9. Батенков К. А. Обобщенный пространственно-матричный вид энергетических ограничений систем связи // Известия Тульского государственного университета. Технические науки. 2013. № 3. С. 238–245.

10. Измерения в ВЧ связи. Устройства обработки и присоединения / под ред. Ю. П. Шкарина. изд. 3, перераб. и доп. М. : Библиотека AnCom, 2014. 123 с.

11. Батенков А. А., Батенков К. А. Дискретизация линейного канала связи с памятью и аддитивным белым гауссовским шумом численным методом // Математическое моделирование. 2009. Т. 21. № 1. С. 53–74.

12. ГОСТ 21655–87. Каналы и тракты магистральное первиной сети единой автоматизированной систмы связи. Электрические параметры и методы измерений. Введ. 1989–01–01. М. : Издательство стандартов, 1988. 106 с.

13. Rec. Q.553. Transmission characteristics at 4-wire amalogue interfaces of digital exchanges. – 2001–11. – Geneva : ITU-T, 2001. 22 p.

14. Баскаков С. И. Радиотехнические цепи с распределенными параметрами : учеб. пособие для вузов. М. : Высш. школа, 1980. 152 с.

15. ГОСТ Р 51700–2000. Технические средства, подключаемые к симметричным линиям. Параметры асимметрии относительно земли. Введ. 2000–12–26. М.: Госстандарт России, 2000. 44 с.

16. Батенков К. А., Миронов А. Е., Королев А. В., Орешин А. Н. Оценка параметров алгоритмов диспетчеризации на основе имитационного моделирования в программной среде Riverbed // Телекоммуникации. 2018. № 8. С. 17–23.

17. Батенков К. А. Дискретные отображения модели непрерывного канала связи на основе обобщенного ряда Фурье // Вестник Рязанского государственного радиотехнического университета. 2013. № 43. С. 12–20.

18. Batenkov K. A. Synthesis of deterministic nonlinear discrete mappings of continuous channel // SPIIRAS Proceedings. 2016. № 2 (45). pp. 75–101.

19. Rec. O.9. Measuring arrangements to assess the degree of unbalance about earth. – 1999–03. – Geneva : ITU-T, 1999. 21 p.

20. Rec. G.117. Transmission aspects of unbalance about earth. – 1996–02. – Geneva : ITU-T, 1996. 22 p.

21. Батенков К. А. Математические модели модулятора и демодулятора с заданным порядком нелинейности // Цифровая обработка сигналов. 2013. № 1. С. 14–21.

22. Батенков А. А., Батенков К. А., Фокин А. Б. Формирование сечений телекоммуникационных сетей для анализа их устойчивости с различными мерами связности // Информатика и автоматизация. 2021. Т. 20. № 2. С. 371–406.

УДК 004.056.57
ГРНТИ 81.93.29

АНАЛИЗ СЕТЕВОЙ АКТИВНОСТИ КАК ИНСТРУМЕНТ ПОВЫШЕНИЯ БЕЗОПАСНОСТИ

Л. С. Беккель, М. Э. Максименко

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье исследуется проблема защиты устройства от вредоносного программного обеспечения (ПО) и сетевых атак с помощью анализа поведения сети и сетевой структуры, приводится пример работы таких программ как nmap и Wireshark. В работе акцентируется внимание на том, что использование лицензионного антивирусного ПО хотя и является наиболее надежным способом защиты устройства, но зачастую пользователи игнорируют его в силу дороговизны. Отдельно рассматривается вопрос анализа сетевого трафика. В статье приводится данные сравнения и сопоставления сетевых атак с фильтрами программы Wireshark, помогающими их обнаружить.

анализ трафика, сетевые атаки, вредоносное программное обеспечение.

Проблема заражения устройства, будь то ноутбук, телефон или ПК, вредоносным ПО не только не теряет своей актуальности, но возрастает в связи с изучением, развитием и повсеместным распространением информационных технологий.

Периодически появляются новые программы, способные нанести вред персональным данным.

Несмотря на это, покупка лицензионного антивирусного ПО является все еще не решенным вопросом для многих пользователей. К тому же существуют методы выявления возможных угроз и уязвимостей «вручную», самим пользователем. В данной статье предпринята попытка рассмотреть несколько таких методов и оценить их эффективность.

Для того чтобы знать где искать слабые места, надо рассмотреть виды возможных угроз для устройства. Так, под вредоносной программой понимается программа, предназначенная для осуществления несанкционированного доступа к информации и (или) воздействия на информацию или ресурсы информационной системы [1]. Типы вредоносных программ представлены в таблице 1.

Вредоносные программы попадают на ноутбук чаще всего через беспроводную сеть.

ТАБЛИЦА 1. Типы вредоносных программ

Вирус	Распространяются вирусы во время передачи программы или документа, к которым они прикреплены, с одного компьютера на другой как по сети, так и посредством носителей информации, а также через общие файловые ресурсы и почтовые вложения
Червь	Проникновение в системы через уязвимость к ней, а не через прикрепление к программе/файлу
Троян	Маскировка под легитимные программы

Помимо вредоносного ПО пользователи сталкиваются и с другими видами угроз, например, с сетевыми атаками, которые представляют собой действия с применением программных и (или) технических средств и использованием сетевого протокола, направленные на реализацию угроз несанкционированного доступа к информации, воздействия на нее или на ресурсы автоматизированной информационной системы [2].

Сетевые атаки можно обнаружить и исследовать с помощью анализа трафика. Изучение локальной сети также позволяет выявить возможные угрозы

Первой утилитой экспериментально использованной для целей исследования выступила «nmap» – доступная программа с открытым исходным кодом. Являясь сканнером портов, она может быть использована в том числе и злоумышленниками для получения данных, необходимых для дальнейшего проникновения вредоносного ПО в устройство.

Мы же на основании этих данных сможем сделать выводы об уязвимости ноутбука и в дальнейшем принять действия по ее устранению

Пример работы программы представлен на рис. 1.

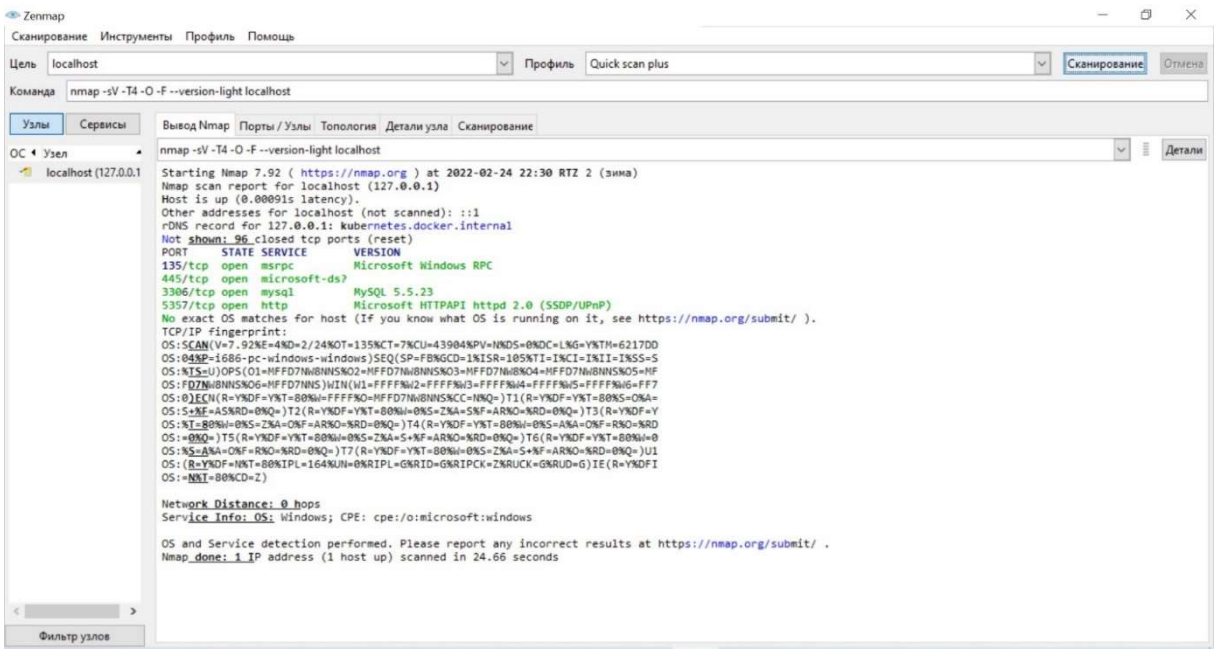


Рис. 1. Работа nmap

Целесообразно рассмотреть протекающие процессы и возможные угрозы.

Первые два открытые порта – 135 и 445 используются приложениями операционной системы, 135 порт отвечает за механизм вызова удаленных процедур. Его закрытие привело бы к сбою ряда приложений, использующих эту функцию, поэтому в данном случае оставить порт открытым – необходимость для продолжения нормального функционирования устройства.

445 порт в Windows зарезервирован под работу с удаленной передачей данных между устройствами домашней сети. Это удобное решение в плане обмена файлов, однако это же может стать угрозой безопасности пользовательского устройства, предоставляя возможность другим компьютерам подключиться к пользовательской сети. При этом его отключение повлечет за собой закрытие доступа внутренней системы для внешних, но не наоборот. Таким образом, в целях повышения безопасности пользователю следует вручную закрыть данный порт.

Версия «MySQL», запущенная на устройстве через порт 3306, является устаревшей и при работе в определенных средах с определенными реализациями функции «memcmp» позволяет злоумышленникам, знающим адрес сервера, удаленно обходить аутентификацию путем повторной аутентификации с одним и тем же неверным паролем, что в конечном итоге вызывает успешную авторизацию из-за неправильно проверенного возвращаемого значения.

Через порт 5357, отвечающий за сетевое обнаружение, подключена служба Microsoft, отвечающая за видимость вашего устройства другими устройствами и наоборот.

Экспериментально анализ трафика будет осуществлен с помощью приложения Wireshark, уже зарекомендовавшего себя как некий стандарт для полноценного администрирования сетей. Рассмотрение примера его работы позволит понять, что происходит в сети в момент просмотра.

В самом верху, зеленым фоном отмечено поля для ввода фильтров. В момент анализа трафика фильтры настроены таким образом, чтобы мы могли видеть отображение пакетов, проходящих через порт, отвечающий за HTTP (*Hypertext Transfer Protocol*). Source – столбец, указывающий источник запроса, Destination – назначение. Мы также можем посмотреть время, за которое произведена передача данных и то, на каком уровне идет обмен информацией.

В первую очередь следует обратить внимание на рост трафика. Сделать это можно используя графическое представление статистики в Wireshark. При просмотре статистики стоит также уделить внимание большому количеству пакетов определенного протокола (impc/wlan/tcp/udp), в зависимости от которого можно говорить об атаке отказа в обслуживании определенного типа.

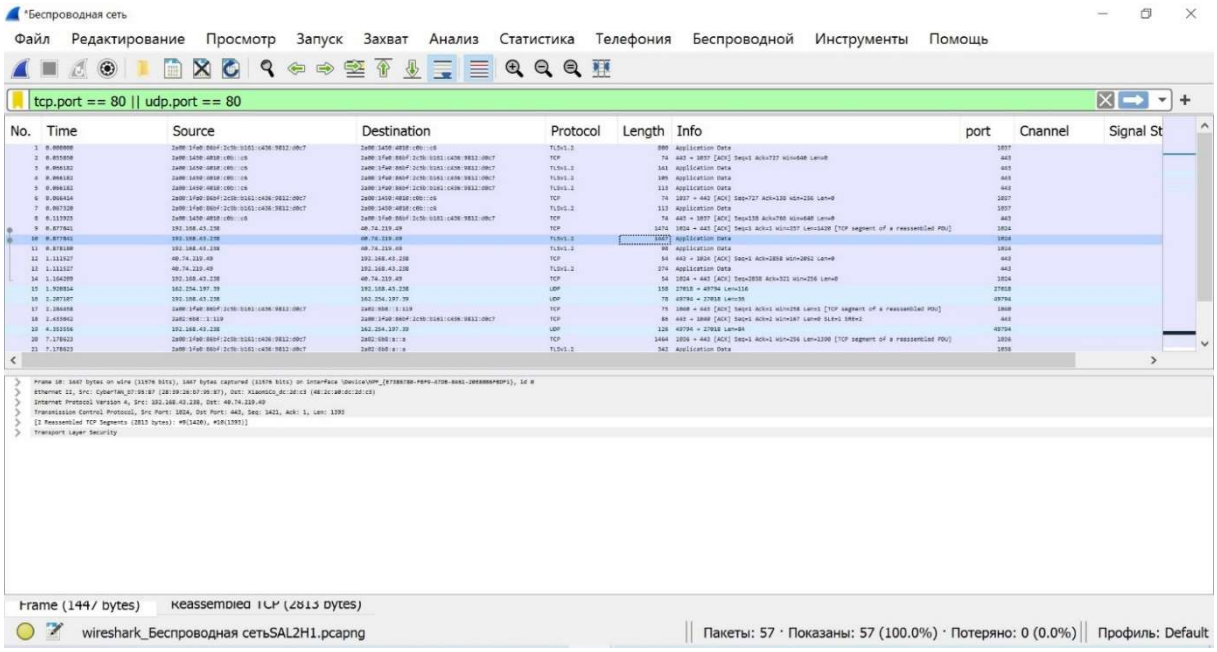


Рис. 2. Пример работы Wireshark

При захвате пакетов можно использовать фильтры, которые помогают выявить следующие виды сетевых атак, представленные в таблице 2.

- Сетевая разведка – сбор информации о сети с помощью общедоступных данных и приложений [3]. Примером сетевой разведки могут послужить описанные выше действие при работе с «nmap».
- Man-in-the-middle – атака, включающая в себя перехват сетевого трафика.
- Атаки типа отказа в обслуживании, которые проявляются в виде отправки большого объема данных. DoS-атаки различаются по протоколу передачи этих данных.

ТАБЛИЦА 2. Выявление сетевых атак с помощью фильтров Wireshark

Наименование	Фильтр Wireshark	Принцип работы
Сетевая разведка	tcp.flags.syn = = 1 and tcp.flags.ack = = 0 and tcp.window size < = 1024	Происходит фильтрация отправленных пакетов с меньшим, чем обычно, размером, которые несут в себе минимальный объем данных или вообще не несут их, что характерно для сканеров сети
Man-in-the-middle	arp.duplicate-address-detected or arp.duplicate-address-frame	Отображает ситуацию, когда один и тот же ip адрес необходим более чем для одного мак адреса

Наименование	Фильтр Wireshark	Принцип работы
DoS-attack	tcp.flags.syn = = 1 and tcp.flags.ack = = 0tcp.flags.syn = = 1 and tcp.flags.ack = = 1	Принцип заключается в сравнении количества отправленных и подтвержденных пакетов. В случае, если первых больше, можно говорить об атаке TCP SYN flood
	icmp and data.len > 48	Выделяются пакеты, размер которых больше принятого. Что указывает на атаку IMPC flood
	wlan.fc.type subtype = = 11	Выделяются фреймы аутентификации, чрезмерное количество которых позволяет обнаружить DoS-атаку аутентификации

С помощью рассмотренных инструментов можно выявить следующие факторы, указывающие на потенциальные уязвимости:

- открытые порты;
- неизвестные подключенные устройства;
- порты, занятые программами с устаревшими версиями;
- нестандартное поведение трафика;
- передачу больших пакетов данных.

В результате, использовав лишь два приложения можно выявить множество недочетов в работе устройства. Однако способны ли эти действия заменить работу полноценного антивируса? В примерах выше не были рассмотрены программы-руткиты, которые, проникая вглубь системы, работают с устройством через права администратора, имеют возможность скрывать свои действия от различных сканнеров сети, что делает их труднодоступными для обнаружения. Даже в случае их обнаружения процедура удаления может быть осложнена из-за вышеупомянутых прав администратора и распространения программы в корне системы.

Процесс анализа трафика сети и сканирования портов требует определенных усилий и периодичности в случае, если использовать его в качестве основного средства борьбы с вредоносным ПО, к тому же в результате приводит лишь к обнаружению, но не устранению с таковым.

Таким образом, проведенный эксперимент позволил выявить определенные критерии, позволяющие сделать вывод об угрозе рассматриваемой системе, с использованием доступных приложений. Однако для полноценной защиты устройства рассматриваемым методом необходимо постоянное администрирование и понимание работы сетевых технологий, уровней сети.

Для безопасности домашнего ПК или рабочего ноутбука лучшим решением в данный момент остается покупка лицензионного антивирусного ПО, которое сэкономит время и гарантированно убережет устройства от нежелательных программ.

Список используемых источников

1. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. М.: ИПК Издательство стандартов, 2008.

2. ГОСТ Р 53114-2008. Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. М.: ИПК Издательство стандартов, 2008.

3. Кадер М. Типы сетевых атак, их описания, средства борьбы // CNews. Аналитика. URL: https://www.cnews.ru/reviews/free/oldcom/security/cisco_ attacks.shtml?print

УДК 004.8
ГРНТИ 28.23.33

ОБЗОР ПЛАТФОРМ АППАРАТНОГО УСКОРЕНИЯ НЕЙРОННЫХ СЕТЕЙ

Т. И. Белая, А. Ю. Березин

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В данной статье будут рассмотрены различные аппаратные платформы для ускорения в области вычислений и обучения нейронных сетей, такие как GPU, ASIC, FPGA. Также нюансы реализации нейронных сетей на платформах аппаратного ускорения. Аппаратные ускорители применяют для увеличения скорости обработки данных. Современные нейронные сети, как правило, очень большие что приводит к увеличению времени обработки. Также тенденции развития сетей, показывает, что размер сетей растет экспоненциально. При этом в требованных современных задач ставят максимально возможный быстрый вывод. Даже современные высокопроизводительные CPU могут не справляться с большими объемами нейронных сетей, как правило из-за задержек передачи данных между памятью и самим CPU.

аппаратное ускорение, искусственный интеллект, нейронные сети, платформы ускорения

Аппаратные устройства расположены на нижнем уровне стека ускорения. Это устройства, выполняющие вычисления, такие как GPU, FPGA и некоторые специализированные ASIC-ускорители. Техника ускорения здесь очевидна: более мощные вычислительные блоки приводят к более быстрому выводу результатов обучения нейронных сетей. Аппаратное устройство

имеет первостепенное значение для стека ускорения; например, GPU может увеличить пропускную способность на порядок по сравнению с CPU. Несмотря на это, прирост скорости от аппаратных устройств ограничен при этом объем вычислений, необходимых крупным системам ИИ, удваивался каждые 3–4 месяца.

Графические процессоры (GPU) предназначены для обработки изображений с помощью массивного параллелизма, но сегодня они используются в аналитике больших данных, ускорении части приложения, требующего высокой пропускной способности и пропускной способности памяти. GPU превосходны в параллельной обработке. Они могут обеспечить ускорение там, где одни и те же операции требуются вычислить много раз в быстрой последовательности. Однако графические процессоры потребляют огромное количество энергии, что создает проблемы для приложений нейронных сетей, которые должны быть включены в ограниченные устройства, особенно работающие от аккумуляторов. Графические процессоры достигают высокой пропускной способности благодаря способности обрабатывать партии входных данных большого размера, но при этом задержка может быть высокой. Поэтому они не подходят для приложений, критичных к задержкам. Ниже представлен график сравнения времени выполнения для обучения нейронных сетей. Время выполнения для CPU и GPU представлено синими и оранжевыми точками. На всех графиках время измеряется в микросекундах, также имеется линия тренда, помогающая визуализировать общую разницу между результатами CPU и GPU. В качестве исследуемых сетей были взяты сети классификатора текста (text-classifier), представленная сверточной сетью из четырех слоев, и взята сеть классификатор цифр (mnist).

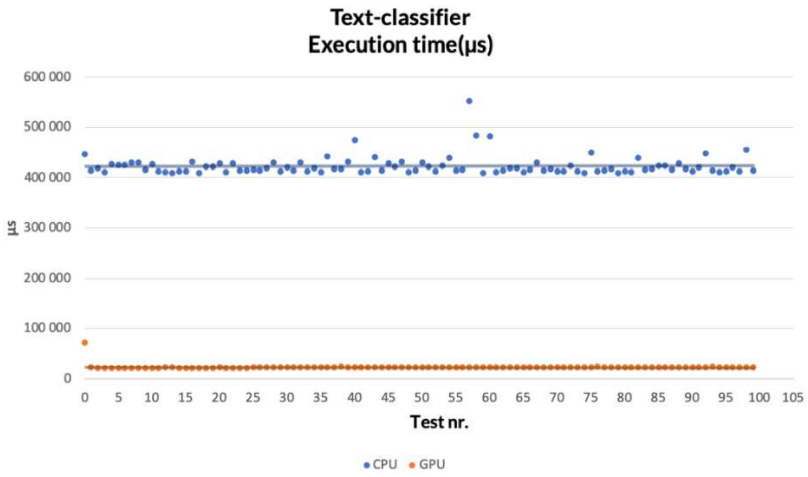


Рис. 1. Время обучения для текстового классификатора

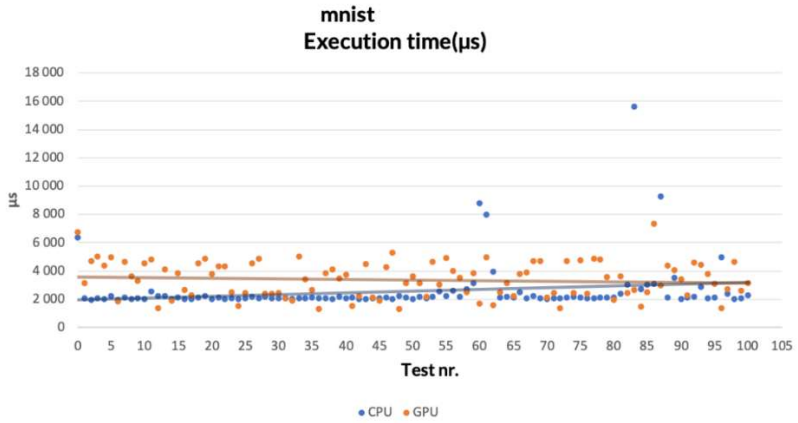


Рис. 2. Время обучения для набора данных mnist, 5 связанных слоев

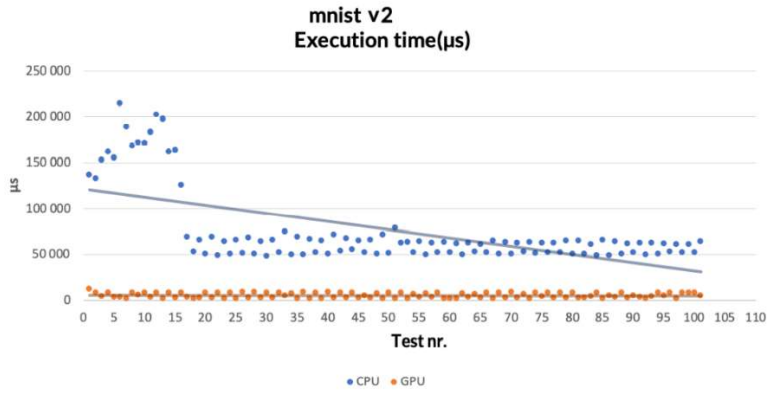


Рис. 3. Время обучения для набора данных mnist использующей пять слоев с тремя конволюционными слоями

Сравнение результатов, полученных на CPU и GPU, показывают, что производительность выигрывает от вычислительной мощности GPU только в том случае, если обучается сложная нейронная сеть.

Результаты продолжительности обучения наглядно демонстрируют взаимосвязь между использованием CPU и GPU, в то время как распределение памяти в основном зависит от объема обучающих данных. На рис. 1 можно видеть, что время обучения на GPU ниже по сравнению с тем же тестом на CPU. Однако на рис. 2 показано, что тесты как на CPU, так и на GPU имеют эквивалентную продолжительность. Это также справедливо для большинства других нейронных сетей, использующих набор данных набор данных mnist. Только самая сложная из нейронных сетей mnist использует GPU и имеет выигрыш в производительности, как показано на рис. 3. Основная разница в нейронных сетях mnist заключается в том, используют ли они сверточные слои или нет. Результаты показывают, что нейронные сети с более высокой сложностью получают преимущества от вычислительной мощности GPU.

ASIC – это Application-Specific Integrated Circuit, т. е. интегральная схема специального назначения. К примеру, реализующая заложенную

в железо нейросеть. При этом большинство вычислительных узлов может работать параллельно. Главными отличиями ASIC от FPGA является реконфигурируемость и оптимизация. Как показывает исследование [4] энергоэффективность ASIC в разы лучше энергоэффективности, которую можно достичь на FPGA, что отображено в таблице. Но при этом использование ASIC чревато тем, что при необходимости изменения нейронной сети возникнет необходимость разрабатывать новый ASIC и, следовательно, плату и производить дополнительную работу по разработке платформы электрической платы, на которой будет размещен ASIC.

ТАБЛИЦА. Сводка производительности FPGA и ASIC

Platform Type	Freq (MHz)	Power (W)	GOP/s	Energy Efficiency (GOP/s/W)
FPGA	100	34.04	11,973	351.7
ASIC	30	1.9	1,326	698

FPGA могут быть использованы для ускорения части алгоритма путем передачи программируемой логике задач, требующих больших вычислений. Они могут достигать высокой производительности за счет широкого параллелизма и в то же время являются энергоэффективными по сравнению с графическими процессорами, а также имеют меньшее время выхода на рынок и меньшую стоимость по сравнению с ASIC. Еще одной важной особенностью FPGA является их реконфигурируемость, которая невозможна для ASIC. Поскольку структуры нейронных развиваются с каждым днем, возможность реконфигурации является дополнительным преимуществом. Применять FPGA имеет смысл на этапе применения нейросети (для обучения в большинстве случаев будет недостаточно памяти). Стоит отметить, что тема выполнения нейронных сетей на FPGA сейчас начала активно развиваться. На рис. 4 представлен пример дизайна FPGA для выполнения нейронной сети.

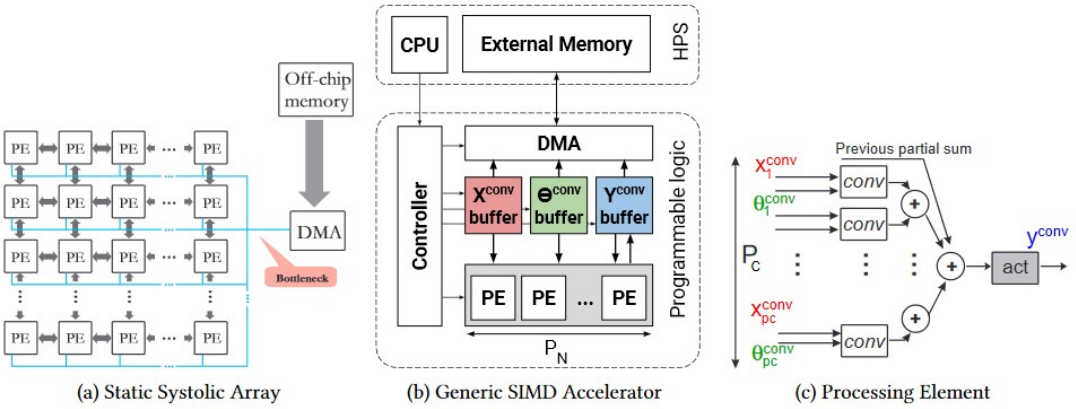


Рис. 4. Пример дизайна FPGA для выполнения нейронной сети

Исходя из данных, приведенных в статье [2] данных производительности нейронной сети, развернутой на GPU и FPGA, можно сказать, что при достаточно большой рабочей нагрузке GPU способен поддерживать высокий параллелизм на уровне потоков для достижения высокой пропускной способности. В отличие от этого, решение на базе FPGA инвариантно к размеру пакета данных (batch size). Результаты показывают, что решение на FPGA превосходит GPU-ускорение энергоэффективности (Рис. 5) и при небольшом пакете данных (batch size) превосходит по производительности (**Ошибка! Источник ссылки не найден.**).

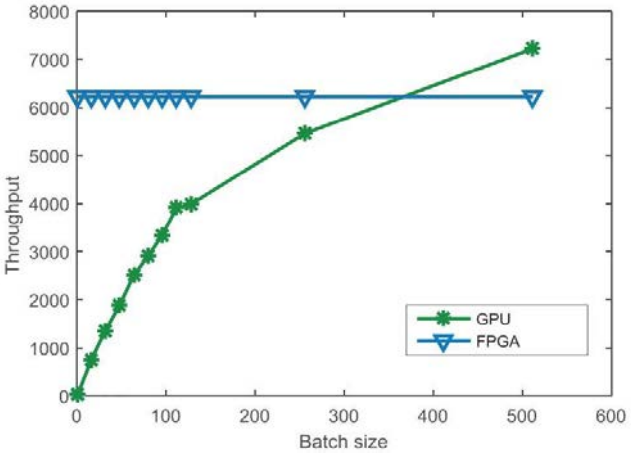


Рис. 5. Сравнение производительности FPGA и GPU

Таким образом можно сказать, что самая производительная платформа аппаратного ускорения выполнения и обучения нейронных сетей – GPU, но при этом имеет самые большие энергозатраты. Также если учесть экономическую часть, то стоимость GPU на данный момент выше, чем на FPGA, но при этом трудозатраты на разработку меньше. Что касается FPGA, сравнительно небольшие энергозатраты, сравнимая производительность с GPU. Использовать ASIC имеет смысл только в больших производственных масштабах и только при полной уверенности, что не придется менять дизайн вычислений и нейронную сеть.

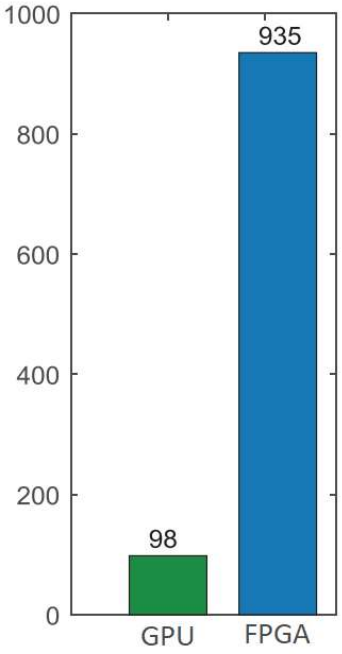


Рис. 5. Сравнение энергоэффективности FPGA И GPU

Список используемых источников

1. ERIC LIND, Ä. P. (7 Июня 2019 г.). A performance comparison between CPU and GPU in TensorFlow. SKOLAN FÖR ELEKTROTEKNIK OCH DATAVETENSKAP. P. 35.

2. Mao, W. (2020). Proceedings of the 2020 on Great Lakes Symposium on VLSI. Energy-Efficient Machine Learning Accelerator for Binary Neural Networks (pp. 77–82). Beijing: ResearchGate.

3. Parateek Shantharama, A. S. (1 Ноября 2017 г.). Hardware-Accelerated Platforms and Infrastructures for Network Functions: A Survey of Enabling Technologies and Research Studies. IEEE Access. P. 65.

4. Yixing Li, Z. L. (1 Июля 2018 г.). A GPU-Outperforming FPGA Accelerator Architecture for Binary Convolutional Neural Networks. Emerging Technologies in Computing Systems. P. 18.

УДК 629.7.02
ГРНТИ 50.47.02

ОРГАНИЗАЦИЯ АВТОМАТИЗИРОВАННОЙ СЕТИ КАМПУСНОЙ ДОСТАВКИ С ПОМОЩЬЮ БЕСПИЛОТНЫХ ЛЕТАТЕЛЬНЫХ АППАРАТОВ

М. А. Бирюков, А. А. Земцов, П. А. Ремденок

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Статья посвящена организации автоматизированной сети кампусной доставки с помощью беспилотных летательных аппаратов. Рассмотрены существующие способы кампусной доставки, их достоинства и недостатки. Описаны: порядок выполнения доставки, новый способ посадки БЛА, с применением компьютерного зрения, подход к построению маршрута.

беспилотные летательные аппараты, автоматизированная доставка, кампусная доставка, взлетно-посадочная площадка, автоматизированная система посадки, автоматизированная система построения маршрута, маркировка на ВПП.

В современном мире нередко можно увидеть дронов над головой, но спектр их применения на данный момент в основном ограничивается аэрофотосъемкой и картографией. Подход реализации автоматизированной сети кампусной доставки с помощью беспилотных летательных аппаратов (далее – БЛА), позволит закрыть потребности в мелкой доставке большой территориально-локализированной коммерческой организации или вуза, а также послужит следующим шагом в применении и развитии технологий в целом [1].

За основу анализа существующих подходов сети кампусной доставки были взяты: Курьерская и Яндекс.Ровер.

Курьерская доставка. У данного подхода есть ряд плюсов, из которых можно отметить надежность и скорость доставки. Курьер имеет полный контроль над процессом и в случае каких-либо эксцессов может самостоятельно их разрешить. Но данный подход не лишен минусов, таких как: постоянные материальные расходы и человеческий фактор.

Яндекс.Ровер – инновационный способ беспилотной доставки от компании ООО «ЯНДЕКС» [2] и американский сервис доставки еды «GRUBHUB», которые запустили в главном кампусе Университета штата Огайо в городе Колумбус роботизированную доставку. Данный подход имеет ряд плюсов: исключение человеческого фактора, что позволяет осуществлять доставку 24 часа в сутки и 7 дней в неделю, и отсутствие посто-

янных материальных расходов. В свою очередь, из минусов можно выделить: способ передвижения, который зачастую мешает прохожим, низкая скорость доставки и угроза кражи ввиду небольшого размера и дороговизны элементарной базы.

Рис. 1. Порядок выполнения доставки

Кампусная доставка с помощью БЛА лишена недостатков предыдущих реализаций. Конечно, дроны не способны перемещать тяжелые и крупногабаритные грузы, но, в свою очередь, они выигрывают по скорости доставки и материальным расходам. Внутри кампуса беспилотники могут доставлять документы и мелкогабаритные грузы.

Доставка будет осуществляться в следующем порядке (рис. 1):

1. Установка мобильной взлетно-посадочной полосы.
2. Вызов дрона в приложении.
2.1. Отправка данных на сервер.
2.2. Анализ свободных БЛА и уровень их заряда.
2.3. Построение маршрута.
2.4. Определение времени доставки.
2.5. Расчет энергозатрат.
2.6. Утверждение дрона исполнителя и его подача к ближайшей зоне погрузки.
3. Загрузка груза.
4. Отправка дрона.
5. Доставка.
6. Прием дрона с грузом.
6.1. Включение камеры.
6.2. Отправка данных на сервер для распознавания ВПП.
6.3. Распознавание ВПП и максимальное сближение с ней.
6.4. Сброс груза.
7. Отправка дрона в зону ожидания для дальнейшей подзарядки.

Принцип работы взлетно-посадочной площадки (далее – ВПП) – (будет рис. 2) для посадки дрона будет использоваться ВПП с нанесенной на ней соответствующей рисунку маркировкой из светоотражающего материала. Маркировка составлена из трех ориентировочных квадратов, с помощью которых дрон будет считывать зону посадки и свое положение относительно ВПП. В центре маркировки

будет располагаться крест, который будет служить для центрирования положения дрона на ВПП.

Перед тем как заказать дрон, пользователю необходимо будет установить мобильную ВПП, при входе в приложение, пользователя будет встречать начальный экран с предложением отсканировать уникальный QR-код на мобильной ВПП. После авторизации пользователю предоставляется возможность указать адрес получателя и заказать БЛА. При заказе дрона геолокация пользователя отсылается на сервер для дальнейшего построения маршрута.

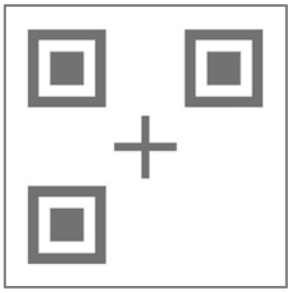


Рис. 2. Маркировка на ВПП

Маршрут строится на основе расстояния от заказчика до зоны ожидания и пункта назначения, после чего рассчитывается время доставки на основе средней скорости БЛА с максимально загруженным контейнером с поправкой на направление и скорость ветра, из которых вычисляются энергозатраты [3]. После всех вычислений идет этап утверждения БЛА, система выбирает ближайший дрон с уровнем заряда достаточного для доставки или превышающим его.

Загрузка БЛА будет осуществляться отправителем на мобильной ВПП. По посадке БЛА отправитель открывает контейнер и кладет груз, который хочет отправить. После загрузки отправитель в приложении отмечает тип груза и отправляет БЛА, по окончании процесса загрузки дрон начинает выполнять маршрут [4].

Система автоматической посадки, устроена следующим образом. Во время посадки дрон активирует камеру и начинает транслировать видео на сервер, который осуществляет поиск необходимой маркировки, по её нахождению сервер отдает необходимые команды БЛА, для того-чтобы дрон занял центральное положение над ВПП, после чего начинается снижение и успешная посадка. Как только процесс посадки завершился, камера выключается и сервер ожидает ответа от пользователя.

Для оптимизации энергозатрат на посадку, БЛА в зависимости от типа груза может менять тип передачи груза получателю. При хрупком грузе БЛА будет осуществлять посадку и ожидать получение груза. В случае если груз не является хрупким, дрон максимально сближается с ВПП и открывает нижнюю часть контейнера, происходит сброс груза с максимально малой высоты. После чего дрон отправится в зону ожидания для дальнейшей подзарядки.

Ввиду вышеизложенного можно с уверенностью сказать, что технология сети автоматизированной кампусной доставки с помощью БЛА один из самых быстрых и оптимальных решений в своей сфере, и поскольку в нашей

стране [5] не ведутся разработки в данном направлении, эта область исследования и практического применения является актуальной и востребованной.

Список используемых источников

1. Порядок использования воздушного пространства РФ беспилотными воздушными судами. URL: https://favt.gov.ru/poryadok-ispolzovaniya-bespilotnyh-vozdychnih-sudov/

2. «Яндекс» и Grubhub запустили в кампусе университета штата Огайо доставку при помощи роботов. URL: https://tarantas.news/posts/id23942-gkzob6djp6ukwktahvzz

3. Бирюков М. А., Брунилин А. А., Саенко И. Б. Способ формирования единой семантической модели предметных областей комплекса разнородных задач // VI Международная научно-техническая и научно-методическая конференция. Актуальные проблемы инфотелекоммуникаций в науке и образовании: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2017. Т. 3. С. 83–88.

4. Карта знаний. Тактико-технические характеристики URL: https://clck.ru/dmDFf

5. Закон о БЛА(БЛА). URL: https://dronomania.ru/faq/zakon-o-bespilotnikah.html

УДК 004.657
ГРНТИ 50.41.21

СРАВНИТЕЛЬНАЯ ОЦЕНКА ВАРИАНТОВ ОРГАНИЗАЦИИ ИНФОРМАЦИОННОГО ВЗАИМОДЕЙСТВИЯ В РАСПРЕДЕЛЕННОЙ СИСТЕМЕ УПРАВЛЕНИЯ

М. А. Бирюков[1], А. А. Макуха[2], И. Б. Саенко[2]

[1]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

[2]Военная орденов Жукова и Ленина Краснознаменная академия связи имени Маршала Советского Союза С. М. Буденного

В статье рассматриваются вопросы синхронизации баз данных в условиях отсутствия детерминированных запросов. Проведена анализ возможных видов синхронной репликации. Обоснованы условия выбора наиболее предпочтительного варианта, учитывающего условия функционирования распределенной системы управления.

информационное пространство, информационное взаимодействие, информационное хранилище, критерии оценки.

С развитием информационных технологий и ростом объемов обрабатываемой информации во всех сферах деятельности все большую значимость приобретают вопросы, связанные с организацией взаимодействия источников этой информации [1, 2].

К взаимодействующим источникам информации относятся: пресса, радио, телевидение, Интернет и другие международные и национальные информационные системы, информационные службы и штабы федеральной пограничной службы, министерства по чрезвычайным ситуациям, министерства внутренних дел, федеральной службы безопасности, федерального агентства правительственной связи, а также диспетчерские службы. Унифицированный для различных ведомств вариант формирования баз данных, которые предназначены для хранения исходной информации из различных ведомственных источников данных, не лишен недостатков, поскольку системы транзакций различных ведомств гетерогенны и формировались, как правило, по различным паттернам, а также могут содержать в отдельные моменты времени противоречивую и несогласованную информацию, не говоря уже о различных форматах и различных платформах.

Территориальная удаленность структурных подразделений и децентрализованная системы управления требуют векторного подхода к информационному взаимодействию субъектов. Одним из вариантов решения могут стать наборы метаданных, которые теоретически содержат необходимое (для организации межведомственного взаимодействия) подмножество служебной информации из хранилищ данных субъектов (ИХ). В случае возникновения ошибки транзакция может быть легко отменена, а информация восстановлена из ИХ практически без потерь. Цель работы заключается в том, чтобы на основе выделения и обоснования множества свойств, которыми отличаются различные варианты логической организации информационного пространства [3, 4], провести их сравнительную оценку, позволяющую выбрать наиболее предпочтительный вариант, учитывающий условия функционирования распределенной системы. Среди этих свойств ИХ присуще следующие:

1) расширяемость – возможность включения новых или изменения существующих прикладных функций ведомственных информационных систем (ВИС), не затрагивая при этом остальные функциональные подсистемы ВИС;

2) масштабируемость – возможность изменения количественных характеристик (размерность решаемых задач, число обслуживаемых пользователей и т. д.) прикладных программ и локальных баз данных (ЛБД), реализуемых на разных платформах, путем настройки параметров, а не путем перепроектирования;

3) переносимость – возможность перемещения ВИС на другие аппаратно-программные платформы в случае их модернизации или замены с наименьшими затратами (как в части приложений, так и в части данных);

4) интероперабельность – свойство, обеспечивающее взаимодействие ВИС с другими системами при обращении к их информационным или вычислительным ресурсам;

5) интегрируемость – возможность объединения нескольких информационных систем назначения в универсальную систему по семантическому принципу или по геопозиции;

6) безопасность – регулирование полномочий доступа к информационным ресурсам, использования криптографических средств защиты информации, электронно-цифровой подписи на протяжении все жизненного цикла информации в ИХ;

7) бесперебойность – безотказное функционирование ИХ, достигаемое дублирование жизненно важных подсистем;

8) высокая готовность – способность системы принимать и успешно выполнять запросы и задания за доступный интервал времени даже в случае отказа какого-либо компонента путем гарантированного автоматического восстановления работоспособности и сохранения целостности баз данных;

9) версирование – добавление метаданных в ИХ о пользователях, непосредственно осуществивших те или иные операции, ответственных за выполнение работ и т. д.;

10) качество и целостность данных – гарантия полноты, точности, воспроизводимости и целостности данных за счет контроля на этапе их загрузки в ИХ путем выполнения различных проверок.

Системный анализ множества известных вариантов организации ИХ на предмет возможности и целесообразности их использования в качестве архитектурных решений физической плоскости для организации информационного взаимодействия в распределенной системе управления позволил обобщить и конкретизировать следующие возможные варианты организации ИХ [5–7]:

Вариант 1: Виртуальные хранилища данных;

Вариант 2: Независимые витрины данных;

Вариант 3: Централизованное ИХ с системой извлечения, преобразования и загрузки;

Вариант 4: Централизованное ИХ с оперативным складом;

Вариант 5: Централизованное ИХ с оперативным складом, зонами временного хранения и витринами данных;

Вариант 6: Централизованная система извлечения, преобразования и загрузки данных с параллельным центральным ИХ, оперативным складом, зонами временного хранения и витринами данных;

Вариант 7: ИХ с накоплением данных в витринах;

Вариант 8: Центральное ИХ с интеграционной шиной;

Вариант 9: Модульное ИХ.

Результаты сравнительной оценки рассмотренных выше вариантов логической организации информационного пространства представлены в таблице. В качестве основных характеристик ИХ, по которым проводилась сравнительная оценка, были выбраны: возможность внесения изменений в структуру хранилища; достоверность обработки данных; дороговизна (финансовые затраты на закурку и обслуживание оборудования); скорость обработки данных; множественность запросов. Каждый вариант получал одну из следующих оценок по данным характеристикам: «–» - нет возможности или низкая характеристика; «+/–» -среднее значение; «+» - есть возможность или высокая характеристика.

ТАБЛИЦА. Варианты проектирования хранилищ данных

Характеристика хранилища	Вариант 1	Вариант 2	Вариант 3	Вариант 4	Вариант 5	Вариант 6	Вариант 7	Вариант 8	Вариант 9
Внесение изменений в структуру	–	+/–	+	-	+/-	+/-	+/-	+/-	+
Достоверность	+	-	+/-	-	+/-	-	+/-	+/-	+
Дороговизна (закупка и обслуживание)	+	+/-	+	+/-	+/-	+	+/-	+	+/-
Скорость обработки данных	+/-	+/-	+	+	+/-	+/-	+/-	+/-	+/-
Множественность запросов	+/-	-	-	+/-	+/-	+/-	+/-	+/-	+

Анализируя результаты проведенной сравнительной оценки, можно сделать вывод, что наибольшей предпочтительностью обладает вариант 9 – модульное ИХ. Он обеспечивает возможность внесения изменений в структуру, высокую достоверность обработки данных и множественность запросов. Кроме того, он не требует больших финансовых затрат на закупку и обслуживание оборудования и не является критичным к используемым вычислительным ресурсам.

Таким образом, полученные результаты могут быть использованы при проектировании и разработке компонентов информационного взаимодействия в распределенной системе управления, в которой необходимо эффективно обеспечивать обработку разнородных информационных ресурсов.

Список используемых источников

1. Саенко И. Б., Брунилин А. А., Ефимов В. В., Ясинский С. А. Организация информационного взаимодействия разнородных автоматизированных систем: онтологический подход // Информация и космос. 2016. № 2. С. 60–64.

2. Котенко И. В., Федорченко А. В., Саенко И. Б., Кушнеревич А. Г. Технологии больших данных для корреляции событий безопасности на основе учета типов связей // Вопросы кибербезопасности. 2017. № 5 (23). С. 2–16.

3. Михалькевич И. С. Повышение достоверности слабо формализованных данных // Научные записки молодых исследователей. 2014. № 2. С. 17–21.

4. Чайковский Д. В. Информационное пространство: анализ определений // Вестник БГУ. 2010. № 14. С. 269–274.

5. Ладин Е. Г. Семантическая модель хранилища данных по технологическим характеристикам процессов переработки и кондиционирования радиоактивных отходов низкой и средней активности: дис. … канд. техн. наук / Московская Государственная Академия тонкой химической технологии им. М.В. Ломоносова. М.: 2006. 92 с.

6. Точилкина Т. Е., Громова А. А. Хранилища данных и средства бизнес-аналитики: учебное пособие. М.: Финансовый университет, 2017. 161 с.

7. Крылатков П. П., Минеева Т. А. Информационное пространство машиностроительного предприятия // Известия УрГЭУ. 2018. № 5. С. 117–129.

УДК 004.654
ГРНТИ 20.53.17

О ПРОБЛЕМЕ РАЗМЕЩЕНИЯ ИНФОРМАЦИОННЫХ РЕСУРСОВ В ЕДИНОМ ИНФОРМАЦИОННОМ ПРОСТРАНСТВЕ

М. А. Бирюков[1], **А. В. Михайличенко**[2], **В. В. Николаев**[2], **И. Б. Саенко**[2]

[1]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

[2]Военная орденов Жукова и Ленина Краснознаменная академия связи имени Маршала Советского Союза С. М. Буденного

Рассматриваются возможные варианты построения единого информационного пространства и используемые при их построении архитектуры систем хранения данных. Приводится сравнительная характеристика вариантов доступа к информационным ресурсам. Обсуждается постановка задачи оптимального размещения информационных ресурсов в едином информационном пространстве исходя из существующих топологий систем хранения данных.

информационное пространство, системы хранения данных, информационный ресурс.

Одним из перспективных направлений развития единого информационного пространства (ЕИП) является решение проблемы оптимизации размещения информационных ресурсов (ИР) при заданном варианте построения системы хранения данных (СХД). Данная задача подразумевает реализацию такого плана построения процессов хранения информации, который бы обеспечил на существующих средствах вычислительной техники и связи улучшение функциональных характеристик ЕИП в целом без реструктуризации аппаратной составляющей и каналов связи.

В связи с тем, что современные каналы передачи информации в ЕИП ограничены по своей пропускной способности, существенную долю во времени решения задач составляет время передачи информации. В этих условиях целесообразным представляется такое распределение информационных ресурсов по узлам ЕИП, которое бы позволило свести к минимуму объем информации, циркулирующей по каналам связи при решении функциональных задач [1].

Решению данной задачи способствует определение наиболее подходящей топологии СХД. От нее зависит насколько быстро сможет пользователь ЕИП получить доступ к размещенным в ЕИП ресурсам.

В существующих СХД выделяют три варианта подключения устройств хранения информации [2]:

1. DAS (*Direct Attached Storage*) или по-другому SAS (*Server Attached Storage*) – представляет собой архитектурное решение, показанное на рис. 1. Суть его заключается в следующем – подключение файлового хранилища осуществляется напрямую к компьютеру пользователя или к серверу.

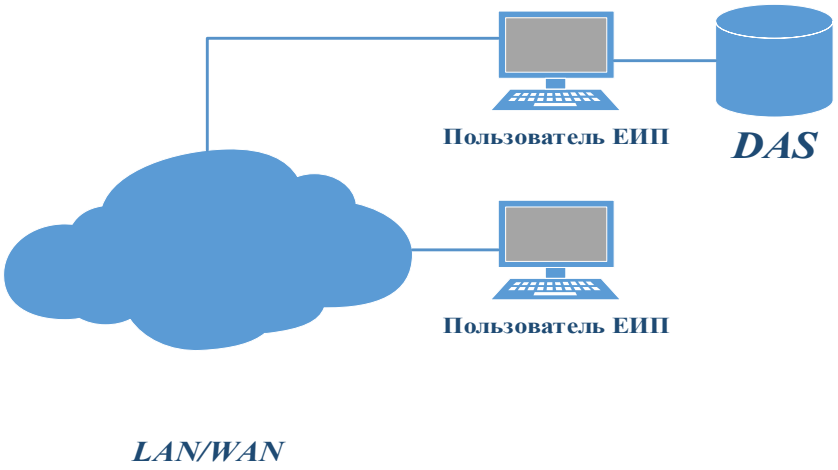


Рис. 1. Архитектурное решение – DAS

У данной архитектуры есть свои плюсы и минусы. Плюсами являются простота использования, то есть администратору сервера не придется прикладывать много усилий для установки, настройки и последующего адми-

нистрирования сервера. В добавок к этому архитектура DAS – это самое дешевое на сегодняшний день архитектурное решение на рынке, обладающее к тому же еще одним преимуществом – высокой скоростью получения информации из файлового хранилища.

В тоже время DAS-системы имеют и свои недостатки, к которым можно отнести:

– низкую надежность – при возникновении проблем в сети или аварии сервера данные становятся недоступны всем сразу;

– высокую латентность, обусловленную обработкой всех запросов одним сервером;

– высокую загрузку сети, часто определяющую пределы масштабируемости;

– плохую управляемость – вся емкость доступна одному серверу, что снижает гибкость распределения данных;

– низкую утилизацию ресурсов – трудно предсказать требуемые объемы данных, у одних устройств DAS может быть избыток емкости, у других ее может не хватать, а перераспределение зачастую невозможно или крайне трудоемко.

2. NAS (*Network Attached Storage*) – это архитектурное решение, при котором доступ к хранилищу данных осуществляется через локальную или глобальную сеть, а само устройство хранения представляет собой одновременно и сервер, и СХД (рис. 2).

NAS-устройства особенно хорошо работают в разнородной среде, когда одновременно идет множество запросов на получение информации из СХД от большого количества пользователей сети. Также, как и DAS-устройства, данная архитектура обладает схожими преимуществами. К ним относятся низкая сложность администрирования такого сервера и низкая рыночная стоимость его установки. Дополнительно к преимуществам можно отнести, то что доступ к таким устройствам могут получать пользователи различных операционных систем [3].

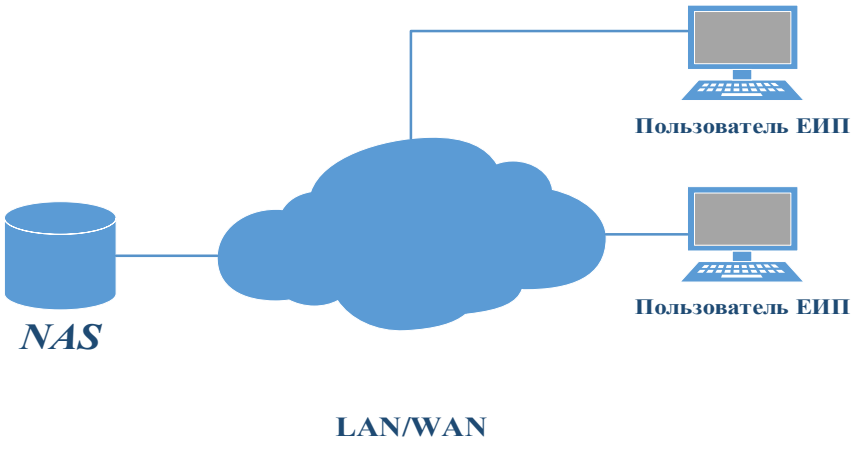


Рис. 2. Архитектурное решение – NAS

К главным недостаткам данного архитектурного решения можно отнести увеличенную нагрузку на сеть, за счет большого количества одновременных запросов и более медленную скорость доступа к информации, связанную с тем что, протоколы сетевых файловых систем зачастую медленнее, чем при использовании DAS-систем.

3. Архитектура SAN (*Storage Area Network*) представляет собой особую сеть, которая выделена из общей глобальной или локальной сети, в которой объединены файловые сервера объединены с серверами приложений (рис. 3).

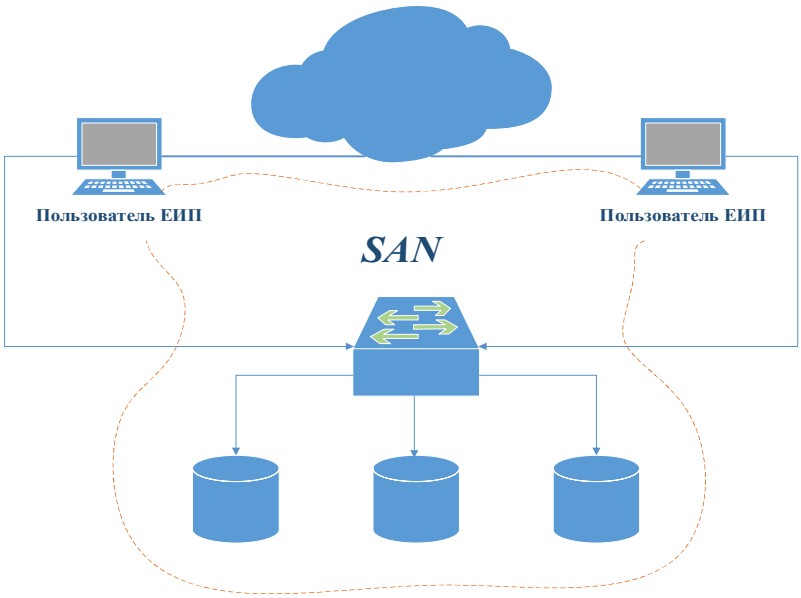


Рис. 3. Архитектурное решение – SAN

В отличии от NAS, SAN не имеет понятия о файлах: файловые операции выполняются на подключенных к SAN серверах. Идеальный результат работы SAN – возможность доступа любого сервера под любой операционной системой к любой части дисковой емкости, находящейся в SAN. Оконечные элементы SAN – это серверы приложений и системы хранения данных. А между ними, как и в обычной сети, находятся адаптеры, коммутаторы, мосты, концентраторы.

К неоспоримым преимуществам данного типа архитектуры относятся: высокая надежность доступа к данным, находящимся на внешних системах хранения; независимость топологии SAN от используемых СХД и серверов; централизованное хранение данных; удобное централизованное управление коммутацией и данными; перенос интенсивного трафика ввода-вывода в отдельную сеть; высокое быстродействие и низкая латентность; масштабируемость и гибкость логической структуры SAN; возможность организации

резервных, удаленных СХД и удаленной системы резервирования и восстановления данных; возможность строить отказоустойчивые кластерные решения без дополнительных затрат на базе имеющейся SAN.

Недостатками являются: более высокая стоимость и сложность настройки элементов системы; более жесткие требования к совместимости и валидации компонентов.

Представленные выше топологические структуры построения СХД соотносятся с возможными вариантами размещения ИР в ЕИП. Так, архитектура DAS – представляет собой децентрализованный вариант организации хранения данных, когда общее хранилище данных отсутствует, а все ИР хранятся распределенным способом у самих пользователей ЕИП [4].

Архитектуры NAS и SAN соответствует централизованному подходу к организации хранения данных, при котором устройства хранения размещены в центре обработки данных (ЦОД) и содержат информацию или ссылки на необходимую информацию, а доступ пользователей ЕИП к ИР осуществляется через сеть.

Оптимальным с точки зрения эффективности использования ИР ресурсов представляется смешанный способ организации построения ЕИП (рис. 4), при котором используются все представленные выше топологии, а ИР частично размещены в ЦОД и частично территориально разнесены и хранятся на файловых серверах пользователей ЕИП [5, 6].

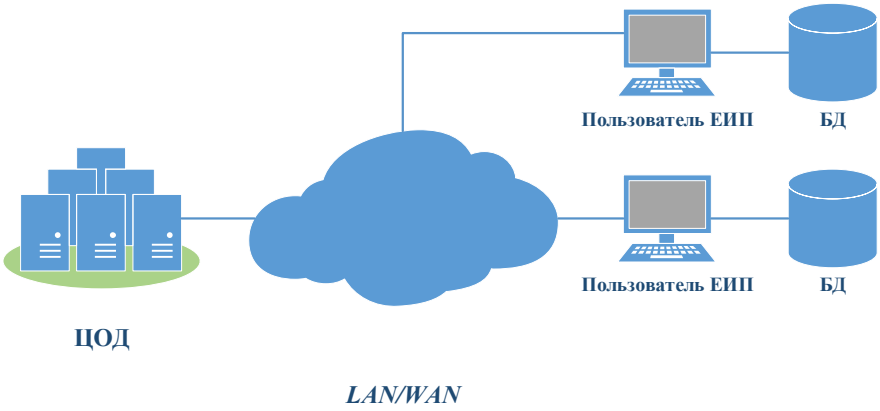


Рис. 4. Смешанный вариант построения ЕИП

При смешанном варианте доступ к ИР можно разделить на доступ к ресурсу, размещенному: в ЦОД, на своем файловом сервере и на чужом файловом сервере. Их сравнительная характеристика в зависимости от выбранных свойств ЕИП представлена в таблице и показывает, что смешанный вариант способен обеспечить необходимый уровень безопасности, устойчивости и оперативности системы, но исключительно при оптимальном размещении самих ИР по местам их хранения.

ТАБЛИЦА 1. Сравнительная характеристика вариантов доступа к ИР

Варианты доступа к информационным ресурсам	Свойства ЕИП		
	Безопасность	Устойчивость	Оперативность
Доступ к ресурсу, находящемуся в ЦОД	средняя	низкая	средняя
Доступ к ресурсу, находящемуся на своем файловом сервере	высокая	высокая	высокая
Доступ к ресурсу, находящемуся на чужом файловом сервере	низкая	средняя	низкая

Таким образом, задача оптимизации размещения информационных ресурсов должна решаться исходя из существующих топологий СХД с учетом выбранного варианта построения ЕИП и максимально возможных значений безопасности, оперативности и устойчивости.

В ходе дальнейших исследований планируется провести анализ существующих методов оптимизации размещения ресурсов и выбрать наиболее подходящий для решения такого рода задач.

Список используемых источников

1. Данилкин Ф. А., Есиков Д. О. Оптимизация распределения информационных ресурсов в вычислительной сети // Инновации в технологиях и образовании: сб. науч. ст. V междунар. науч.-практ. конф., Белово: Изд-во КузГТУ. 2012. Ч. 2. С. 157–159.

2. Vishvanath R, Azra Nasreen. Survey on recent technology of storage area network and network attached storage protocols // International journal of innovative research in electrical, electronics, instrumentation and control engineering. 2014. No. 2. Pp. 1784–1789.

3. Shrivastava A. От хранения данных к управлению информацией / пер. с англ. М. Вильчинского. СПб.: Питер, 2016. 544 с.

4. Куваев В. О., Ефимов В. В., Чечулин А. А., Лыжинкин К. В. Варианты построения единого информационного пространства для интеграции разнородных автоматизированных систем // Информация и космос. 2015. № 4. С. 83–87.

5. Саенко И. Б., Фабияновский И. Н. Оценка и выбор вариантов размещения информационных ресурсов в едином информационном пространстве // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VIII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2019. Т. 2. С. 529–532.

6. Котенко И. В., Саенко И. Б., Макуха А. А., Бирюков М. А. Варианты построения хранилищ данных в едином информационном пространстве с учетом безопасности информации // Информатизация и связь. 2021. № 7. С. 48–55.

УДК 004
ГРНТИ 50.05.15

ОБЗОР МЕТОДОВ УВЕЛИЧЕНИЯ СКОРОСТИ ЗАГРУЗКИ ВЕБ-СТРАНИЦ

М. А. Бирюков, О. А. Якубова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье рассмотрены различные способы оптимизации загрузки HTML страниц. Эти способы были поделены на 4 подхода и расположены в порядке по мере усложнения внедрения в проект.

веб-разработка, оптимизация, скорость загрузки.

Введение

Оптимизация загрузки HTML страниц обеспечивает комфортную работу с сайтом, увеличивает пропускную способность сетей. Сокращаются используемые вычислительные мощности, а значит, уменьшается энергопотребление.

Долгая загрузка страницы повышает вероятность того, что пользователь покинет её, не дождавшись появления контента, понижает её в результатах поиска в поисковых системах. Считается, что оптимальным является время загрузки не более 3 секунд [1].

Разработчики должны знать способы оптимизации и закладывать их ещё на этапе проектирования.

Различные методы уже используются в настоящий момент. Проблема в том, что инструменты веб-разработчиков зачастую не позволяют реализовать эти методы в полном объёме без дополнительных средств.

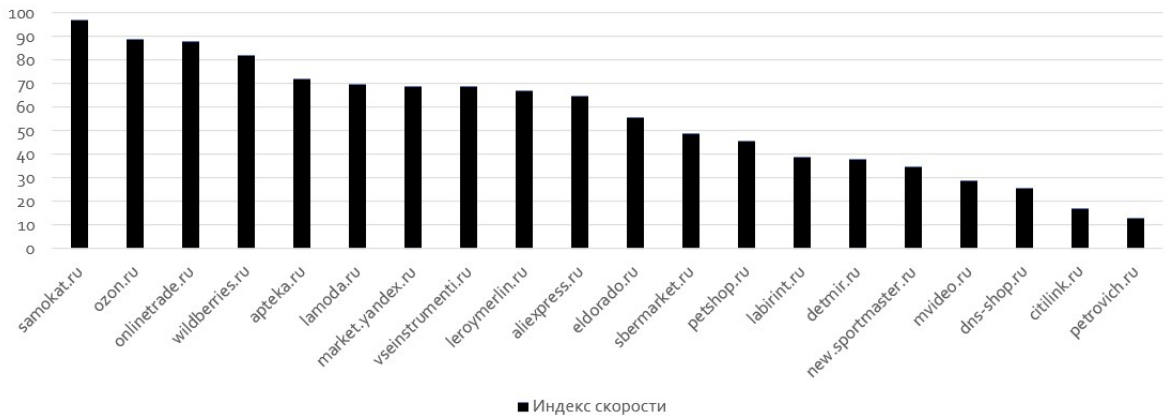


Рис. 1. Индекс скорости по версии PageSpeed Insights (от 14.02.2022)

Для примера были взяты 20 сайтов крупнейших интернет-магазинов. Измерение скорости показало, что 40 % рассмотренных сайтов обладают индексом скорости меньшим, чем 50 (согласно PageSpeed Insights (см. рис. 1)), что означает чрезмерно большое время загрузки [6, 11, 18].

Различные способы оптимизации были поделены на 4 подхода и расположены по мере усложнения процесса внедрения в проект. Эта классификация позволяет выбрать глубину оптимизации ещё на этапе проектирования в зависимости от бюджета и сложности проекта.

Обзор подходов оптимизации

Первый подход – уменьшение размера кода. Чем меньше размер файла, тем быстрее он загружается браузером:

1) Минификация – удаление лишних пробелов, переносов строк и тегов, сокращение имён переменных и т. д. Данный метод поддаётся автоматизации, поэтому в настоящее время существует множество различных онлайн оптимизаторов [3, 8, 10].

2) Удаление комментариев может сделать код менее читаемым и усложнить дальнейшую работу с ним. Чтобы решить эту проблему, достаточно хранить две версии HTML кода: понятную разработчику и оптимизированную [3, 8, 10].

3) Удаление избыточного кода, сокращение. Этот метод зависит от навыков веб-разработчика, создающего HTML код. Практически каждую задачу можно решить несколькими способами, от разработчика требуется выбрать наиболее оптимальный их них [3, 8, 10].

4) Удаление параметров в тегах. Использование стилей вместо параметров позволит браузеру хранить их в виде кэша, а значит, при следующем обращении к сайту они будут браться с локального диска. Кроме того, это опять же уменьшит размер HTML кода [7].

5) Сжатие файлов разными способами.

GZIP – сжатие файла с возможностью полного восстановления. Основан на алгоритме DEFLITE, объединяющем в себе алгоритм LZ77 (замена повторов «ссылками» на первый экземпляр) и алгоритм Хаффмана (ни одно кодовое слово не является префиксом другого). Этот способ не является самым эффективным с точки зрения степени уменьшения размера, зато он поддерживает довольно быструю скорость сжатия и распаковки. По статистике, GZIP используется 53,9 % всех веб-сайтов, а любое сжатие файлов используется 87,5 %. Известные сайты, пользующиеся GZIP, это Google.com, Wikipedia.org, Amazon.com и др. [2, 20].

Обфускация – преобразование исходного кода в нечитаемый вид с сохранением функционала. Обычно этот метод используют, чтобы защитить исполняемый код от декомпиляции, скрыть уязвимости, которыми могли бы

воспользоваться злоумышленники. Однако, в некоторых случаях он способен уменьшить размер исполняемого кода и ускорить работу [4].

6) Уменьшение разрешения и качества растровых изображений. Чем больше размер изображения, тем больше времени оно требует на загрузку. Поэтому следует уменьшать непосредственно размер самого изображения, а не размер его отображения [3, 8, 10].

Более того, полезно использовать современные форматы изображений, векторную графику и Canvas – элемент HTML, позволяющий создавать графические объекты с помощью языка программирования. Этот метод поддерживают многие браузеры. С ним нужно работать осторожно, так как можно наоборот понизить скорость загрузки веб-сайта [9].

7) Отказ от использования (или минимизация – только те буквы, которые используются) нестандартных (дизайнерских) веб-шрифтов. Есть шрифты, которые с наибольшей степенью вероятности поддерживаются операционной системой, а значит, их не нужно подключать отдельными файлами, например, Arial, Helvetica, Courier New и т. д. [14].

Второй подход – уменьшение времени ответа сервера:

1) Кэширование на стороне сервера, когда клиенту отдаётся статичная копия динамической страницы, а не собирается при каждом запросе.

2) Уменьшение количества переадресаций, если это возможно (например, перенастройка CMS, или системы управления контентом сайта) [3, 8, 10].

3) Уменьшение расстояния между сервером и клиентом.

4) CDN – система серверов, распределённых в различных географических точках, позволяющая сократить время получения ответа пользователю сайта, так как происходит взаимодействие с ближайшим сервером [12].

5) Оптимизация серверных скриптов, написанных на разных языках программирования, в т. ч. PHP, Python, Java и т. д. Написание качественного, корректного и адекватного кода (увеличение скорости работы исполняемых файлов). Скорость работы серверных скриптов может зависеть от таких факторов как мощность оборудования, версии операционной системы, корректности настроек сервера, например, интерпретатора (для php, Python, java и т д), mySQL, Nginx, Apache и т. д.

6) Повышение вычислительной мощности используемого сервера.

Третий подход – уменьшение времени до отображения контента на странице:

1) Загрузка только того контента, который находится в видимой области, остальное подгружается по мере пролистывания страницы (Lazy Load), использование асинхронных запросов [13, 17].

2) Разделение CSS, JavaScript и HTML фрагментов на те, что должны загрузиться в первую очередь, и те, что позже. Сделано для того, чтобы

пользователь мог читать текст ещё до полной загрузки контента на странице. Размещение CSS и JavaScript, которые должны грузиться в первую очередь, непосредственно в коде страницы [3, 8, 10].

3) Уменьшение количества HTTP-запросов до загрузки видимой части страницы. Избегание использования @import в коде CSS. Объединение файлов CSS и файлов JavaScript [3, 8, 10].

4) Использование только быстрых CSS-анимаций (Иногда это позволяет реализовывать сложные анимации с помощью кода, небольшого по объёму.) [15].

5) Отказ от использования загрузки файлов (CSS, JavaScript, изображений и т. д.) со сторонних ресурсов, либо кэширование их в целях уменьшения количества DNS-запросов [3, 8, 10].

6) Keep-Alive – режим, при котором скачивание файлов происходит через одно TCP соединение, а не через несколько HTTP запросов [21].

Четвёртый подход – Современные способы реализации взаимодействия с сервером:

1) Использование принципа Single-page application – создания одностраничного приложения, не требующего перезагрузки страницы для обновления контента [5].

2) REST API – правила обмена данными между сервером и клиентом [19].

Оценка методов

Как было сказано ранее, для исследования мы взяли 20 сайтов крупнейших интернет-магазинов. Были рассмотрены различные характеристики их загрузки. Оказалось, что часто разработчики используют только часть возможностей для оптимизации, но при этом игнорируют другие. Например, только 25% HTML кода занимали менее чем 40 строк и были лишены хотя бы некоторой части необязательных
пробелов, переносов и комментариев.

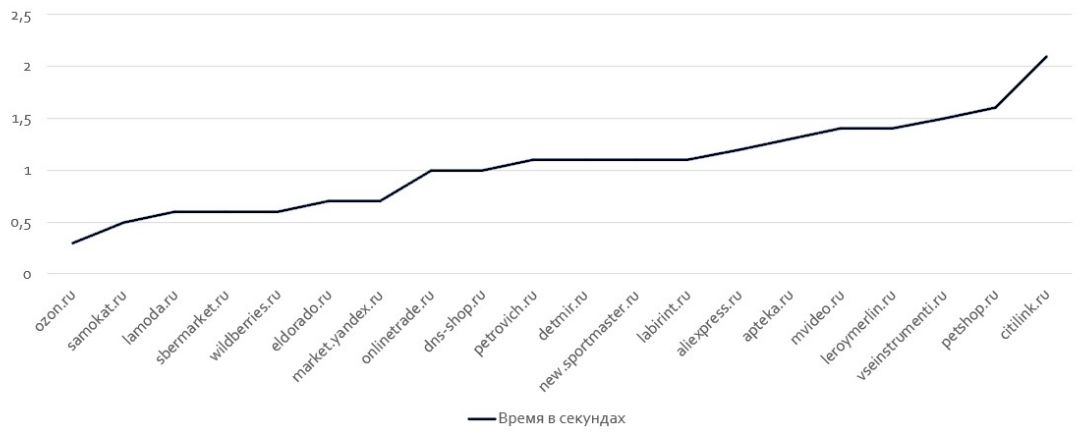


Рис. 2. Время загрузки первого контента

Из графика «Время загрузки первого контента» (рис. 2) видно, что есть сайт, который загружает первый контент менее, чем за 0,5 секунды. Остальные сайты делают это дольше, например, крайний правый за 2 секунды.

Стоит учитывать, что каждый проект отличается деталями реализации, поэтому некоторые подходы оптимизации в нём реализовать легче, чем другие.

Вывод

На современном этапе развития технологий не существует универсального оптимизатора веб-страниц. В дальнейшем возможно создание алгоритма автоматической оптимизации, использующего некоторые из этих методов в комбинации. Это перспективный предмет дальнейшей научной работы.

Зная о существовании этих подходов, разработчик может найти новые возможности для оптимизации проекта, над которым он работает.

Список используемых источников

1. Зачем нужна оптимизация загрузки сайта: WEBCodius. URL: https://webcodius.ru/seo/zachem-nuzhna-optimizaciya-zagruzki-sajta.html (дата обращения: 14.02.2022).

2. Буханов П. Ю., Смирнов Д. М., Хан Г. Г., Бирюков М. А. Обзор методов шифрования // В сб.: Региональная информатика и информационная безопасность. 2017. С. 58–60.

2. Как работает сжатие GZIP // Хабр (habr.com). URL: https://habr.com/ru/post/221849/ (дата обращения: 14.02.2022).

3. Как сделать сайт быстрее // Вебмастер. Справка (yandex.com). URL: https://yandex.com/support/webmaster/yandex-indexing/page-speed.html (дата обращения: 14.02.2022).

4. Методы и средства обфускации программ (stud.wiki). URL: https://stud.wiki/ programming/2c0a65625a2bc78b5c53b88421306d36_0.html (дата обращения: 14.02.2022).

5. Одностраничные Приложения: Плюсы и Минусы // Purrweb. URL: https://www.purrweb.com/ru/blog/odnostranichnye-prilozheniya-polnyj-gid-po-razrabotke/ (дата обращения: 14.02.2022).

6. Особенности Google PageSpeed: улучшение оценки сайта и его рейтинга в поиске // Хабр (habr.com). URL: https://habr.com/ru/company/ruvds/blog/462005 (дата обращения: 14.02.2022).

7. Преимущества стилей | HTMLbook.ru. URL: http://htmlbook.ru/samcss/preimushchestva-stiley (дата обращения: 14.02.2022).

8. Рекомендации Google по оптимизации скорости загрузки сайтов // Т-Дизайн (t-design.ru). URL: https://www.t-design.ru/faq/rekomendatsii-google-po-optimizatsii-skorosti-zagruzki-sajtov.html (дата обращения: 14.02.2022).

9. Руководство по Canvas // Интерфейсы веб API | MDN (mozilla.org). URL: https://developer.mozilla.org/ru/docs/Web/API/Canvas_API/Tutorial (дата обращения: 14.02.2022).

10. Топ-10 советов о том, как увеличить скорость загрузки страницы // Хабр (habr.com). URL: https://habr.com/ru/post/137239/ (дата обращения: 14.02.2022).

11. ТОП-100 2020 (datainsight.ru). URL: https://www.top100.datainsight.ru/ (дата обращения: 14.02.2022).
12. Что такое CDN и как это работает? // Хабр (habr.com). URL: https://habr.com/ru/company/selectel/blog/463915/ (дата обращения: 14.02.2022).
13. AddyOsmani.com – Native image lazy-loading for the web! URL: https://addyosmani.com/blog/lazy-loading/ (дата обращения: 14.02.2022).
14. CSS: Стандартные (безопасные) шрифты (puzzleweb.ru). URL: https://puzzleweb.ru/css/6_fonts3.php (дата обращения 14.02.2022).
15. CSS-анимации (javascript.ru). URL: https://learn.javascript.ru/css-animations (дата обращения: 14.02.2022).
16. How Loading Time Affects Your Bottom Line (neilpatel.com). URL: https://neilpatel.com/blog/loading-time/ (дата обращения: 14.02.2022).
17. Lazy Load — отложенная загрузка изображений. Категория: Web-разработка • JavaScript и jQuery (tokmakov.msk.ru). URL: https://tokmakov.msk.ru/blog/item/30 (дата обращения: 14.02.2022).
18. PageSpeed Insights (web.dev). URL: https://pagespeed.web.dev/ (дата обращения: 14.02.2022).
19. REST API: что это такое простыми словами, примеры запросов (skillfactory.ru). URL: https://blog.skillfactory.ru/glossary/rest-api/ (дата обращения: 14.02.2022).
20. Usage Statistics of Gzip Compression for Websites, February 2022 (w3techs.com). URL: https://w3techs.com/technologies/details/ce-gzipcompression (дата обращения 14.02.2022).
21. What is Keep-Alive? – Articles for Developers Building High Performance Systems (stackpath.com). URL: https://blog.stackpath.com/glossary-keep-alive/ (дата обращения: 14.02.2022).

УДК 62-91
ГРНТИ 49.33.29

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ ФРАГМЕНТА МУЛЬТИСЕРВИСНОЙ СЕТИ СВЯЗИ ДЛЯ ОЦЕНКИ ЭФФЕКТИВНОСТИ ИСПОЛЬЗОВАНИЯ ЕЕ РЕСУРСОВ

К. Б. Боброва, И. В. Захаров, М. А. Сахарова

ЗАО «Институт телекоммуникаций»

В условиях развития мультисервисных сетей связи (МСС) следующего поколения, способных предоставить доступ к услугам для различных потребителей, обеспечение требуемого качества обслуживания является нетривиальной задачей. Даже частные решения поставленной задачи для разного типа передаваемых данных являются актуальными и востребованными.

Авторами разработаны модели, позволяющие рассчитать и спрогнозировать эффективность функционирования МСС с учетом накладываемых ограничений. В статье представлена разработанная математическая модель оценки эффективности использования ресурсов МСС в зависимости от характеристик используемых каналов передачи данных.

Результат моделирования позволил получить вероятностно временные характеристики (ВВХ), необходимые для успешной доставки при различных условиях работы сети.

мультисервисные сети связи, математическая модель, эффективность, ресурсы сети, вероятностно временные характеристики.

В современных МСС происходит непрерывная смена и модернизация технологий. Стоит отметить, что смена технологической базы не может происходить мгновенно в силу инертности операторов связи и потребителей, а также экономических факторов. Таким образом МСС могут иметь принципиальные различия в архитектуре и характеристиках на различных участках сети [1]. Кроме того, появляются новые потребители услуг сетей связи, такие как разнородные сенсоры, беспилотные аппараты, устройства промышленного и медицинского назначения, аппаратура виртуальной реальности и др.

Появление новых потребителей влечет за собой расширение и уточнение спектра предоставляемых услуг, как правило, все более требовательных к качеству сетевых сервисов, например, аудио и видео трансляции в реальном времени; телеметрия беспилотных аппаратов; датчики жизнеобеспечения медицинского оборудования; управление узлами программно-определяемых сетей и группами беспилотных летательных аппаратов и т. д.

В таких условиях развитие МСС, способных предоставить доступ к услугам для различных потребителей и обеспечить требуемое качество обслуживания, является нетривиальной задачей. Для решения подобной задачи особое значение приобретают модели, позволяющие рассчитать и спрогнозировать эффективность функционирования МСС с учетом накладываемых ограничений.

Использование различных технологий связи определяет требования к топологическим характеристикам МСС, которые зависят от свойств каналов и требований к показателям качества обслуживания трафика. Исходя из этого была сформирована задача по определению вероятности успешной передачи сообщения при определенных параметрах сети. В данном контексте была рассмотрена следующая система:

1) Объект системы – пакетная МСС с топологией типа «точка-точка»;

2) Субъект системы – лицо, принимающее решения, согласовавшее предельное время доставки;

3) Предмет системы – время процесса доставки сообщения;

4) Внешняя среда – элементы, участвующие в доставке сообщения, исключая объект и субъект;

5) Цель системы – доставка сообщения с заданными показателями *QoS*.

Моделируемый участок сети, состоит из двух граничных устройств доступа – генератора (автоматизированное рабочее место оператора или система управления) и потребителя данных (управляемый технологический процесс). Пошаговая декомпозиция процесса передачи сообщения на выбранном участке сети позволила выделить основные подпроцессы его функционирования. Были определены параметры исследуемого процесса и условия функционирования рассматриваемого участка сети. Для решения поставленной задачи разработан граф состояний рассматриваемого участка МСС (рис. 1) и определены средние значения времени их реализации, приведенные в таблице.

ТАБЛИЦА. Основные подпроцессы функционирования исследуемого участка сети

Обозначение	Состояние	Среднее время Δt, мс
S_1	Подготовка команды на управление	0,03
S_2	Определение интерфейса/маршрута передачи	0,1 или 5
S_3	Оценка доступных каналов передачи	0,2
S_4	Передача в радиоканал	0,125
S_5	Сигнал не достиг приемника	0
S_6	Воздействие помех при передаче	1,5
S_7	Разрыв соединения / маршрута	1,5
S_8	Доставка сообщения до приемника	0,1
S_9	Верное выделение сигнала канального уровня	0,125
S_{10}	Перегрузка узла (входного буфера)	0,2
S_{11}	Проверка имитовставки	0,01
S_{12}	Доведение до потребителя	0,12
S_{13}	Квитирование	2

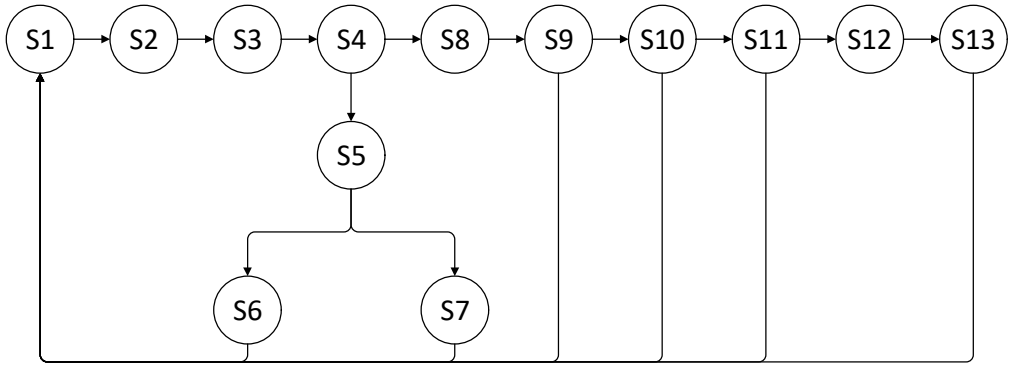


Рис. 1. Граф состояний рассматриваемого участка МСС

С помощью топологического преобразования [2, 3] получены вероятностно-временные характеристики исследуемого участка МСС, в том числе функция распределения (ФР) времени доведения сообщения при изменении вероятности переполнения входного буфера принимающего устройства (P_o) и времени поиска маршрута (t). Полученные результаты представлены на рис. 2 и 3.

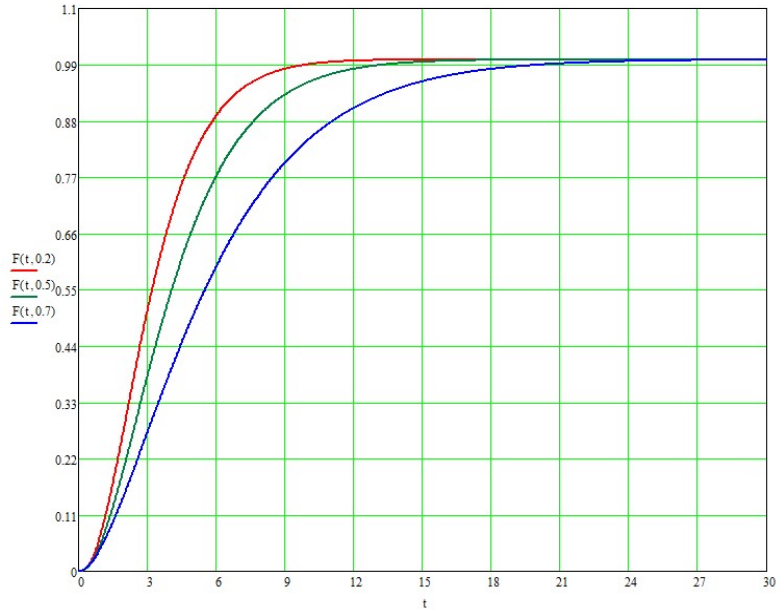


Рис. 2. ФР времени передачи сообщения по исследуемому участку сети при изменении значений P_o = 0.2, 0.5, 0.7 и t = 0,1 мс

Рис. 3. ФР времени передачи сообщения по исследуемому участку сети при изменении значений P_o = 0.2, 0.5, 0.7 и t = 5 мс

Анализ полученных результатов позволяет сделать ряд выводов.

С увеличением вероятности переполнения входного буфера приемного устройства снижается вероятность успешного доведения сообщения при одном и том же времени доведения. Так, например, для t = 5 мс, и требуемом времени доведения t_d = 30 мс вероятность успешного доведения $F(P_o)$ составит: $F(0.2) = 0.95$, $F(0.5) = 0.85$, $F(0.7) = 0.66$.

При выполнении требования успешного доведения сообщения ($F \rightarrow 1$) время доведения вырастает с увеличением вероятности переполнения входного буфера приемного устройства. Так, например, для t = 5 мс, и требуемой вероятности успешного доведения $F(P_o)$ = 0,99 среднее (минимальное) время составит: $t_d(0.2) = 45$ мс, $t_d(0.5) = 68$ мс, $t_d(0.7) = 120$ мс.

Полученная модель позволяет прогнозировать изменение среднего времени доведения сообщения в зависимости от характеристик используемых каналов передачи данных. Например, увеличение вероятности переполнения входного буфера принимающего устройства на величину $\Delta P_o = 0.5$ приведет к увеличению среднего времени успешного доведения сообщения на 90 мс.

С другой стороны, изменение среднего времени доведения сообщения до получателя может быть использовано для отслеживания эффективности использования ресурсов участка сети МСС. Например, увеличение среднего времени доведения сообщения может сигнализировать о необходимости принятия мер по снижению вероятности переполнения входного буфера приемного устройства. К таким мерам могут быть отнесены: замена устройства на более производительное, применение иной политики управления потоками данных и т. д.

Список используемых источников

1. Захаров И. В., Сахарова М. А. Подход к обеспечению доставки приоритетного трафика в мультисервисных сетях с высоким уровнем загрузки // СПБНТОРЭС: Труды ежегодной НТК. СПб.: ООО «Триста точек», 2019. С. 182–185.

2. Привалов А. А. Метод топологического преобразования стохастических сетей и его использование для анализа систем связи ВМФ. СПб.: ВМА, 2000. 166 с.

3. Pritsker A. A. B GERT: Graphical Evaluation And Review Technique. Санта-Моника, США : Whiley, 1966. 24 p.

УДК 004.056
ГРНТИ 81.93.29

ИНСТРУМЕНТЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ IP-ТЕЛЕФОНИИ

М. Э. Богомаз, Л. А. Михайлова, А. В. Поляничева

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Актуальность статьи обусловлена преимуществами использования IP-телефонии в качестве инструмента усовершенствования сети передачи данных на предприятии, и как следствие, возрастающей необходимостью защиты информации от несанкционированного доступа и утечек в сетях VoIP. В статье будут рассмотрены некоторые инструменты обеспечения безопасности, которые разработаны для защиты информации в технологии IP-телефонии. В результате работы над статьей осуществлено сравнение перспективных и эффективных методов защиты сетей IP-телефонии, на основе которого представлены рекомендации по обеспечению безопасности в среде VoIP.

телефония, безопасность IP –телефонии, Voice over IP, VPN, IPsec.

IP-телефония – это современная удобная технология передачи голосового трафика с помощью беспроводных интернет-каналов. Эта технология не требует наличия проложенных телефонных линий, а также АТС для офиса. IP-телефония позволяет осуществлять и принимать вызовы со многих устройств связи, например, с ПК, смартфона либо ноутбука. К преимуществам также можно отнести низкую стоимость, что позволяет поставщикам связи предлагать абонентам выгодные тарифные планы.

В связи с широким распространением этой технологии актуальным является вопрос обеспечения безопасности VoIP. Очевидно, что иметь надежный набор инструментов защиты и предупреждения атак необходимо для успешной работы любой системы [1]. Рассмотрим некоторые способы, которые позволяют обеспечить защиту IP-телефонии.

- Использование зашифрованных VPN-туннелей.

Для обеспечения защиты системы с VoIP можно использовать подключение удаленных пользователей с помощью виртуальных частных сетей (VPN) [2]. В случае перехвата пакетов, которые отправлены по шифрованным VPN-туннелям, их содержание будет доступно только тем пользователям, которые владеют ключом шифрования. Однако имеются недостатки, которые ограничивают применение этой технологии, например, ухудшение качества связи, вызванное задержками, создаваемыми шифрованием; усложнение структуры сети; возрастающая нагрузка на оборудование и каналы связи.

- Применение IPsec.

IPsec является набором служб безопасности на уровне IP и дает системе возможность определения протоколов безопасности, а также использования криптографических ключей. IPsec обеспечивает защиту пакетов SIP и RTP [3], которые проходят через сетевой уровень модели OSI.

- Применение протокола TLS.

Протокол TLS обеспечивает защищенность от подслушивания и порчи либо подделки сообщений. Версия TLS 1.0 известна как SSL – Secure Socket Layer 3.1. Протокол обеспечивает безопасность SIP пакетов на транспортном уровне модели OSI.

- Применение SRTP.

SRTP обеспечивает конфиденциальность, аутентификацию сообщений и защиту от повтора. Возможно использование для обеспечения защиты пакетов RTP на транспортном уровне модели OSI.

Для определения более актуального подхода к защите IP-телефонии осуществим сравнение описанных выше способов обеспечения безопасности [4]. Результаты сравнения приведены в таблице.

ТАБЛИЦА. Сравнение IPSec и SRTP+TLS

Параметр	IPsec	SRTP+TLC
Сложность реализации	Высокий уровень сложности	Низкий уровень сложности
Время смены ключей сеанса, мс	26	1,3
Размер пакета, байт	270	254
Полоса пропускания, кбайт/с	107	101, 5
Управление сетью	Заголовки пакетов скрыты	Заголовки пакетов открыты
Сокрытие топологии	Есть	Нет

С точки зрения сложности реализации, TLS интегрировать с SIP проще, чем IPsec. При этом к реализации TLS предъявляется примерно 200 требований RFC, а к IPsec предъявляется более 500 требований, которые описаны в 11 RFC.

Сравнивая время, необходимое для осуществления изменения ключей [5], можно заметить, что у IPsec на это затрачивается в 20 раз больше времени, чем у TLS. Это не будет являться проблемой для единичного изменения, но с точки зрения одновременной замены ключей у тысячи устройств нельзя считать этот метод эффективным.

С точки зрения сетевого управления и обслуживания, большое преимущество SRTP заключается в открытости заголовков UDP и RTP пакетов для

технического персонала. IPsec шифрует заголовки, таким образом скрывая эту информацию [6].

В сокрытии топологии сети IPsec имеет преимущества перед TLS и SRTP, так как способен инкапсулировать первоначальный заголовок. У TLS и SRTP такая опция отсутствует, поэтому для ее обеспечения необходимо внешнее NAT-устройство.

С точки зрения шифрования разница в обеспечении безопасности несущественна, так как протоколы используют схожие методы шифрования.

В результате сравнения применения IPsec и связки TLS+SRTP [7] для обеспечения безопасности VoIP, рекомендуется, чтобы при планировании организации сети разработчики применяли TLS и SRTP. Реализация внедрения и поддержка этой связки проще и доступнее, а также она является более выгодной с точки зрения использования полосы пропускания, чем IPsec. Существенного преимущества в обеспечении защиты с помощью IPsec, в сравнении с TLS и SRTP, нет. Такое заключение получено на основе анализа действующих стандартов, текущих версий TLS и SRTP у вендоров VoIP и научно-ориентированных реализаций IPsec.

Список используемых источников

1. Полугина Ю. К. Угрозы безопасности VoIP // Региональная ифнорматика и информационная безопасность: сб. науч. тр. / Изд-во Санкт-Петербургского общества информатики, вычислительной техники, систем связи и управления, 2017. С. 231–234.

2. Балашов Д. Безопасность VoIP // Технологии и средства связи. 2013. N 4. С. 38–40.

3. Коптев Д. С., Шевцов А. Н., Щитов А. Н. Анализ работы протокола защиты сетевого трафика на IP-уровне (IPsec) // Наука и современность. 2016. № 3. С. 133–142.

4. Алексеев А. С., Сокол Д. С. Обеспечение защищенности VoIP // Вестник современных исследований. 2019. № 3.3. С. 4–8.

5. Ковцур М. Протоколы обеспечения безопасности IP-телефонии // Первая миля. 2012. № 5. С. 18–27.

6. Бельтриков Ю. Н., Коробко А. Ю. Протокол IPsec: использование российских стандартов шифрования // Известия ТРТУ. 2003. № 4. С. 282–285.

7. Бордашевич Е. А. Сравнение протоколов IPsec и TLS для использования в системах интернета вещей // Современная школа России. Вопросы модернизации. 2021. № 3-1. С. 252–254.

Статья представлена заведующим кафедрой ЗСС СПбГУТ кандидатом технических наук, доцентом А. В. Красовым.

УДК 339.13
ГРНТИ 06.81.12

КОНЦЕПЦИЯ РЕИНЖИНИРИНГА БИЗНЕС-ПРОЦЕССОВ ФРАНЧАЙЗИ ПРОИЗВОДИТЕЛЯ ОТЕЧЕСТВЕННОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

М. А. Богомолова, А. И. Казенкин

Поволжский государственный университет телекоммуникаций и информатики

Современные инструменты управления бизнесом, среди которых выделяется реинжиниринг бизнес-процессов, позволяют перестроить процессы компании для ускорения технических процедур, снижения затрат, введения корпоративной культуры. В условиях перехода на отечественное ПО этот инструмент особенно актуален для оптимизации деятельности партнерских организаций, работающих под единой маркой «1С:Франчайзинг», получивших подтверждение вендора о предоставлении качественных услуг по автоматизации с помощью программных продуктов 1С.

реинжиниринг бизнеса, реинжиниринг бизнес-процессов, 1С:Франчайзи, 1С, облачные программные продукты.

В новых рыночных условиях для современных компаний актуальной становится оптимизация деятельности с помощью метода, который авторы [1] назвали реинжинирингом бизнес-процессов (БПР). В отличие от статистического управления БПР становится возможным благодаря применению новых способов, методов и приемов управления компанией – в частности, путем использования новых информационных технологий [2].

В качестве объекта исследования рассмотрим компанию, являющуюся официальным партнером Фирмы «1С», крупного производителя и поставщика отечественного программного обеспечения. Имеет статус 1С:Франчайзи, занимается продажей и внедрением программных продуктов 1С, а также их доработкой в связи с потребностями заказчиков.

В последние годы компания не отличалась передовыми позициями на рынке 1С:Франчайзи, при этом эффективность деятельности стала снижаться, затраты увеличиваться, а прибыль сокращаться. При этом увеличилась текучесть кадрового состава: средняя продолжительность работы в компании ранее составляла 5 лет, однако за последние 3 года она снизилась до двух и сравнялась со среднестатистическим в данной отрасли. Найм высококвалифицированных специалистов, исходя из финансовых оборотов компании, стал невозможен.

Указанные проблемы оказывали отрицательное влияние на введение в работу новых передовых технологий и сервисов «1С», позволяющих как

удерживать компанию на актуальных позициях рейтинга, так и двигаться вперед. В этой связи владельцами бизнеса было принято решение принять на работу нового сотрудника и назначить его на должность директора по развитию, наделив полномочиями руководителя. Его основной задачей являлся БПР компании с целью повышения показателей эффективности деятельности. Временным промежутком оценки работы был назначен календарный год, с последующим аналогичным периодом для оценки стабильности работы компании с внедренными изменениями.

По результатам осуществленного анализа бизнес-процессов компании были выделены следующие направления БПР, а именно:

– реорганизация кадровой политики и кадрового состава;

– организация комплексных мер по повышению квалификации сотрудников, а также формирования навыков, способствующих их взаимозаменяемости;

– организация эффективного взаимодействия с клиентами;

– установление контроля за качеством оказываемых услуг, а также за сохранностью клиентской базы;

– выявление нерентабельных направлений деятельности организации;

– разработка нового подхода к выполнению плановых годовых показателей компании с целью повышения ее рейтинга и репутации.

По каждому из указанных направлений в ходе БПР были применены типовые способы и приемы перепроектирования бизнес-процессов, в том числе с использованием двух групп новых информационных технологий: упрощающих проведение БПР и порождающих новые бизнес-процессы. Например, облачная АТС, облачные программных продукты «1С», включение сервисов в тарифные планы на информационно-технологическое сопровождение.

1) Было принято решение о проведении аттестации и проверки соответствия занимаемым должностям с учетом требований стандарта информационно-технологического сопровождения Фирмы «1С». Треть команды компании не прошли аттестацию и не изъявили желания дальнейшего повышения своей квалификации. Проведя качественный отбор на вакантные должности, взамен 7 уволенных было принято 3 новых специалиста возрастом, не превышающим 35 лет, имеющих профильное образование.

2) В связи с проведенной реорганизацией кадрового состава возник вопрос взаимозаменяемости специалистов компании. Ранее повышение квалификации осуществлялось в стихийном порядке. Было принято решение о плановом повышении квалификации и еженедельно проводимых в коллективе тренингах.

3) Одним их ключевых требований компании 1С:Франчайзи является качество оказываемых клиенту услуг. Ранее в компании использовались 2 канала связи, а именно проводные телефоны, установленные в офисе, и

мобильные корпоративные телефоны. В этой связи было принято решение на замену средств связи за счет использования облачной АТС с возможностью записи разговоров специалистов. Спустя 2 месяца работы в новом режиме появились первые положительные результаты. Главным достоинством облачной телефонии стала возможность коррекции общения сотрудников компании с клиентами и объективный разбор сложных ситуаций, недоразумений и немногочисленных конфликтов.

4) Проведенный новым руководителем аудит, выявил нерентабельное направление деятельности компании – «1С-Клуб программистов». Проанализировав рынок по данному направлению и финансовые результаты работы было принято решение о прекращении дальнейшего финансирования проекта.

5) Компания 1С-Франчайзи на постоянной основе подвергается тщательному контролю за показателями работы со стороны разработчика – Фирмы «1С». Ранее стратегия компании строилась на количественном подходе в заключении договоров информационно-технологического сопровождения (ИТС) продуктов 1С. Проанализировав предъявляемые требования, одной из основных задач компании наряду с договорами на ИТС, стали продажи «сервисов». В результате были модернизированы все предлагаемые к покупке тарифные планы на ИТС, в состав в обязательном порядке включены необходимые сервисы, состав сервисов варьировался исходя из потребностей клиентов, тем самым помимо выполнения плановых финансовых показателей обеспечивалась и полнота предлагаемых услуг.

Несмотря на пересмотр тактических целей, организации требовались новые идеи, позволяющие расширить спектр предоставляемых услуг и, тем самым, повысить прибыльность и рентабельность. Таким решением стало введение в прайс компании облачных программных продуктов «1С».

Таким образом, осуществлённый комплексный подход БПР позволил добиться высоких показателей и вывести организацию на новый уровень развития. Кадровые изменения способствовали увеличению уровня заработных плат, что стабилизировало ситуацию с текучестью кадров. Рентабельность бизнеса за планируемый срок увеличилась на 30 %, что говорит о правильности выбранной стратегии. Помимо финансовых показателей, увеличился рейтинг компании среди компаний-франчайзи, что позволило поднять доверие со стороны потенциальных клиентов и, как следствие, получать больше заявок с сайта Фирмы «1С». Данный пример успешной модели БПР может быть использован партнерскими компаниями, работающими под единой маркой «1С:Франчайзинг» для сохранения высоких стандартов качества в работе и предоставлении квалифицированных услуг по обслуживанию пользователей системы «1С».

Список используемых источников

1. Хаммер М., Чампи Дж. Реинжиниринг корпорации: манифест революции в бизнесе. СПб.: Изд. СПбГУ, 1997. 328 с.

2. Димов Э. М., Маслов О. Н., Скворцов А. Б. Новые информационные технологии: подготовка кадров и обучение персонала. Ч. 1. Реинжиниринг и управление бизнес-процессами в инфокоммуникациях. М.: ИРИАС, 2005. 386 с. ISBN 5-93592-013-1.

УДК 004.85
ГРНТИ 28.23.25

РАЗРАБОТКА ПРИЛОЖЕНИЯ ВИРТУАЛЬНОЙ РЕАЛЬНОСТИ «VR-PROJECTION» ДЛЯ ОБУЧЕНИЯ ВОЖДЕНИЮ

М. А. Богомолова, К. А. Ушаков

Поволжский государственный университет телекоммуникаций и информатики

Предлагается проект разработки новой методики обучения вождению на основе создания программного обеспечения с использованием технологии виртуальной реальности. В рамках проекта планируется спроектировать тренировочные маршруты, представленные средствами интерактивной визуализации виртуальных объектов, а также создать новую систему оценивания приобретенных навыков.

приложение виртуальной реальности, обучение вождению, виртуальная реальность, шлем виртуальной реальности, очки виртуальной реальности.

Виртуальная реальность – это технология, которая позволяет заменить реальную жизнь на восприятие виртуальной жизни, искусственным образом стимулируя наши чувства и обманывая наше тело в принятии другой версии реальности [1]. Сегодня данная технология применяется в том числе и в сфере обучения вождению. Например, активно используются компьютерные симуляторы вождения, которые представляют движение транспортного средства в реальном времени от первого лица, и объединяют в себе как программные, так и аппаратные средства. Но на данный момент рынок в сфере компьютерных симуляторов вождения неактивен. Ранее это направление развивала компания Samsung, но проект в итоге был приостановлен.

В связи с этим предлагается разработать программное приложение, которое на основе использования технологии виртуальной реальности улучшит погружение в симуляцию [2]. Обучение вождению будет организовано

в форме видеоигры. В зависимости от качества прохождения выданных заданий обучающемуся будут присуждаться звезды (от одной до трех). Уровни можно пройти заново для формирования требуемых умений и навыков перед выездом на автодром.

Целью выполнения проекта является разработка новой методики обучения вождению на основе создания программного обеспечения с использованием технологии виртуальной реальности «VR-projection».

Таким образом, автошколы будут иметь возможность сократить использование реальных транспортных средств при обучении вождению, сократить расходы на их обслуживание, что позволит снизить выброс вредных веществ, а также повысить безопасность обучения. Обучающиеся смогут приобрести опыт управления транспортным средством перед реальной практикой на автодроме и снизить уровень страха сесть за руль реального транспортного средства.

Задачи по проекту:

– сбор и анализ требований для разработки приложения виртуальной реальности;

– консультация со специалистами и сбор данных для компьютерного моделирования внутри приложения;

– разработка архитектуры приложения;

– разработка пользовательского интерфейса приложения.

Перечень необходимых устройств для использования приложения:

– очки (шлем) виртуальной реальности;

– мощный компьютер;

– автосимулятор (кресло, руль, КПП, ручник, панель приборов);

– монитор.

Рассмотрим научную новизну предлагаемых в проекте решений.

1) Методика обучения вождению, предлагаемая в проекте, отличается от существующих реализацией принципа управления по обратной связи с диагностикой состояния обучающихся за счет объединения возможностей различных аппаратных и программных средств обучения: обучающего программного обеспечения с использованием технологии виртуальной реальности, очков виртуальной реальности, реальных транспортных средств.

2) Предлагается ранее не используемая обучающая программная система, которая за счет использования инструментов виртуальной реальности в сфере обучения вождению транспортными средствами реализует технологию интерактивной визуализации в дорожных условиях, отличающаяся представлением виртуальных трёхмерных объектов тренировочных маршрутов в реальном времени и в реальном размере.

Рассмотрим достоинства и недостатки имеющихся аналогов.

1) Samsung Drive. Медиа-сервис, цель которого – помощь начинающим и неопытным водителям при возникновении нестандартных и аварийных

ситуаций при управлении транспортным средством. Концепт заключается в информировании обучающихся об опасных аспектах вождения, чтобы не создавать помех для остальных участников дорожного движения. Недостатками являются высокая стоимость, отсутствие поддержки русского языка, в том числе в технической поддержке, отсутствие функции управления транспортным средством в виртуальном режиме.

2) TeenDrive 365 by Toyota. Комплексный программный продукт, являющийся совместным проектом компаний Discovery Education и Toyota. Цель проекта – помощь несовершеннолетним в сохранении концентрации при вождении для повышения уровня безопасности. Недостатки: англоязычный продукт, отсутствие поддержки русского языка, в том числе в технической поддержке, отсутствие возможности применения виртуальных очков или шлема, отсутствие функции управления транспортным средством в виртуальном режиме.

Преимущества предлагаемого решения по сравнению с аналогами: отечественный разработчик, частые обновления, русскоговорящая техническая поддержка, низкая стоимость по сравнению с аналогичными сервисами. Приложение решает проблему боязни учеников автошкол сесть за руль, так как оформлено в форме игры с обучением на движке Unreal Engine.

Разработан календарный план реализации проекта.

Первый этап – разработка приложения.

– исследование предметной области, сравнительный анализ аналогов;
– разработка концепции продукта;
– сбор данных для компьютерной визуализации;
– создание контента: моделирование и текстурирование, риггинг и анимация, аудио- видео эффекты;
– сборка приложения (сборка проекта в игровом движке: создание сцены, добавление контента; оптимизация графики).

Второй этап – тестирование приложения.

– тестирование приложения;
– портирование на VR-устройство;
– испытание прототипа в реальных условиях;
– доработка приложения.

План коммерциализации проекта: программное приложение будет распространяться образовательным учреждениям, автошколам, а также частным лицам. Каналы продвижения: социальные сети, веб-аналитика, поисковое продвижение, контекстная реклама, контент-маркетинг.

Рассмотрим практическую значимость проекта. Приложение виртуальной реальности предназначено для повышения эффективности обучения вождению в автошколах за счет совершенствования методики обучения, для

чего требуются специальные учебные классы с необходимым оборудованием. Также программное приложение актуально для учебных заведений дополнительного профессионального образования с целью подготовки обучающихся к курсам вождения. Предлагаемый проект планируется к реализации как на уровне субъектов РФ, так и на международном уровне.

Список используемых источников

1. Смолин А. А., Жданов Д. Д., Потемин И. С. Системы виртуальной, дополненной и смешанной реальности / под ред. А. А. Смолина. СПб. : Университет ИТМО, 2018. 59 с.

2. Гнатышина Е. В., Саламатов А. А. Цифровизация и формирование цифровой культуры. Социальные и образовательные аспекты // Вестник Челябинского государственного педагогического университета. 2017. № 8. С. 19–24.

УДК 621.391.1
ГРНТИ 49.43.01

ПРИМЕНЕНИЕ СЕМАНТИЧЕСКИХ ТЕХНОЛОГИЙ В ИНФОРМАЦИОННО-ОРИЕНТИРОВАННЫХ СЕТЯХ ICN

Я. А. Боровская, А. Ю. Гребешков

Поволжский государственный университет телекоммуникаций и информатики

Архитектурная и информационная интеграция сетей связи пятого поколения и информационно-ориентированных сетей ICN (5G-ICN) даёт целый ряд преимуществ в доставке контента пользователю. Анализ архитектурных возможностей 5G-ICN в части возможности кеширования данных показывает необходимость применения новых семантических технологий доля управление кешированием контента. Базовой задачей становится построение обобщенной информационной модели с учетом рассмотренных параметров кэшируемого именованного объекта.

информационно-ориентированные сети, контент, кэширование, сети пятого поколения, семантические технологии.

С каждым годом увеличивается общий объем информации, которая предоставляется пользователю с использованием инфокоммуникационных технологий (Интернет). Поскольку потребности в оперативном получении высококачественного контента по запросу с каждым годом растут, большое внимание уделяется «качеству восприятия» *(Quality of Experience*, QoE) пользователем услуг связи. Это оказывает существенное влияние на организацию процессов взаимодействия пользователь-сеть. В этой связи, чтобы

удовлетворить возрастающие и изменяющиеся требования пользователей в части непрерывности предоставления информации, соблюдения конфиденциальности, обеспечения требований приложений реального времени была разработана новая концепция информационно-ориентированных сетей ICN прежде всего на базе 5G. Поэтому актуально рассмотрения новых способов и решений, касающихся вопросов общего подхода к управлению сетью, основанного не только на количестве, но на содержании, в более широкой трактовке – на смысле, передаваемых потоков данных. Для этого предлагается рассмотреть вопрос применения семантических технологий применительно к архитектурной интеграции 5G-ICN.

Согласно Рекомендации МСЭ-Т Y.3075, ICN есть новая концепция сетевой организации, где основными компонентами являются именованные объекты данных. К именованным объектам могут быть отнесены и устройства – источники информации. Одним из основных преимуществ ICN сетей является возможность предоставления гибкого кэширования именованных объектов данных вместе с контентом [1]. Кеширование есть процесс временного хранения данных для доступа.

В статье [3] была предложена архитектура интегрированного решения 5G-ICN, где функции ICN доступны пользователям через стандартизованные интерфейсы 5G, и поэтому воспринимаются 5G как стандартные функции (рис. 1). При этом можно выделить проблемно-ориентированный контент, который используется сетями либо уже частично загружен серверы граничных вычислений или на терминал пользователя UE. Более сложным случаем является кеширование неструктурированной информации, которая ещё не была востребована, но возможно будет предоставлена пользователю или сети в обозримое время, в том числе в связи с уже используемым контентом.

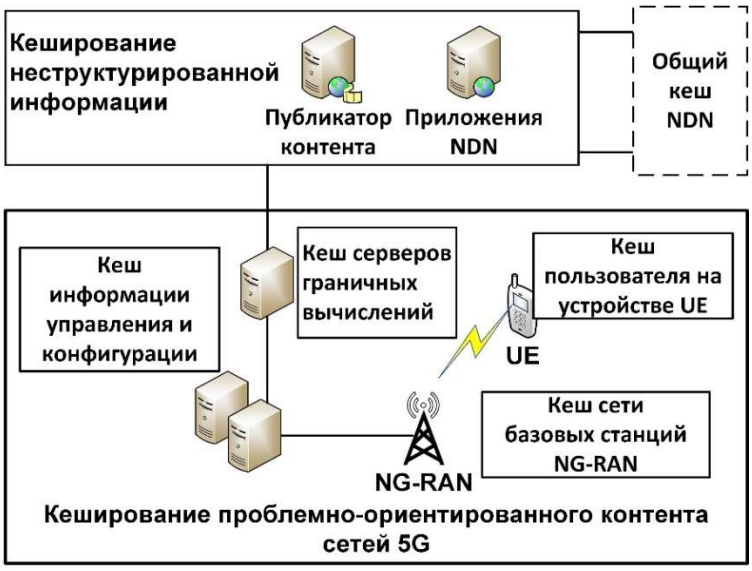


Рис. 1. Архитектурная интеграция 5G-ICN

Базовое условие кеширования есть своевременное обновление информационного содержания объектов данных и одновременное уменьшение время доставки информации по запросам пользователей. Для решения первой задачи и ускорения поиска требуемой информации можно использовать символьные имена объектов, которые запрашивает пользователь согласно имеющимся протоколам информационной технологии сетевого именования данных (*Named Data Networking*, NDN) [3]. Обращение к объекту данных позволяет получить связанный с ним контент. Таким образом, ICN представляется как новая концепция интеллектуальной сети поиска и хранения информации.

Объективно возникает задача интеллектуализации процесса хранения, пересылки, извлечения и эффективного использования большого потока разнородных данных, которые могут быть записаны в ICN кеше (ICN Cache). Из рис. 2 видно, что для организации общего кеша NDN предлагается использовать методы онтологического проектирования – семантические технологии, чтобы описать смысл информации, доступной через объекты данных. Это один из перспективных способов внедрить обобщенную информационную модель интеллектуального управления предоставлением контента, которая будет способствовать переходу к управлению в сети, основанному на содержании данных.

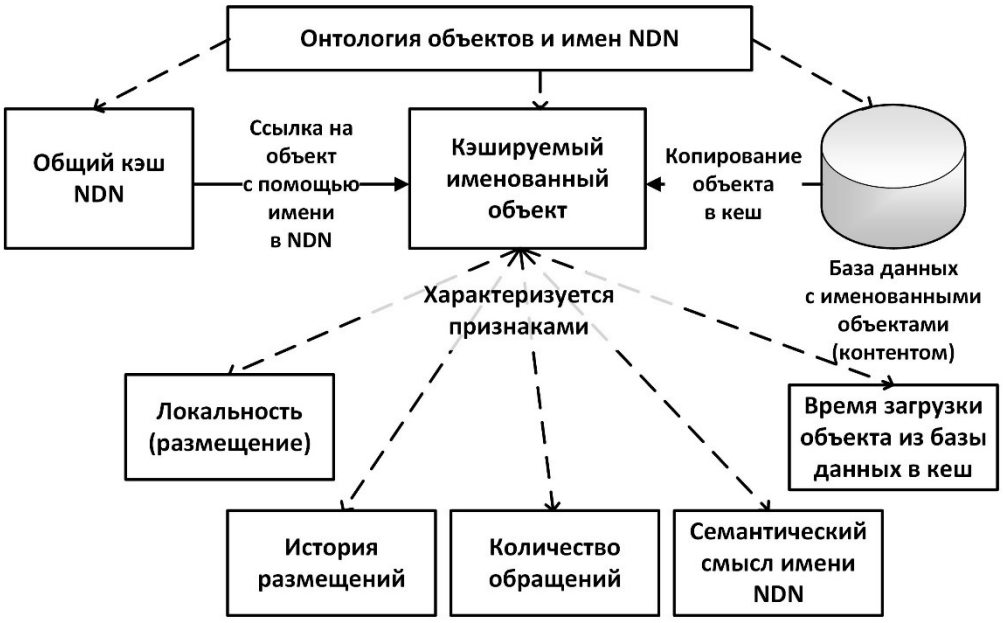


Рис. 2. Характеристики кешируемого объекта

Предполагается, что кешируемый объект характеризуется тремя параметрами:

– локальность (время пассивности объекта) – разница между текущим системным временем и последним временем обращения к объекту;

– история размещений – тренд появления именованного объекта в кеше;

– количество обращений – сумма/интенсивность обращений к объекту за временной интервал;

– время загрузки объекта из базы данных в кэш-память – время появления объекта в кеше с момента запроса;

– семантический смысл имени NDN – содержательное описание в виде метки или хэш-тега, которое имеет смысловое значение.

В качестве формальной основы проектируемой базы знаний и онтологии, представляющих собой основу информационной модели управления ICN предлагается использовать графодинамические модели – смысловые модели представления и обработки знаний, в основе которых лежат семантические сети [4, 5]. Фактически речь идет о создании формальных средств описания смысла различных видов знаний и формальных средств описания обработки знаний на смысловом уровне для ICN. Предлагается организовать семантическую память узла ICN, которая в виде графа хранит сведение относительно логических и семантических связей именованных объектов в процессах обработки данных для виртуального или физического объекта и делает эту информацию доступной для всех пользователей ICN посредством единого семантического пространства. Таким образом, семантическая память играет решающую роль в распределенном сборе и интеграции данных во всей архитектуре ICN сети. Существуют различные способы реализации семантической памяти с широким спектром технических реализаций в различных областях применения. Данные семантической памяти могут быть интерпретированы широким спектром программного обеспечения, имеющего доступ или интерфейс с описанием семантических примитивов и онтологии, которые используются для записи содержимого памяти. Если именованный объект находится в контуре управления одной платформы в течение своего жизненного цикла, то использование в рамках другой платформы без формальной машинно-понятной семантики в рамках семантической памяти может быть затруднительным, поскольку возможна различная интерпретация хранимой информации, особенно с учетом класса измерений. Предлагаемая архитектура позволяет решить такую проблему.

Таким образом, предложенная концептуальная структура 5G-ICN с использованием семантической памяти узлов ICN является весьма перспективной в части общего перехода к уровню сетей доставки контента. В перспективе ICN сеть может «поглотить» текущую IP структуру с общей возможностью внедрения ICN слайса для доступа и кеширования семантически близки объектов. На основе семантической памяти в дальнейшем будет разработана обобщенная модель для оптимального хранения и управления кешированием данных 5G-ICN.

Список используемых источников

1. Гребешков А. Ю., Боровская Я. А. ICN и сети именованных данных // XXIII Международная научно-техническая конференция «Проблемы техники и технологии телекоммуникаций, ПТиТТ-2021: сб. докладов. Самара: ПГУТИ, 2021. С. 103–104.
2. Гребешков А. Ю., Боровская Я. А. Построение информационно-ориентированных сетей 5G-ICN // Вестник связи. 2021. № 11. С. 13–17.
3. ITU-T Y.3071 (03/2017) Data aware networking (information centric networking) – Requirements and capabilities. 18 p. URL: https://www.itu.int/rec/T-REC-Y.3071-201703-I/ (дата обращения: 04.01.2022).
4. Голенков В. В., Гулякина Н. А. Графодинамические ассоциативные модели и средства параллельной обработки информации в системах искусственного интеллекта // Доклады Белорусского государственного университета информатики и радиоэлектроники. 2004. №1. С. 92–101.
5. Wahlster W. Foundations of Semantic Product Memories for the Internet of Things // Springer-Verlag Berlin Heidelberg. 2013. 394 p.

УДК 004.451.9
ГРНТИ 81.93.29

ИССЛЕДОВАНИЕ ЭВОЛЮЦИИ МЕХАНИЗМОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОПЕРАЦИОННОЙ СИСТЕМЫ WINDOWS 11

А. А. Браницкий, А. А. Манукян

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В данной статье показана эволюция механизмов информационной безопасности на примере операционной системы Windows 11 и проанализированы основные характеристики.

конфиденциальность, безопасность, система, Майкрософт, операционная система, разработка, приложение.

Последние несколько лет стали очень распространены программы-вымогатели и шифровальщики, поэтому компания Microsoft планирует оградить будущее информационного пространства от уязвимостей, которые позволяют распространяться вредоносным программам.

Официальная дата выхода *Windows 11* состоялась 5 октября 2021 года. В новом релизе компания Майкрософт делает упор на безопасность и стабильность операционной системы, выдвигая завышенные системные требования, которые предъявляются не только к вычислительному ресурсу, но и к «железу» ПК напрямую.

В статье выделены основные направления, обновления и нововведения в системе.

– нулевое доверие (*Zero Trust*) и *Windows;*
– аппаратная безопасность;
– безопасность приложений;
– безопасность пользователей и защищённая идентификация;
– безопасность операционной системы;
– облачные сервисы.

Нулевое доверие

Нулевое доверие в *Windows* – это авторизация и проверка подлинности на основе всех доступных данных, включая личность пользователя, местоположение, состояние устройства, сервис или рабочую нагрузку, классификацию данных и мониторинг аномалий. Ограничение доступа пользователей с помощью адаптивных политик, основанных на оценке риска, и защиты данных, чтобы обеспечить безопасность данных и сохранить производительность [1]. Общая архитектура *Zero Trust* показана в рис. 1.

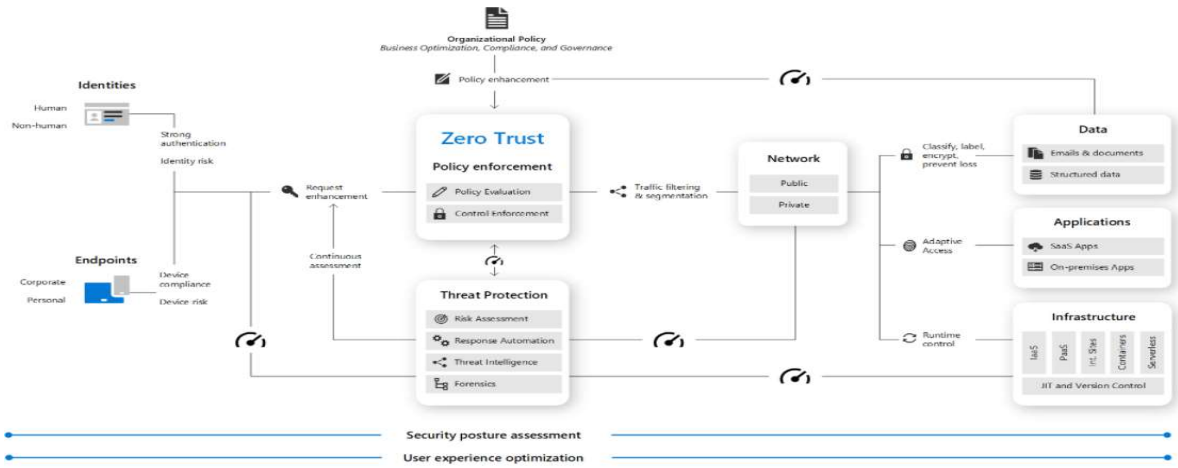


Рис. 1. Общая архитектура *Zero Trust*

Аппаратная безопасность

Trusted Platform Module (TPM) является одной из наиболее важных функций безопасности в *Windows 11*. Это микросхема, которая помогает выполнять такие действия, как генерация, хранение и ограничение использования криптографических ключей. Многие TPM включают несколько физических механизмов защиты, чтобы сделать их устойчивыми к взлому и предотвратить вмешательство вредоносных программ в функции безопасности TPM. Чип TPM добавляется в процессор или интегрируется в материнскую плату компьютера.

Устройства горячего подключения PCI позволяют пользователям подключать новые классы внешних периферийных устройств, включая видеокарты и другие устройства PCI, к своим ПК с опытом, идентичным USB. Поскольку порты PCI для горячего подключения являются внешними и легкодоступными, ПК подвержены атакам с прямым доступом к памяти (DMA). От атак прямого доступа к памяти была разработана политика *Kernel* DMA *Protection*, которая ограничивает возможность внешних периферийных устройств напрямую копировать память, когда пользователь заблокировал свой ПК.

Безопасность приложений

Благодаря *Windows* безопасности электронной почты S/MIME пользователи могут шифровать исходящие сообщения и вложения, чтобы их могли прочитать только адресаты, имеющие цифровой идентификатор (ID). Как показано на рис. 2, пользователи могут ставить цифровую подпись на сообщениях, которая подтверждает личность отправителя и гарантирует, что сообщение не было подделано.

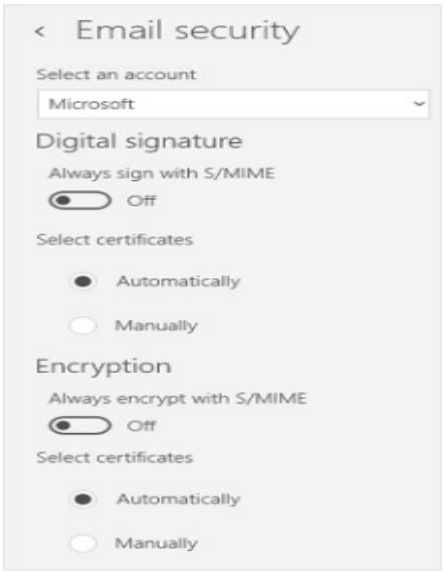


Рис. 2. Настройка параметров S/MIME

Windows Sandbox предоставляет легкую среду рабочего стола для безопасного запуска приложений в изоляции. Программное обеспечение, установленное в этой среде, остается в «песочнице» и запускается отдельно от основной машины. Когда она закрывается, все программное обеспечение, файлы и состояние удаляются [2].

Облачные сервисы

Windows 11 поддерживает MDM, решение для управления предприятием, помогающее управлять политиками безопасности и бизнес-приложениями организации. При добавлении учетной записи Майкрософт в *Windows 11* пользователи могут использовать на своих устройствах параметры *Windows*, файлы и другие параметры.

Microsoft Azure Active Directory (Azure AD) – это комплексное облачное решение по управлению идентификацией и доступом для управления идентификационными данными и каталогами, предоставления доступа к приложениям и защиты идентификационных данных от угроз безопасности. *Windows 11* легко взаимодействует с *Azure* AD, обеспечивая безопасный доступ и управление идентификацией из любого места [3].

Безопасность пользователей и защищённая идентификация

Windows Hello (для бизнеса) заменяют аутентификацию на основе пароля более надежной моделью аутентификации для входа в устройство с помощью пароля (PIN-кода) или другой биометрической аутентификации.

Windows Defender Credential Guard помогает защитить системы от методов атаки с кражей учетных данных, а также предотвратить доступ вредоносных программ к системным секретам, даже если процесс запущен с привилегиями администратора.

Windows 11 поддерживает вход с устройства с помощью ключей безопасности FIDO 2*,* а в *Microsoft Edge* или других современных браузерах поддерживает использование безопасных учетных данных на основе FIDO для защиты учетных записей пользователей.

Приложение *Microsoft Authenticator* - идеальный помощник для обеспечения безопасности в *Windows 11*. Оно позволяет легко и безопасно входить во все учетные записи в Интернете с помощью многофакторной аутентификации, входа с телефона без пароля или автозаполнения пароля, а также может использоваться для настройки многофакторной проверки подлинности для пользователей.

Безопасность операционной системы

Secure Boot и *Trusted Boot* помогают предотвратить загрузку вредоносных программ и поврежденных компонентов при запуске устройства *Windows. Secure Boot* начинает с защиты начальной загрузки, а затем процесс подхватывает *Trusted Boot*. Вместе они помогают обеспечить безопасную и надежную загрузку системы *Windows*.

BitLocker Drive Encryption – это функция защиты данных, которая интегрируется в операционную систему и устраняет угрозы кражи или раскрытия данных с потерянных, украденных или неправильно выведенных из эксплуатации компьютеров. *BitLocker* обеспечивает максимальную защиту при использовании с модулем доверенной платформы TPM версии 1.2 или более поздней.

Microsoft Defender Antivirus включен во все версии *Windows* 10, *Windows Server* 2016 и более поздние версии, а также *Windows* 11. *Microsoft Defender Antivirus* интегрирован с облачной защитой, что позволяет практически мгновенно обнаруживать и блокировать новые и возникающие угрозы.

Defender for Endpoint также является частью *Microsoft 365 Defender,* унифицированного пакета защиты предприятия до и после атаки, который координирует обнаружение, предотвращение, расследование и реагирование на конечных точках, идентификационных данных, электронной почте и приложениях для обеспечения комплексной защиты от сложных атак [4].

Нововведения и обновления механизмов информационной безопасности в ОС *Windows* 11 представлены в таблице.

ТАБЛИЦА. Нововведения и обновления механизмов информационной безопасности в ОС *Windows* 11

Механизмы информационной безопасности	Обновления	Нововведения
Trusted Platform Module	+	-
Безопасность электронной почты S/MIME	-	+
Windows Sandbox	+	-
MDM	-	+
Microsoft Azure Active Directory	+	-
Windows Hello	-	+
Windows Defender Credential Guard	+	-
Microsoft Authenticator	-	+
Secure Boot и *Trusted Boot*	+	-
BitLocker Drive Encryption	+	-
Microsoft Defender Antivirus	+	-
Defender for Endpoint	-	+
Поддержка ключей безопасности FIDO 2	-	+

Таким образом, можно сделать вывод, что приоритетной задачей компании Майкрософт является закрытие уязвимостей в системе безопасности, поэтому разработчики параллельно внедряют нововведения как в *Windows* 11, так и в предыдущие версии.

Список используемых источников

1. Официальный сайт Windows. URL: https://www.microsoft.com/en-us/security/business/zero-trust?rtc=1

2. Официальный сайт Windows. URL: https://docs.microsoft.com/ru-ru/windows/security/threat-protection/windows-sandbox/windows-sandbox-architecture

3. Официальный сайт Windows. URL https://azure.microsoft.com/ru-ru/services/active-directory/

4. Официальный сайт Windows. URL: https://docs.microsoft.com/ru-ru/microsoft-365/security/defender-endpoint/defender-endpoint-plan-1-2?view=o365-worldwide

5. Официальный сайт Windows. URL: https://docs.microsoft.com/en-us/windows/security/

УДК 004.054
ГРНТИ 50.43.19

АНАЛИЗ МЕТОДОВ ПОВЫШЕНИЯ ОТКАЗОУСТОЙЧИВОСТИ ОБЛАЧНОЙ ИНФРАСТРУКТУРЫ СРЕДСТВАМИ МОНИТОРИНГА И ПРЕДСКАЗАНИЯ СОСТОЯНИЯ КОМПОНЕНТОВ

Е. С. Бугрова, И. Е. Пестов, И. Ф. Тарабанов, А. А. Швидкий

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Целью статьи является исследование методов повышения отказоустойчивости облачной инфраструктуры. Особое внимание уделено процессу мониторинга, а именно рассмотрению состояния работоспособности компонентов облака. В статье раскрывается проблема недостаточного функционала одиночных инструментов мониторинга. На основе исследования выявляются различные способы мониторинга, а также выполняется поиск вариантов, обеспечивающих предсказание возможных сбоев для их оперативного устранения.

система мониторинга, облачная инфраструктура, метрики, отказоустойчивость.

В мире цифровых технологий пользователи информационных услуг обращают свое внимание на высокодоступные сервисы, такие как облачные сервисы. Облачная инфраструктура – это модель сетевого доступа в режиме по требованию, которая предполагает использование вычислительных ресурсов сторонней ИТ-инфраструктуры. При разработке и проектировании облачной инфраструктуры необходимо использовать методы повышения отказоустойчивости такие как: резервирование, автоматизация, унификация, сокращение времени непрерывной работы. Данные методы могут привести как к повышению доступности, так и к дополнительным издержкам в обслуживании и уменьшению пропускной способности системы. Одним из самых информативных и надежных методов является мониторинг.

Мониторинг – это непрерывный процесс наблюдения и регистрации параметров объекта в соответствии с заданными критериями. Мониторинг помогает оперативно обнаружить сбои в работе серверов, операционных систем и приложений, а также позволяет гарантировать своевременное устранение ошибок, для обеспечения высокого уровня доступности объектов облачной инфраструктуры.

Целью исследования является повышение отказоустойчивости облачной инфраструктуры средствами мониторинга. Для ее достижения необходимо решить следующие задачи:

– провести аналитический обзор метрик;

– выделить метрики, необходимые для определения состояния компонентов облачной инфраструктуры;

– предложить вариант предсказания возможных сбоев компонентов облачной инфраструктуры.

В облачной инфраструктуре существуют динамически изменяющиеся объекты. Различные автоматизированные инструменты отслеживают множество метрик, отслеживающих производительность объектов облачной инфраструктуры. Одни инструменты встроены прямо в облачные сервисы, другие предлагаются сторонними платформами. Решения для мониторинга облачной инфраструктуры включают настраиваемые показатели. Следует начать исследование с выбора метода мониторинга. Существует несколько подходов [1]:

- Управление производительностью приложений – сквозной мониторинг распределенных облачных приложений на одной панели;
- Мониторинг баз данных – отслеживание запросов, доступности, использования и целостности информации в базах данных, к которым обращаются облачные приложения;
- Мониторинг виртуальной инфраструктуры – традиционный мониторинг инфраструктуры с дополнительным преимуществом управления облачными приложениями;
- Мониторинг облачных серверов – соотношение производительности инфраструктуры с производительностью приложений;
- Мониторинг взаимодействия с конечными пользователями – сбор важных показателей производительности веб-приложений и мобильных приложений, таких как сбои, сведения о загрузке страниц и частота сетевых запросов;
- Единый мониторинг – полный контроль всей ИТ-инфраструктуры, включая компоненты, работающие в облаке.

Рациональным выбором подхода к мониторингу облачной инфраструктуры, будет работа с единой системой мониторинга. Основываясь на анализе, проведенным в работе [2], решено остановиться на платформе Grafana [3], поскольку это один из вариантов, который целесообразно использовать для мониторинга компонентов облачных инфраструктур. В данной платформе присутствуют: информативность графиков, гибкость настройки, сортировка значений таблиц и возможность вывода нескольких графиков на одну информационную панель.

Так как Grafana не хранит данные, а только собирает, следует использовать данный инструмент в связке с дополнительными компонентами [4],

такими как Prometheus [5] и Node Exporter [6], используемыми для хранения и передачи метрик, что позволит добиться положительного результата при мониторинге компонентов.

В первую очередь необходимо провести аналитический обзор метрик, для этого возможно взять существующее решение – информационную панель «Node Exporter Full» [7]. В данной панели присутствуют основные и дополнительные компоненты, которые необходимо отслеживать в облачной инфраструктуре (табл. 1).

ТАБЛИЦА 1. Обзор разделов информационной панели «Node Exporter Full»

Название раздела	Описание
Basic CPU/Mem/Disk	Базовая информация о процессоре, памяти и дисках
CPU/Memory/Net/Disk	Углубленная информация о процессоре, памяти и дисках
Memory Meminfo	Информация о всех видах памяти
Memory Vmstat	Информация об активной и неактивной памяти
System Timesync	Информация о синхронизации системы по времени
System Processes	Информация о системных процессах
System Misc	Дополнительная информация о системе
Hardware Misc	Дополнительная информация об аппаратном обеспечение
Systemd	Информация о запущенных сервисах
Storage Disk	Информация о диске хранения данных
Storage Filesystem	Информация о памяти файловой системы
Network Traffic	Информация о всем трафике, проходящем в сети
Network Sockstat	Информация о сокетах сети
Network Netstat	Информация об основных протоколах, работающих в сети
Node Exporter	Информация о состоянии экспортера

Данное решение актуально, так как содержит все необходимые разделы для полного комплексного мониторинга [8].

На основе проведенного аналитического обзора разделов «Node Exporter Full», возможно предположить, что основными компонентами, которые напрямую влияют на работоспособность облачной инфраструктуры

являются: процессор, оперативная память, сеть. Чтобы предсказать возможные сбои необходимо контролировать данные составляющие. Для этого необходимо проанализировать последствия отслеживания выделенных метрик на систему (табл. 2).

ТАБЛИЦА 2. Анализ метрик для предсказания возможных сбоев

Название метрики	Описание	Влияние на систему
CPU Busy	Загруженность процессора	При нагрузке больше 80 %, система может отказать
RAM Used	Зарезервированная оперативная память	Если оперативная память переполнена, система может отказать
Root FS Used	Зарезервированное место в корневой системе	При полном заполнении, система может отказать
Sys Load (5m avg)	Средняя скорость загрузки всех ядер процессора за пять минут	При высоком показателе, сервер начнет зависать и медленно работать
IOwait	Процент времени, в течение которого процессор ожидает ввода-вывода	При высоком показателе, диски будут работать медленно
Receive и Transmit Network Traffic	Скорость загрузки и выгрузки сетевого интерфейса	При большой нагрузке, скорость сетевого доступа снижается

На основе вышеописанного анализа, установлено, что данные метрики способствуют своевременному обнаружению аномалий для оперативного устранения, что повысит отказоустойчивость облачной инфраструктуры.

Данное решение использовалось для одного узла. Чтобы отслеживать все хосты облачной инфраструктуры, возможно создать совокупность имеющихся метрик, для получения информации о состоянии облачной инфраструктуры (рис.).

При анализе процесса мониторинга облачных сервисов, сделан вывод как о возможности применения инструмента реализации предоставления информации об ошибках – «Node Exporter Full», так и о возможности предсказывать сбои в работе сервиса, на основании анализа, представленного в таблице 2, что позволяет повысить отказоустойчивость облачной инфраструктуры.

Проведен сравнительный анализ инструментов облачного мониторинга, на основании которого выявлено, что не все инструменты обладают достаточным функционалом, что в конечном итоге приводит к выводу о рациональности реализации комплексного подхода к мониторингу. Данный результат позволяет контролировать необходимые в каждом конкретном случае метрики, влияющие на работоспособность как системы в целом, так и отдельных компонентов облачной инфраструктуры.

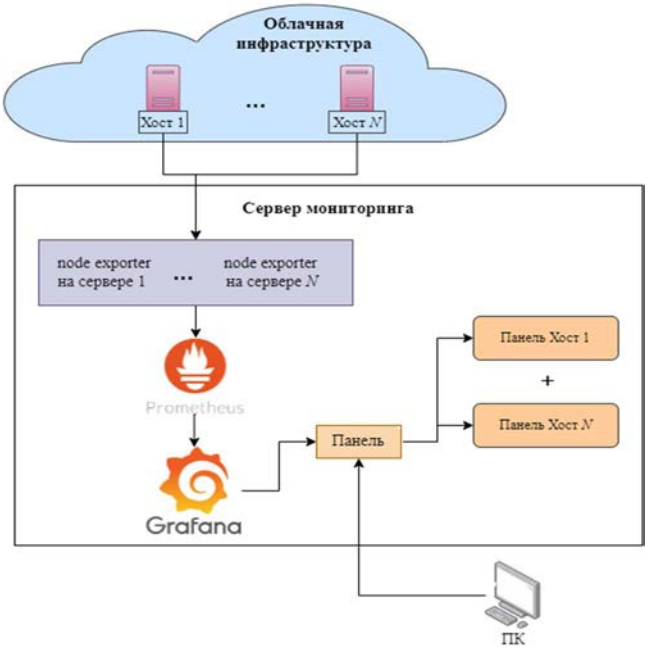


Рисунок. Схема комплексного подхода к мониторингу облачной инфраструктуры

Результат исследования позволяет утвердить значимость мониторинга для предоставления услуг и контроля их качественных характеристик.

Список используемых источников

1. Cisco. URL: https://www.cisco.com/c/ru_ru/solutions/cloud/what-is-cloud-monitoring.html (дата обращения: 10.02.2022).

2. Дедухова А. А., Швидкий А. А. Сравнительная оценка систем мониторинга компонентов облачной инфраструктуры // Актуальные проблемы инфотелекоммуникаций в науке и образовании. X Юбилейная Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2021. Т. 1. С. 292–296.

3. Хабр. URL: https://habr.com/ru/company/southbridge/blog/431122/ (дата обращения: 10.02.2022).

4. Dmosk. URL: https://www.dmosk.ru/instruktions.php?object=prometheus-linux (дата обращения: 10.02.2022).

5. Prometheus. 2014. URL: https://prometheus.io/ (дата обращения: 10.02.2022)

6. Github. URL: https://github.com/prometheus/node_exporter (дата обращения: 10.02.2022).

7. Grafana Labs. 2017. URL: https://grafana.com/grafana/dashboards/1860 (дата обращения: 10.02.2022).

8. ProgrammerSought. URL: https://programmersought.com/article/28581026302/ (дата обращения: 10.02.2022).

Статья предоставлена заведующим кафедрой ИКС СПбГУТ, кандидатом технических наук, доцентом А. А. Зарубиным.

УДК 004.052.42
ГРНТИ 50.43.19

АНАЛИЗ МЕТОДОВ МАШИННОГО ОБУЧЕНИЯ ДЛЯ ОТСЛЕЖИВАНИЯ СОСТОЯНИЯ РАСПРЕДЕЛЕННЫХ СИСТЕМ ХРАНЕНИЯ ДАННЫХ

Е. С. Бугрова, Н. М. Редругина, И. Ф. Тарабанов, А. А. Швидкий

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Работа посвящена анализу методов машинного обучения применимых к распределённым системам хранения данных. Были рассмотрены различные методы машинного обучения и выбран наиболее подходящий под систему хранения данных Ceph. После выбора метода обучения были выбраны инструменты для машинного обучения. На их примере был произведен анализ для отслеживания аномалий в работе системы хранения данных.

Opensearch, системы хранения данных, диагностическая информация.

Для задач мониторинга используется множество различных методологий для обнаружения ошибок в работе системы. Все большую популярность на рынке мониторинга [1], получают методологии с применением машинного обучения. Верным решением будет выбор одно из существующих решений распределенных систем хранения данных для дальнейшего его анализа. Как фактор стоит учесть, что для исследования не будет использованы проприетарные решения из-за их закрытости и меньшей гибкости в их настройке или ограниченному доступу к диагностической информации. Это делает анализ таких систем невозможным с целью повышения производительности. Системы на базе открытого исходного кода дают большую гибкость в своей конфигурации и анализе.

Из систем с открытым исходным кодом были выделены три проекта для рассмотрения [2], такие как MiniIO, Ceph, Linstore (табл.).

ТАБЛИЦА. Сравнение систем хранения данных

Критерий	MiniIO	Ceph	Linstore
Относительная производительность	Низкая	Низкая	Высокая
Обеспечение объектного доступа	Да	Да	Нет
Обеспечение блочного доступа	Нет	Да	Даа
Обеспечение файлового доступа	Нет	Да	Да
Максимальное количество узлов (Теория)	32 [5]	Нет ограничений	16 [4]

Критерий	MiniIO	Ceph	Linstore
Максимальное количество узлов (Практика)	32 [5]	225 [3]	16 [4]
Наличие механизмов поиска ошибок	Да	Да	Нет

Путем сравнения различных программно-определяемых систем хранения данных была выбрана наиболее подходящая система хранения для анализа Ceph, за счет большей универсальности в работе с ней, и отсутствием теоретических ограничений на количество узлов. Ceph состоит из нескольких основных элементов:

- MON – сервис монитора, используется для поддержания актуальных карт и аутентификации. В кластере необходимо иметь более 3 узлов и общее их число не должно быть четным;
- OSD – сервис хранилища, отвечает за хранение данных, с помощью OSD происходит запись/чтение/удаление данных пользователей этой системы;
- MDS – сервер метаданных (необходим при использовании CephFS).

В нашем случае собирались и обрабатывались данные с двух элементов MON и OSD.

Также стоит учитывать, что современные системы очень сложны для отслеживания состояние [6]. При работе системы стоит оценивать не только службы работающие для обеспечения работы самой РСХД (распределенной системы хранения данных), но и системы, которые связанны с работой РСХД. Стоит учитывать службы пользовательских данных, и операционной системы, которые работают с использованием РСХД.

Выбор типа машинного обучения начинается с выбора категории машинного обучения [7]:

– обучение с учителем – тип обучение при котором существует заранее размеченный набор данных, с помощью которых алгоритм может производить обучения и в будущем предсказывать ответы для аналогичных данных;

– обучение без учителя – тип обучения, при котором не существует заранее размеченных данных и алгоритму необходимо самому вывести зависимости в данных;

– обучение с подкреплением – тип обучением при котором алгоритм получают оценку своих действий после достижения своих целей.

Был выбран тип обучения без учителя, так-как объем данных, генерируемых системой хранения данных и связанными с ними другими системами большой данных и сложно поддаются к разметке. После определения типа обучения, выбираем алгоритм обучения.

После изучения доступных алгоритмов обучения был выбран Random Cut Forest (RCF) [8]. Этот алгоритм позволяет обнаруживать аномалии

в данных без формирования обучающих данных. Он может определять аномалии в виде неожиданных всплесков в данных временного ряда, разрывов в периодичности данных или не поддающиеся классификации данных. С каждым сообщением, содержащим диагностическую информацию, алгоритм связывает балл аномалии. Низкий балл означает, то, что эти данные считаются "нормальными". Высокие значения указывают на аномалию данных. Балл для признания данных аномальными для каждого конкретного приложения может изменять, но общей практикой является признание данных аномальными с отклонением на 3 от среднего значения. Этот алгоритм предназначен для работы с произвольными размерами данных.

После того как был определен алгоритм работы машинного обучения, необходимо произвести выбор инструментов поддерживающим алгоритм RCF. В ходе исследования было обнаружено два подходящих продукта:

- Elasticsearch – система полнотекстового поиска и аналитики с возможностями анализа, поиска и хранения больших объемов данных [9];
- Opensearch – свободная реализация Elasticsearch, после смены компанией Elastic лицензии Apache-2 на лицензию закрытого типа SSPL [10–12].

Был сделан выбор в сторону Opensearch, из-за использования им лицензии Apache-2 [13]. После выбора инструмента был развернут стенд (рис. 1).

После выбора основного инструмента Opensearch, был построен кластер из 3 узлов Opensearch для обработки информации из них все три узла с функцией хранения данных, узел с функциями машинного обучения и мастер узел (узел управляющей конфигурацией кластера и распределением данных между узлами). Сбор данных происходил с помощью перенаправления вывода Syslog [14] на удаленный узел Logstash [14], на котором происходит первичная обработка поступающих сообщений и изменения формата сообщения на совместимый с Opensearch формат JSON, а также автоматическое распределение данных по полям, что упрощает и ускоряет в дальнейшем работу Opensearch.

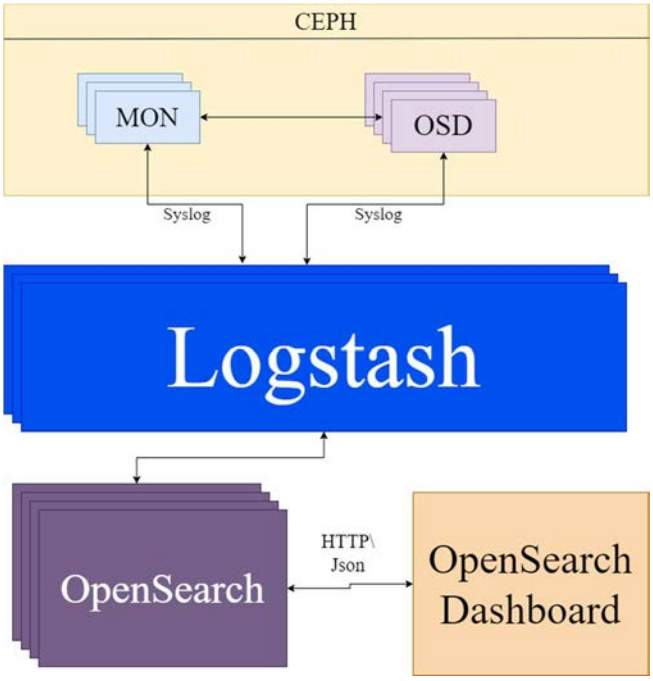


Рис. 1. Схема стенда

После обработки информации Logstash происходит перенаправление вывода на один из узлов Opensearch, заранее определенных в конфигурациях Logstash. Logstash контролирует доставку этих сообщений и уменьшает вероятность потерь, за счет реализации очередей. Между узлами Opensearch происходит равномерное распределение данных по всему кластеру, что дает устойчивость к выходу из строя одного из узлов. При поломке мастер узла автоматически будет выбран новый узел мастер. В случаи поломки любого из узлов произойдет перераспределение информации.

При настройки сбора информации с устройств, был получен поток сообщений примерно в 42 тысячи сообщений в минуту. Во время сбора информации в течение двух недель был настроен детектор аномалий с фильтрацией по названию приложений генерирующими сообщения. В процессе проведение анализа была графически отображена информация о программах работающих с аномалиями (рис. 2). Элемент, связанные с работой Ceph не были признаны как аномальные. На основании нештатной работы других систем и генерации сообщений без всплесков можно сделать выводы о работе СХД.

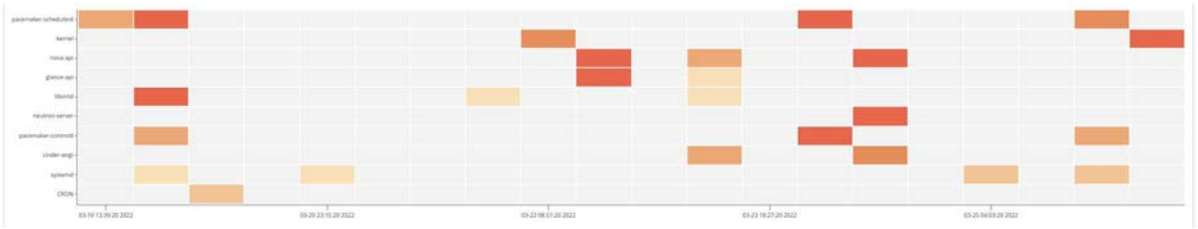


Рис. 2. Аномалии в работе модулей системы

Был проведен анализ существующих решений для выявления аномалий в работе сложных информационных систем. Во время проведения анализа был выявлен наиболее подходящий алгоритм машинного обучения для анализа диагностической информации РСХД. Также была настроена реализация алгоритма RCF, для анализа работающего кластера Ceph в целях выявления аномалий в работе.

Список используемых источников

1. Key IT monitoring trends in 2022 URL: https://network-king.net/key-it-monitoring-trends-in-2022/ (дата обращения: 20.03.2022).

2. Васюткин А. В., Швидкий А. А. Исследование производительности отказоустойчивого программно-конфигурируемого хранилища в гиперконвергентных системах // Актуальные проблемы инфотелекоммуникаций в науке и образовании. IX Международная научно-техническая и научно-методическая конференция: сб. науч. ст., СПб.: СПбГУТ, 2020. С. 216–220.

3. New in Luminous: Improved Scalability // CEPH. URL: https://ceph.com/community/new-luminous-scalability/ (дата обращения: 20.03.2022).

4. LINBIT HA-Solutions Gmbh. Block Storage Management for Containers. URL: https://linbit.com/linstor/ (дата обращения: 20.03.2022).

5. Intel. Implementation Guide for MinIO. Storage-as-a-Service. URL: https://min.io/ resources/docs/CPG-MinIO-implementation-guide.pdf (дата обращения: 20.03.2022)
6. Gregg B. Systems Performance (Addison-Wesley Professional Computing Series) 2nd Edition. Pearson, 2020. 929 p.
7. Машинное обучение: просто о сложном. SberCloud URL: https://sbercloud.ru/ru/warp/machine-learning-about (дата обращения: 21.03.2022).
8. Random Cut Forest (RCF) Algorithm. URL: https://docs.aws.amazon.com/sagemaker/latest/dg/randomcutforest.html (дата обращения: 21.03.2022).
9. Elasticsearch. Школа Больших Данных. URL: https://www.bigdataschool.ru/wiki/elasticsearch (дата обращения: 28.03.2022).
10. 1.0 is released! / A. Hopp. URL: https://opensearch.org/blog/updates/2021/07/opensearch-general-availability-announcement/ (дата обращения: 24.03.2022).
11. Shay, Banon Amazon: NOT OK – why we had to change Elastic licensing. URL: https://www.elastic.co/blog/why-license-change-aws (дата обращения: 24.03.2022).
12. The SSPL is Not an Open Source License. Open Source Initiative. URL: https://opensource.org/licenses/Apache-2.0 (дата обращения: 24.03.2022).
13. Apache License, Version 2.0. URL: https://opensource.org/licenses/Apache-2.0 (дата обращения: 28.03.2022).
14. Тарабанов И. Ф., Швидкий А. А. Оценка подходов к анализу диагностической информации узлов гиперконвергентной инфраструктуры // Актуальные проблемы инфотелекоммуникаций в науке и образовании. X Юбилейная Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2021. Т. 1. С. 670–674.

Статья предоставлена заведующим кафедрой ИКС СПбГУТ, кандидатом технических наук, доцентом А. А. Зарубиным.

УДК 621.315
ГРНТИ 49

КОНТРОЛЬ СОСТОЯНИЯ СМОТРОВЫХ УСТРОЙСТВ ТРАНСПОРТНОЙ МНОГОКАНАЛЬНОЙ КОММУНИКАЦИИ ВОЛОКОННО-ОПТИЧЕСКОЙ ЛИНИИ

В. А. Бурдин, В. О. Гуреев, Д. В. Сосунов, О. В. Шабан

Поволжский государственный университет телекоммуникаций и информатики

В работе предложен метод контроля состояния смотровых устройств линейно-кабельных сооружений транспортной многоканальной коммуникации с использованием системы распределенного вибро-акустического мониторинга. Приведен результат экспериментальных измерений на полигоне. Измерения производились на полимерном смотровом устройстве, в котором размещен запас оптоволоконного кабеля двух типов.

оптоволоконный кабель, смотровое устройство, транспортные многоканальные коммуникации, контроль состояния, система вибро-акустического мониторинга.

В настоящее время активно развивается технология прокладки волоконно-оптических линий связи на базе линейно-кабельных сооружений транспортной многоканальной коммуникации (ЛКС ТМК) [1]. У данной технологии имеется ряд преимуществ при проведении строительно-монтажных работ, в том числе высокая надежность и упрощение процессов технической эксплуатации [2]. При использовании данного метода прокладки снижается стоимость и сокращаются сроки проектирования волоконно-оптических линий связи. Для размещения оптоволоконного кабеля в микротрубке используется пневмопрокладка, которая практически исключает избыточные нагрузки на оптоволокно и тем самым увеличивает срок его службы. Также неоспоримым преимуществом использования ТМК является сокращение сроков восстановительных работ при авариях на линии – кабель задувается в резервную микротрубку, а поврежденная восстанавливается с помощью фитинга. Использование ТМК позволяет создавать полностью диэлектрические конструкции, которые не нуждаются в дополнительной защите на участках сближения с линиями высокого напряжения, в оборудовании заземления и контрольно-измерительных пунктах.

Известно, что в процессе эксплуатации ЛКС ТМК наблюдается заиливание смотровых устройств, что в дальнейшем окажет негативное влияние на надежность ВОЛС и может вызывать проблемы в ходе аварийно-восстановительных работ.

Таким образом для поддержания непрерывного исправного функционирования линейно-кабельных сооружений транспортной многоканальной коммуникации волоконно-оптических линий связи необходимо обеспечивать контроль за состоянием смотровых устройств [3].

При этом следует отметить, что зачастую доступ к смотровым устройствам затруднен, в особенности при прокладке ЛКС в обочине автомобильных дорог. Следовательно, необходима разработка метода контроля состояния смотровых устройств, не требующего непосредственного доступа к ним, и позволяющего минимизировать земляные работы.

В настоящее время на волоконно-оптических линиях связи получают применение системы распределенного акустического мониторинга (DAS) для непрерывного отслеживания виброакустических событий вдоль оптоволоконного кабеля [4]. В работе предлагается метод контроля состояния смотровых устройств с использованием системы СВАМ.

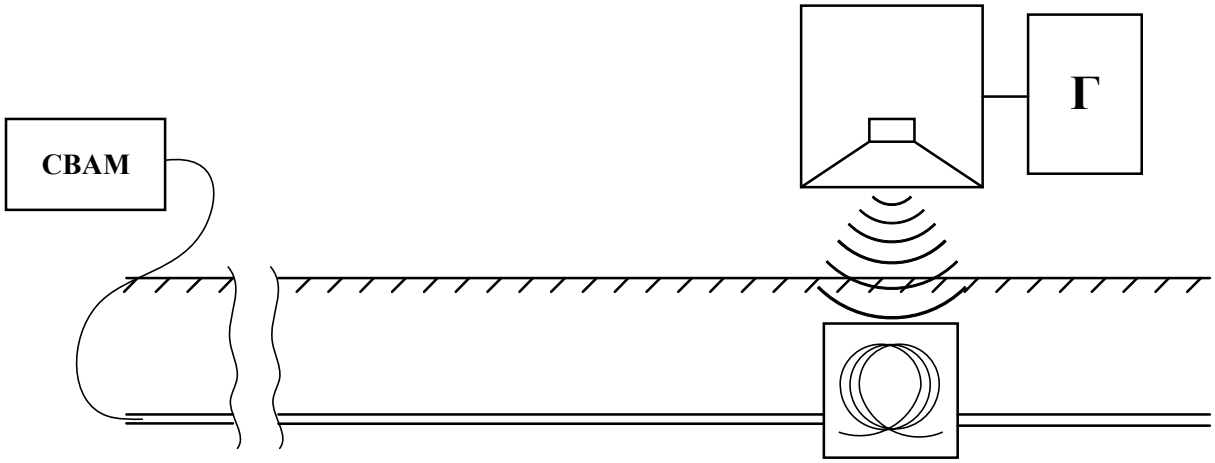


Рис. 1. Принцип работы метода контроля состояния смотровых устройств ТМК ВОЛС акустическими методами

Основной принцип предлагаемого метода заключается в следующем:

1. На этапе ввода в эксплуатацию снимаются и сохраняются опорные амплитудно-частотные характеристики отклика смотровых устройств с помощью системы вибро-акустического мониторинга. Для этого в месте расположения смотрового устройства на поверхности размещается источник акустического воздействия, позволяющий генерировать сигнал в заданном диапазоне частот.

2. В ходе планово-профилактических работ производятся измерения текущих АЧХ откликов.

3. После измерений выполняется обработка полученных данных с учетом опорных АЧХ и определяется состояние смотровых устройств.

Для реализации данного метода необходимо произвести анализ характерных АЧХ типовых смотровых устройств с различными вариантами наполнения: запас оптического кабеля; запас ОК с оптической муфтой; транзитный проход микротрубки, а также при различных состояниях.

Были выполнены экспериментальные измерения на полигоне участка ЛКС ТМК, построенного на территории Поволжского государственного университета телекоммуникаций и информатики. Измерения производились на полимерном смотровом устройстве, в котором размещен запас оптоволоконного кабеля двух типов: ОКЛм – полностью диэлектрический микрокабель, ОКБ – кабель, бронированный стальной проволокой. Примеры реализации данного метода представлены на рис. 2.

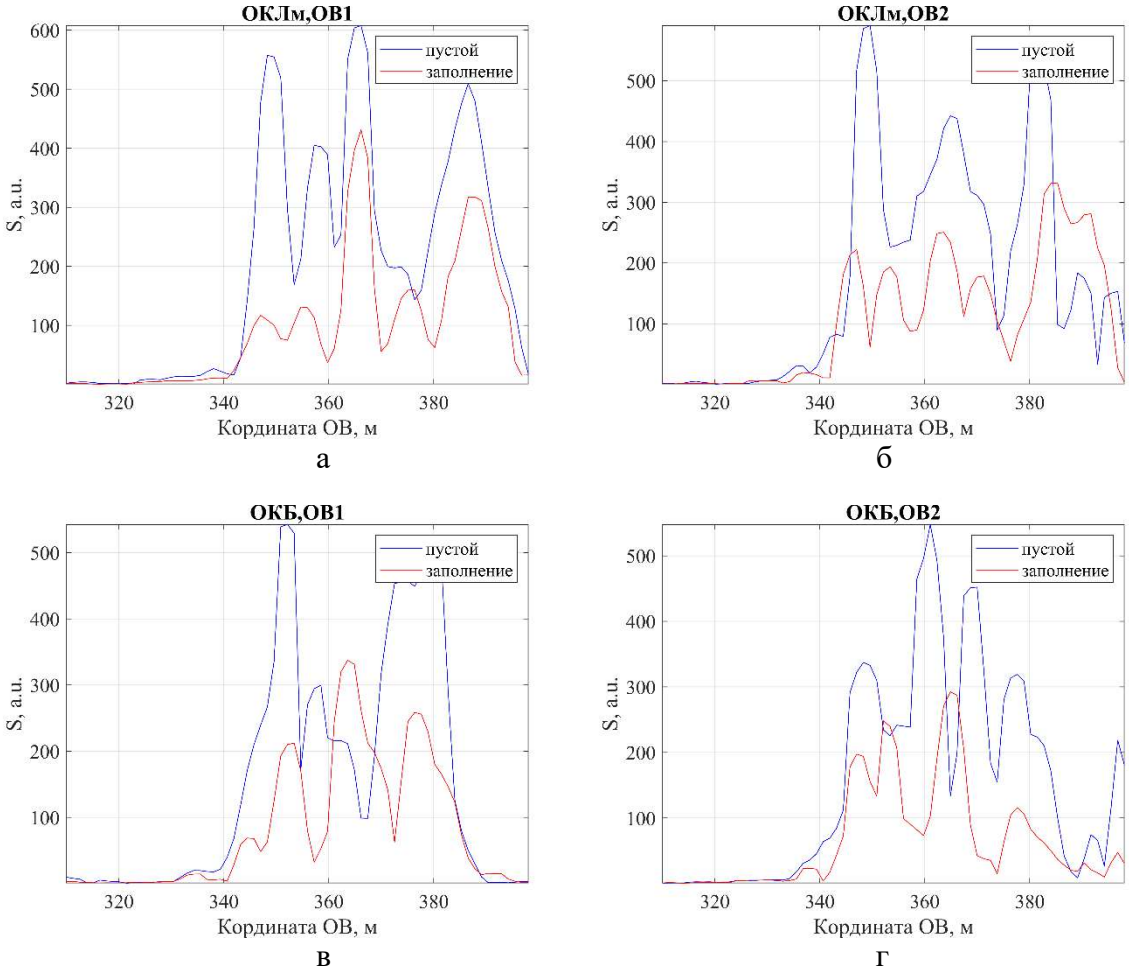


Рис. 2. Результаты апробации метода контроля состояния смотровых устройств ТМК ВОЛС акустическими методами
а, б – полностью диэлектрический микрокабель;
в, г – кабель, бронированный стальной проволокой

Таким образом результаты эксперимента продемонстрировали возможность применения системы распределенного вибро-акустического мониторинга для контроля состояния смотровых устройств транспортной многоканальной коммуникации волоконно-оптической линии связи.

Список используемых источников

1. Recommendation ITU-T L.153/L.48 (03/2003) Mini-trench installation technique. URL: https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-L.48-200303-I!!PDF-E&type=items (дата обращения: 10.09.2021).

2. Цым А. Ю., Иванов И. А. ТМК – инновационная технология модернизации российской информационной инфраструктуры // Фотон-экспресс. 2011. № 2 (90). С. 34–39.

3. Андреев В. А., Бурдин В. А. Стратегии технического обслуживания междугородной кабельной канализации волоконно-оптических линий передачи // T-Comm: Телекоммуникации и Транспорт. 2011. Т. 5. № 8. С. 34–36.

4. Т8 Сенсор. Распределенный акустический сенсор «Дунай». Система для организации рубежей охраны и мониторинга протяженных объектов. URL: https://t8.ru/wp-content/uploads/2017/08/ПАК-Дунай_rus_web.pdf (дата обращения: 15.10.2021).

Статья представлена научным руководителем,
кандидатом технических наук, доцентом М. В. Дашковым.

УДК 681.7.068
ГРНТИ

МОДЕЛЬ КУСОЧНО-РЕГУЛЯРНОЙ МАЛОМОДОВОЙ ВОЛП С УЧЕТОМ СОСТОЯНИЯ ТОРЦЕВОЙ ПОВЕРХНОСТИ ФЕРРУЛ ВОЛОКОННО-ОПТИЧЕСКИХ КОННЕКТОРОВ

А. В. Бурдин[1,2,3], Е. В. Дмитриев[4], Е. С. Зайцева[1], С. С. Пашин[1]

[1]Поволжский государственный университет телекоммуникаций и информатики
[2]АО «Научно-производственное объединение Государственный оптический институт им. С.И. Вавилова»
[3]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
[4]Научно-исследовательский институт радио

Предложена модель кусочно-регулярной волоконно-оптической линии передачи (ВОЛП) с многомодовыми оптическими волокнами (ММ ОВ), функционирующей в маломодовом режиме, дополненная возможностью учета влияния характера и степени загрязнения торцевой поверхности феррул волоконно-оптических коннекторов разъемных соединений оконечных устройств коммутации линейного тракта на искажения передаваемого оптического сигнала. Приведены результаты апробации модели на примере расчета огибающих оптических импульсов системы передачи спецификации 10GBase-LX на выходе указанной ВОЛП с ММ ОВ 50/125 кат. ISO/IEC OM2 для разных условий ввода сигнала с выхода когерентного источника трансивера, определяемых состоянием торцевой поверхности феррул волоконно-оптических коннекторов.

волоконно-оптический коннектор, многомодовое оптическое волокно, дифференциальная модовая задержка, структурированные кабельные системы.

В работе предложено дополнение ранее разработанной [1] модели маломодовой кусочно-регулярной волоконно-оптической линии передачи (ВОЛП), позволяющее учитывать состояние торцевой поверхности феррул волоконно-оптических коннекторов оконечных устройств коммутации – характер и степень их загрязнения, определяемых, в том числе, непосредственно по фотографиям протоколов штатных систем видеодиагностики.

Исходная модель базируется на кусочно-регулярном представлении с элементами метода расщепления по физическим процессам [2]. Так, в пределах регулярного сегмента заданной длины Δz геометрия световода – в частности, радиус сердцевины, параметры профиля показателя преломления и пр. – остаются постоянными, связь мод отсутствует, а модовые компоненты сигнала распространяются независимо друг от друга. Предполагается, что каждая направляемая мода, постоянная распространения которой, изменяясь от сегмента к сегменту, удовлетворяет условию отсечки для всех регулярных световодов, составляющих исследуемое многомодовое ОВ, переносит одиночный импульс заданной формы, идентичной вводимому сигналу (например, гауссовой). Кроме того, в пределах регулярного сегмента амплитуда импульса уменьшается за счет собственных потерь моды.

Границы регулярных сегментов рассматриваются в виде соосного соединения двух многомодовых оптических волокон (ММ ОВ) с разбросом технологических параметров (например, диаметром сердцевины) с некоторым заданным малым угловым рассогласованием, что позволяет непосредственно учесть наличие изгибов ОВ и остаточных механических воздействий, неизбежно возникающих на практике при инсталляции строительных длин ОК. Перераспределение мощности сигнала между амплитудами отдельных составляющих как результат взаимодействия и смешения модового состава определяется путем оценки коэффициентов связи на вышеописанных стыках по известной методике, базирующейся на хорошо известном методе интеграла перекрытия полей взаимодействующих мод.

На приемную сторону указанные «одиночные» импульсы, переносимые соответствующими «индивидуальными» направляемыми модами LP_{lm}, приходят с определенной задержкой относительно друг друга, обусловленной разбросом значений групповых скоростей этих направляемых мод или, иными словами, разбросом модовой задержки. В случае появления новой модовой компоненты форма переносимого данной модой сигнала представляет собой результат сложения гауссовых импульсов всех направляемых мод, которые непосредственно передали часть своей мощности указанной составляющей пропорционально соответствующему значению коэффициента связи. На приемной стороне результирующая огибающая импульса рассматривается как суперпозиция всех существующих модовых компонентов сигнала, которая для частотного отклика оптического сигнала, переносимого M модовыми компонентами LP_{lm} в регулярном многомодовом ОВ длиной z, в общем случае, имеет следующий вид:

$$H_{\text{вых}}(\omega,z)=F[h_{\text{вх}}(t)]\sum_{p}^{M}A_{(N_z+1)}^{(p)}\exp\left[-\alpha_{(N_z+1)}^{(p)}\left(z-N_z\Delta z\right)\right]\times$$
$$\times\exp\left[-j(\omega-\omega_0)\tau_{\text{з}}^{(p;N_z+1)}\left(z-N_z\Delta z\right)\right]\exp\left[-j\frac{1}{2}(\omega-\omega_0)^2\beta_2^{(p;N_z+1)}\left(z-N_z\Delta z\right)\right]\times \quad (1)$$
$$\times\prod_{q=1}^{N_z}A_q^{(p)}\exp\left(-\alpha_q^{(p)}\Delta z\right)\exp\left(-j(\omega-\omega_0)\tau_{\text{з}}^{(p;q)}\Delta z\right)\exp\left(-j\frac{1}{2}(\omega-\omega_0)^2\beta_2^{(p;q)}\Delta z\right),$$

где F – прямое преобразование Фурье; $h_{\text{вх}}(t)$ – импульс на входе ММ ОВ; $A_p^{(0)}$ и α_p начальная амплитуда и коэффициент затухания p-й направляемой моды LP_{lm} (p=1…M); $\beta_1^{(p)}$ и $\beta_2^{(p)}$– дисперсионные параметры p-й направляемой моды LP_{lm}, которые являются элементами разложения частотной зависимости постоянной распространения $\beta(\omega)$ в ряд Тейлора – хорошо известный алгоритм записи основного уравнения распространения, подробно описанный в [2], где первый элемент этого ряда является непосредственно задержкой p-й направляемой моды LP_{lm} $\beta_1^{(p)}=\tau_{\text{з}}^{(p)}$, в то время как второй параметр $\beta_2^{(p)}$ позволяет учесть вклад хроматической дисперсии; $N_z=E(z/\Delta z)$; $E(x)$ – целая часть действительного числа x; $h_{\text{вх}}(t)$ – импульс на входе ММ ОВ;

$A_q^{(p)}$, $\alpha_q^{(p)}$, $\tau_{\text{з}}^{(p;q)}$ и $\beta_2^{(p;q)}$ – амплитуда, коэффициент затухания, задержка и параметр хроматической дисперсии p-й направляемой моды LP_{lm} (p=1…M) на q-м регулярном сегменте, соответственно.

В данной работе математическое описание ввода маломодового оптического сигнала в ОВ с учетом характера и степени загрязнения торца феррула, подключаемого к источнику излучения коннектора, осуществляется с помощью ранее разработанного и экспериментально верифицированного метода расчета коэффициентов связи мод [3–6], базирующимся на оригинальном представлении интеграла перекрытия полей в виде конечных вложенных сумм по компонентам радиального распределения полей этих мод:

$$\eta_{mn}=\frac{\left[\sum_p\sum_q F_m^{(l_m)}(x_p,y_q)F_{n(q)}^{(l_n)}(x_{\text{р}},y_q)\right]^2}{\left\{\sum_p\sum_q\left[F_m^{(l_m)}(x_p,y_q)\right]^2\right\}\cdot\left\{\sum_p\sum_q\left[F_n^{(l_n)}(x_{\text{р}},y_q)\right]^2\right\}}, \quad (2)$$

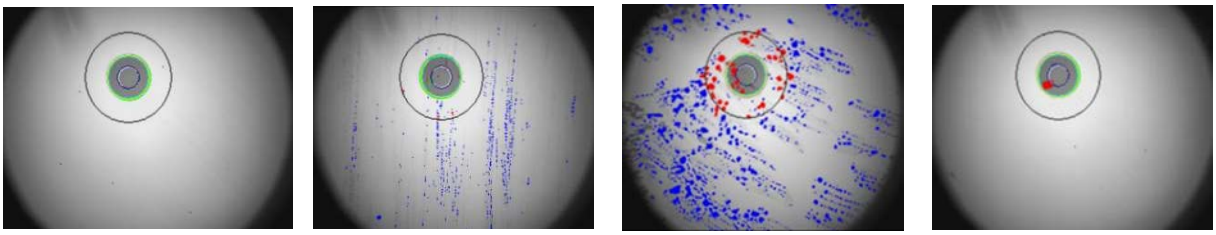
где $F_m^{(l_{\text{м}})}$ и $F_n^{(l_{\text{п}})}$ – радиальные распределения полей взаимодействующих мод – поступающей / вводимой «Tx»-моды LP_{lm} и возбуждаемой «Rx»-моды LP_{ln}; l, m и n – азимутальный и радиальные порядки мод LP_{lm} и LP_{ln}, соответственно; x и y – координаты Декартовой системы координат.

Формально радиальные распределения полей взаимодействующих мод могут быть непосредственно корректно рассчитаны через представление,

например, в базисе функций Лагерра-Гаусса либо с помощью строгих численных методов, где в качестве исходных данных могут использоваться протоколы измерений профиля показателя преломления промышленных образцов ОВ, выполненных с помощью штатных лабораторных комплектов анализаторов волоконных световодов. Подобное «сеточное» представление соединения ОВ позволяет вводить нулевые компоненты радиального распределения поля вводимой и/или возбуждаемой моды в загрязненных локациях сердцевин стыкуемых ОВ и, как результат, учитывать данный фактор в итоговом значении коэффициента связи. Иными словами, предлагаемый подход позволяет использовать в качестве исходных данных непосредственно фотографии торцов феррул коннекторов анализируемого разъемного соединения, получаемые штатными полевыми комплектами видеодиагностики (например, [7]).

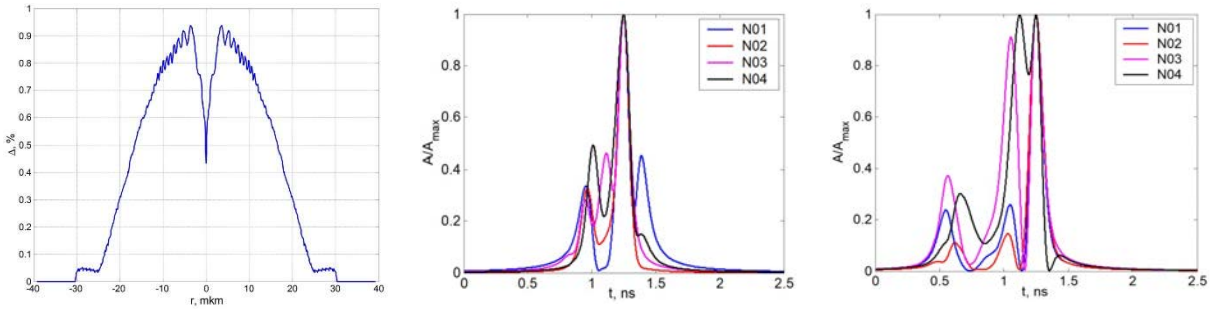
В свою очередь, согласно [3–6], используется представление анализируемого разъемного соединения в виде эквивалентного стыка ОВ с введенным заданным прецизионным радиальным рассогласованием и дискретизацией полей взаимодействующих мод, с учетом искажения последних за счет загрязнения торца ОВ путем наложения соответствующим образом предварительно обработанного в соответствии с ранее разработанной методикой изображения феррула.

Для апробации дополненной модели ВОЛП проведен расчет огибающей оптического импульса волоконно-оптической системы передачи (ВОСП) спецификации 10GBase-LX (10 Гбит/с, λ = 1 310 нм) при распространении в ММ ОВ кат. ISO/IEC OM2. Нерегулярная структура ОВ была представлена в виде флуктуаций диаметра сердцевины, при этом распределение значений указанного параметра задавались на основе серии протоколов датчиков контроля внешнего диаметра ОВ, измеряемого в процессе вытяжки строительной длины световода [8]. Предполагается, что ввод излучения с выхода лазера в многомодовое ОВ линии осуществляется без применения специализированных устройств согласования непосредственно через типовую проходную оптическую розетку. Рассматривались следующие 4 варианта ввода: здесь торец феррула коннектора пигтейла лазерного диода (ЛД) выбирался как успешно прошедший тест по всем трем зонам ABC [7], в то время как феррул коннектора пигтейла соединяемого ММ ОВ линии был загрязнен в разной степени и характере вплоть до полного «провала» тестов по всем трем зонам ABC (рис. 1).



(а) (б) (в) (г)

Рис. 1. Изображения (фотографии) фрагмента торца
феррула коннектора разъемного соединения на передающей стороне:
(а) № 1 чистый торец, тест АВС пройден;
(б) № 2 сильное загрязнение, тест АВС не пройден;
(в) № 3 экстремально сильное загрязнение, тест АВС не пройден;
№ 4 умеренное загрязнение, АВ не пройден, С пройден



(а) (б) (в)

Рис. 2. Результаты расчета огибающей оптического импульса системы 10GBase-LX
(B = 10 Гбит/с, λ = 1 310 нм), в «контрольных точка» ВОЛП:
(а) профиль показаиеля преломления ММ ОВ ВОЛП; (б) 250 м; (в) 500 м.

На рис. 2 представлены градиентный профиль показателя преломления ММ ОВ 50/125 моделируемой линии, восстановленный по данным протокола измерения ММ ОВ кат. ОМ2 и результаты расчета огибающей оптического импульса ВОСП 10GBase-LX на выходе указанной многомодовой ВОЛП длиной 250 и 500 м.

Анализ полученных результатов наглядно демонстрирует необходимость контроля качества подготовки (очистки) торцов феррул волоконно-оптических коннекторов разъемных соединений линейного тракта ВОЛП с ММ ОВ, функционирующих в маломодовом режиме передачи сигналов мультигабитных ВОСП, трансиверы которых оснащены когерентными источниками оптического излучения. Из полученных данных, хорошо видно, что для всех трех сопоставляемых вариантов ввода с загрязненными коннекторами (ни один из которых не прошел тест в зоне А) на вводе характер и степень проявления искажения оптического импульса проявляется неодинаково и существенно отличается для случая чистого торца феррула.

Работа подготовлена при финансовой поддержке РФФИ в рамках научного проекта № 19-37-90150 «Аспиранты».

Список используемых источников

1. Bourdine A. V. Modeling and simulation of piecewise regular multimode fiber links operating in a few-mode regime // Advances in Optical Technologies. 2013. Vol. 2013. P. 469389-1–469389-18.

2. Агравал Г. Нелинейная волоконная оптика. М.: Мир, 1996. 323 с.

3. Bourdine A. V., Bylina M. V., Pashin S. S., Praporshchikov D. E., Zaitseva E. S. Method for estimation of reflection on fiber optic connection based on ferrule end-face photo-image analysis // Proceedings of SPIE. 2021. Vol. 11793. P. 1179319-1–1179319-12

4. Бурдин А. В., Пашин С. С. Оценка коэффициента отражения на разъемном соединении одномодовых оптических волокон по результатам анализа фотографий торцевых поверхностей феррул коннекторов // Труды учебных заведений связи. 2020. Т. 6, № 4. С. 16–27.

5. Bourdine A. V., Pashin S. S, Giniatulina A. M., Vasilets A. A., Antonov S. A. Fast and simple method for estimation of the insertion loss at the connection of singlemode optical fibers with contaminated ferrule end faces // Proceedings of SPIE. 2019. Vol. 11516. P. 115161O-1–115161O-11.

6. Bourdine A. V., Pashin S. S, Giniatulina A. M., Vasilets A. A., Antonov S. A. Development and approbation of procedure for automated localization of fiber optic connector contaminated ferrule end face image artifacts // Proceedings of SPIE. 2019. Vol. 11146. P. 111461N-1–111461N-12.

7. Westover FBP P-5000 FiberCheck2™. Руководство пользователя: Пер. с англ., 2008. 58 с.

8. Demidov V. V., Ter-Nersesyants E. V., Bourdine A. V., Burdin V. A., Minaeva A. Yu., Matrosova A. S., Khokhlov A. V., Komarov A. V., Ustinov S. V., Golyeva E. V., Dukelskii K. V. Methods and technique of manufacturing silica graded-index fibers with a large central defect of the refractive index profile for fiber-optic sensors based on few-mode effects // Proceedings of SPIE. 2017. Vol. 10342. P. 103420X-1–103420X.

Статья представлена научным руководителем, доктором технических наук, профессором кафедры ЛС и ИТС ПГУТИ А. В. Бурдиным.

УДК 004.05
ГРНТИ 81.93.29

ПОДХОД К ФОРМИРОВАНИЮ ПРАВИЛ ФИЛЬТРАЦИИ В СИСТЕМЕ ЗАЩИТЫ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ

В. В. Бухарин[1], **Е. С. Долгирева**[2], **А. С. Никитин**[3]

[1]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
[2]ЗАО «Защита электронных технологий»
[3]АО «НИИ «Рубин»

В статье рассматривается подход формирования правил фильтрации в системе информационно-телекоммуникационная сети, за счет дополнительного анализа «Черного» списка IP-адресов используя временные параметры, при реализации деструктивных программных воздействий.

информационно-телекоммуникационная сеть, деструктивные программные воздействия, правила фильтрации.

В настоящее время системы защиты информационно-телекоммуникационных сетей (ИТКС) от компьютерных атак находятся в постоянном развитии, что связанно с постоянным увеличением, как их количества, так и многообразия, что в свою очередь напрямую зависит от расширения вида средств и оборудования ИТКС, а также от увеличения их функциональности.

В современных системах защиты ИТКС от компьютерных атак одним из основных элементов являются межсетевые экраны. При этом основой работы межсетевых экранов является фильтрация информационного трафика, в основном основанная на списках *IP*-адресов, так называемых «Черных» списков, являющиеся адресами выявленных подозрительных сетевых узлов [1].

Существующий подход формирования «Черных» списков *IP*-адресов определяется, как правила фильтрации трафика являются результатом действия правил антиспуфинга, выбранного режима безопасности для каждого сетевого интерфейса. При этом «Черные» списки *IP*-адресов формируются специализированными в области информационной безопасности организации и в дальнейшем используется в системах защиты ИТКС с возможностью периодического обновления, что делает их недостаточно актуальными и имеющие достаточно низкую оперативность при появлении новых.

Фильтрация трафика осуществляется с учетом установленных соединений, то есть соединений, образующихся на основании разрешенного правилами входящего или исходящего пакета, при этом фиксируются разные параметры этих пакетов. На основании полученных данных создается временное правило соединения для дальнейшего пропуска пакетов в прямом и обратном направлении. Такое правило существует, пока есть трафик, соответствующий данному соединению [2].

Основной атакой с возможностью и необходимостью постоянного обновления IP-адресов является атаки «отказ в обслуживании» (*DDoS*), которые существенно влияют на доступность информационных ресурсов. Атака «отказ в обслуживании» считается успешной, если она привела к недоступности информационного ресурса. В данном случае речь идет о большом количестве злонамеренных запросов, поступающих на сервер из множества разных мест. Обычно такие атаки организуются посредством бот-сетей. Бот-сеть генерирует большое количество запросов к серверу, что приводит к превышению допустимой нагрузки на сервер и, следовательно, отказу в обслуживании легитимных пользователей [6].

Для формирования правил фильтрации предлагается подход, который основан на необходимости дополнительного анализа параметров *IP*-пакетов в ходе мониторинга сетевого трафика. Под мониторингом сети понимают процесс сбора и анализа сетевого трафика, по результатам которого можно судить о качественных и количественных характеристиках работоспособности сети или ее отдельных компонентов. Программы мониторинга сети позволяют выполнять захват пакетов и их реассемблирование для дальнейшего анализа [3].

При этом сохраняются данные о *IP*-адресе отправителя и *IP*-адресе получателя, а также количество *IP*-пакетов, переданных между этими парами [5]. Кроме того, присваивают всем соединениям на сервере информационной безопасности (ИБ) численный идентификатор. Таким образом, формируется массив $i = \{1 \ldots I\}$, где i – номер соединения, I – количество соединений на сервере ИБ. При этом каждому соединению будет соответствовать *IP*-адрес с которого происходит обращение к серверу.

В дальнейшем при определении сервером ИБ инцидента соответствующего реализации *DDoS* атаки сбрасывают все текущее соединения. Это осуществляется для возможности в дальнейшем на основе параметров повторного запроса на сеанс к серверу ИБ определить является ли узел элементом бот-сетей. Формальные признаки, по которым можно определить *DDoS* атаку представлены в [7].

При получении повторных запросов от ранее зафиксированных *IP*-адресов производится определение промежутков времени t_i до повторного запроса на восстановление соединений имеющие соответствующие иденти-

фикаторы, которые сохраняются в массив памяти T. В формируемом массиве памяти T храниться значения промежутков времени от сброса соединения до повторного запроса на восстановление $t_i = \{t_1 \ldots t_I\}$ для всех соединений сервера ИБ.

После этого, осуществляется проверка наличия совпадений определенных значений промежутков времени t_i из массива T. В случае совпадений нескольких значений промежутков времени соответствующие соединения объединяют в массив P_1. При наличии последующих совпадений других значений промежутков времени соответствующие соединения объединяют в массив P_j. Таким образом, после полной проверки массива T на наличии совпадений значений промежутков времени t_i будут сформированы J массивов P, т. е. определенные соединения будут объединены в массивы учитывая их одинаковые значения промежутков времени t_i.

Для осуществления *DDoS* атак злоумышленник формирует бот-сеть, которая состоит из компьютеров-зомби зараженные ботом управляемых удаленно (рис.). Под ботом понимается программа, выполняющая определенные действия, например, отправка пакетов на атакуемый компьютер, по командам удаленного центра управления – компьютера злоумышленника [8].

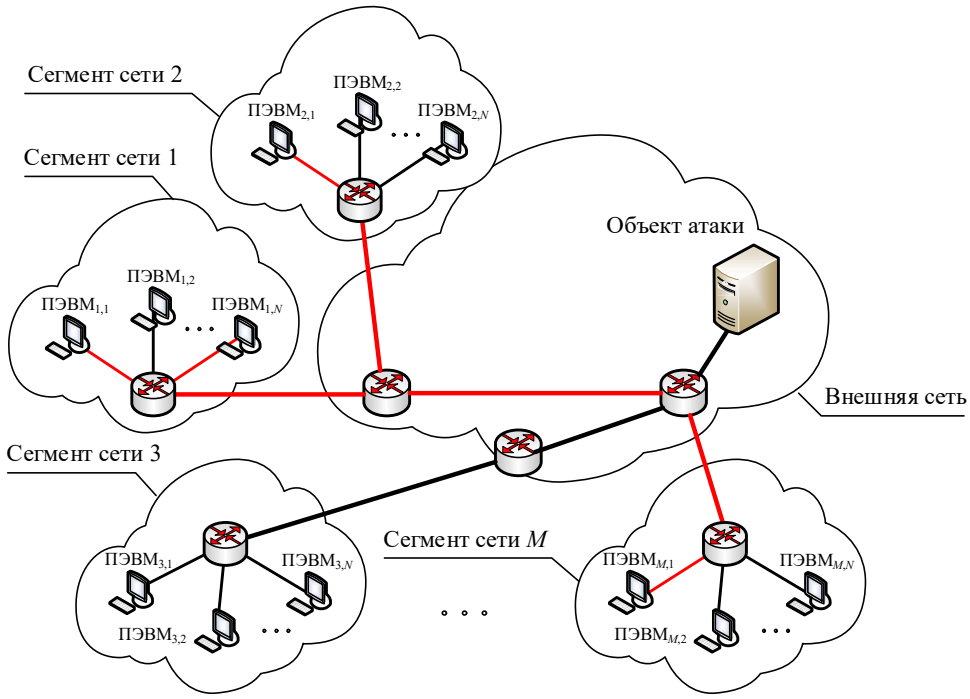


Рисунок. Схема поясняющая формирование бот-сети

В большинстве случаях бот-сети организуются злоумышленником из существенно большого количества компьютеров расположенных в непосредственной близости к атакуемому компьютеру, что упрощает реализацию *DDoS* атаки и гарантирует ее успешное завершение.

На рисунке выделены компьютеры из сегментов сети являющимися бот-сетью и осуществляющие *DDoS* атаку на компьютер, расположенный во внешней сети.

При этом на компьютерах-зомби, входящих в одну и ту же бот-сеть, злоумышленник устанавливает одну и ту же управляющую программу. Учитывая, что действия, выполняемые на компьютерах-зомби одни и те же, то и запросы на повторные соединения на сервер услуг при реализации *DDoS* атаки будут производиться через достаточно одинаковые (имеющие существенно небольшое расхождение значений) промежутки времени после сброса соединения, что позволяет использовать их в качестве дополнительного параметра при анализе сетевого трафика по *IP*-адресам.

Таким образом, из имеющихся соединений на сервере ИБ будут сформированы множества $P_j = \{1 \ldots J\}$, где J – количество зафиксированных бот-сетей, узлов сети имеющие определенные *I*P-адреса, которые объединяются в дополнительный «Черный» список.

В качестве выводов необходимо отметить то, что «Черный» список *IP*-адресов сформированный при дополнительном анализе позволяет более точно определить принадлежность узлов сети к бот-сетями злоумышленника, даже если в бот-сетях осуществляются изменения конфигураций. Кроме того, дополнительные правила фильтрации являются наиболее достоверными так, как учитывают реальное состояние активности злоумышленников в ИТКС, и могут динамически изменяться в соответствии с текущим состоянием фактически в режиме реального времени.

Список используемых источников

1. Справка Dr. Web. Черный и «Белый» списки. URL: http://download.geo.drweb.com (дата обращения: 10.11.2021).

2. Основные принципы фильтрации. URL: http://mybiblioteka.su (дата обращения: 12.11.2021)

3. Мониторинг сети. Сниффер Wireshark. URL: http://www.4stud.info (дата обращения: 13.11.2021)

4. Мониторинг сетевого трафика с помощью Netflow. URL: http://www.opennet.ru (дата обращения: 14.11.2021)

5. Отчеты наборов элементов сбора системных данных. URL: https://msdn.microsoft.com (дата обращения: 12.11.2021)

6. DDoS-атаки: типы атак и уровни модели OSI. URL: https://firstvds.ru (дата обращения: 15.11.2021)

7. Определение DoS/DDoS атак на сервер. URL: https://www.stableit.ru (дата обращения: 15.11.2021)

2. Олифер В. Г., Олифер Н. А. Компьютерные сети. Принципы, технологии, протоколы. 5-е изд. СПб.: Питер, 2016. 928 с.

УДК 621.39
ГРНТИ 49.44

УПРАВЛЯЕМЫЙ ПЕРЕМЕННЫЙ АТТЕНЮАТОР ОТРАЖАЮЩЕГО ТИПА

А. Р. Былин, М. С. Былина, А. О. Николаенко

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В работе моделируется переменный оптический аттенюатор, основным элементом которого является микроэлектромеханическая система (MEMS), представляющая собой матрица микрозеркал, каждое из которых может находиться в одном из двух положений. Излучение из входного оптического волокна коллимируется и попадает на массив микрозеркал. Зеркала в зависимости от их текущего положения отражают излучение так, что оно либо попадает (положение 1), либо не попадает (положение 2) в выходное оптическое волокно. Если все зеркала находятся в положении 1, аттенюатор вносит минимальное собственное затухание. Переводя часть зеркал в положение 2, можно увеличивать затухание. В работе рассчитана зависимость внесенного затухания от числа зеркал, переведенных в положение 2, оценена точность установки затухания.

переменный оптический аттенюатор, Variable Optical Attenuator, VOA, микроэлектромеханическая система, MEMS, волоконно-оптическая система связи.

Переменные оптические аттенюаторы (*Variable Optical Attenuator*, VOA) применяются для управления мощностью излучения в волоконно-оптических системах связи (ВОСС).

В [1] описан VOA, основным элементом которого является микроэлектромеханическая система (MEMS), представляющая собой матрица микрозеркал (рис. 1). Излучение из выходного оптического волокна (ОВ) коллимируется GRIN линзой и попадает на матрицу подвижных микрозеркал (МЗ). Каждое МЗ может находиться в одном из двух положений – под углами +θ или –θ к поверхности матрицы.

МЗ расположены так, чтобы захватить большую часть падающего излучения (рис. 2). В зависимости от угла МЗ будет отражать падающее на него излучение либо в сторону выходного ОВ (+θ), либо в сторону контрольного ОВ (–θ).

Затухание VOA можно определить следующим образом:

$$A = 10 \cdot \lg\left(I_{in} / I_{out}\right), \quad (1)$$

где I_{in} и I_{out} – интенсивности излучения во входном и выходном ОВ.

Если все МЗ находятся в положении +θ, VOA вносит минимальное затухание, определяемое потерями на вводе и выводе излучения в ОВ, потерями в коллиматорах и потерями в матрице МЗ. Если часть зеркал перевести в положение –θ, отражаемое ими излучение будет перенаправлено в контрольное ОВ, мощность излучения P_{out} в выходном ОВ уменьшится, и затухание VOA возрастет.

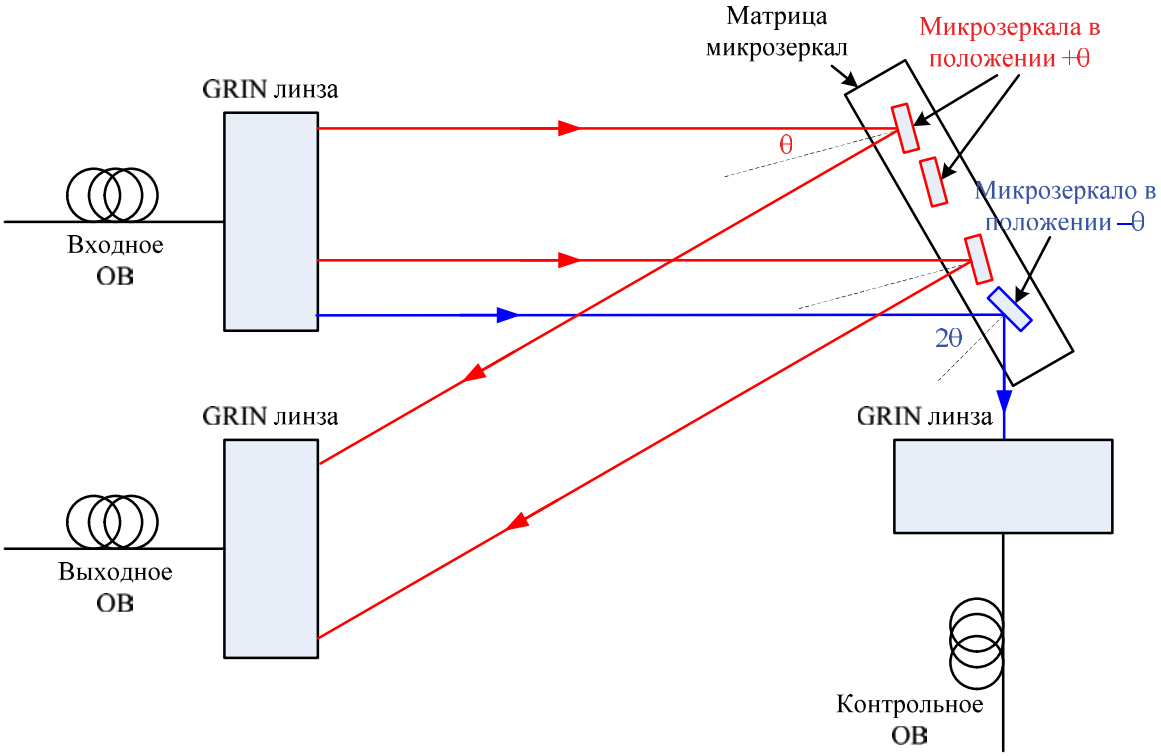


Рис. 1. Конструкция моделируемого аттенюатора

В [2] описана матрица, содержащая 500 тысяч квадратных МЗ размером 16×16 мкм^2 с расстоянием 17 мкм между соседними МЗ. Будем считать, что в нашем аттенюаторе используется матрица из МЗ такого размера, то есть с учетом зазоров между МЗ: $d = d_x = d_y$ =16.5 мкм.

Будем полагать распределение напряженности электрического поля E в коллимированном пучке гауссовым с радиусом в области перетяжки W_0 = 0.45 мм. Предположим также, что матрица МЗ расположена под углом

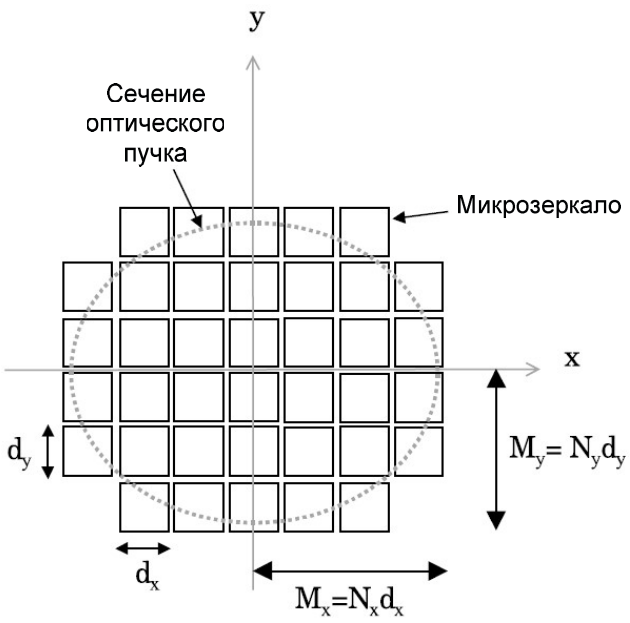


Рис. 2. Матрица микрозеркал

$\alpha = 45^0$ к оптической оси входного ОВ. Тогда излучение из ОВ образует на ней эллиптическое пятно с отношением полуосей, равным 1 / cos α, и для максимального числа МЗ вдоль осей *X* и *Y* (рис. 2) можно записать:

$$N_y / N_x = \cos\alpha . \tag{2}$$

Общее число микрозеркал *N* можно оценить как отношение площади пятна, засвеченного коллимированным пучком на поверхности матрицы, к площади одного МЗ:

$$N = \pi M_x M_y / d^2 . \tag{3}$$

Радиус коллимированного пучка W_m в месте расположения матрицы будет равен [3]:

$$W_m = W_0 \sqrt{1 + \left(\lambda \cdot l_m / \left(\pi W_0^2\right)\right)^2} , \tag{4}$$

где λ – длина волны излучения, l_m – расстояние от коллиматора до матрицы. Для W_x и W_y вдоль осей *X* и *Y* получаем:

$$W_x = W_m / \cos\alpha , \; W_y = W_m \tag{5}$$

Найдем интенсивность излучения, падающего на микрозеркала:

$$I_m = E_0^2 \int_{-M_x}^{M_x} \int_{-M_y}^{M_y} \exp\left(\frac{-2x^2}{W_x^2}\right) \exp\left(\frac{-2y^2}{W_y^2}\right) dx dy . \tag{6}$$

Полная интенсивность излучения в пучке равна:

$$I_0 = E_0^2 \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} \exp\left(\frac{-2x^2}{W_x^2}\right) \exp\left(\frac{-2y^2}{W_y^2}\right) dx dy = \frac{E_0^2}{2} \pi W_x W_y . \tag{7}$$

Из (5) и (7) получаем:

$$I_m = I_0 \cdot \mathrm{erf}\left(\sqrt{2M_x / W_x}\right) \cdot \mathrm{erf}\left(\sqrt{2M_y / W_y}\right). \tag{8}$$

Учитывая соотношения (2), перепишем (7) в виде:

$$I_m = I_0 \cdot \mathrm{erf}\left(\sqrt{2N_x(d+\Delta d)/W_x}\right) \cdot \mathrm{erf}\left(\sqrt{2N_y(d+\Delta d)/W_y}\right). \quad (9)$$

Если принять, что N_{x+} и N_{y+} определяют число зеркал, отражающих свет в выходное ОВ, то есть находящихся в положении +θ, из (9) и (1) получим выражение для затухания аттенюатора A:

$$A = -10 \cdot \lg\left[\mathrm{erf}\left(\sqrt{2N_{x+}d/W_x}\right) \cdot \mathrm{erf}\left(\sqrt{2N_{y+}d/W_y}\right)\right]. \quad (10)$$

Если все зеркала находятся в положении +θ, интенсивность излучения в выходном ОВ $I_{out} = I_m$. На рис. 3 представлены зависимости $A_{\min}$ от максимального числа МЗ по оси Y. Длина волны излучения была принята равной 1.55 мкм.

Из рис. 3 видно, что для получения $A_{\min} \le 0.05$ дБ число МЗ по оси Y должно быть не меньше 27. Учитывая (2), для дальнейших расчетов примем $N_y = 27$ и $N_x = 38$. Из (3) следует, что общее число МЗ будет равным $N = 3\,239$.

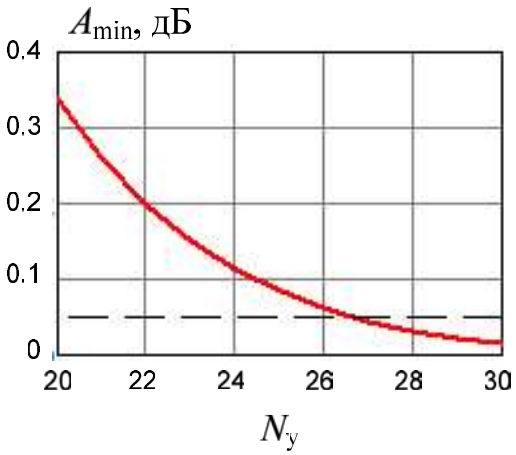


Рис. 3. Определение числа МЗ

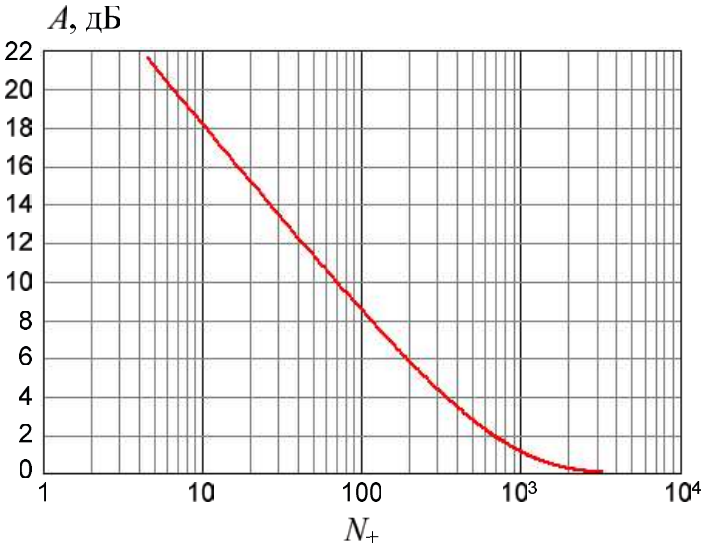


Рис. 4. Зависимость затухания VOA от числа МЗ, находящихся в положении +θ

На рис. 4 представлена зависимость затухания VOA от N_+ – общего числа МЗ, отражающих свет в выходное ОВ, то есть находящихся в положении +θ. При расчете полагалось, что для увеличения затухания одновременно поворачиваются все МЗ внутри кольца, ограниченного двумя эллипсами с радиусами N_{x+}+1, N_{y+}+1 и N_{x+}, N_{y+}.

Из рис. 4 видно, что смоделированное устройство позволяет управлять затуханием в диапазоне до 22 дБ. Если количество МЗ N_+, отражающих свет в выходное ОВ, не превышает 500, зависимость A от lg N_+ является почти линейной.

Список используемых источников

1. Sumriddetchkajorn S., Riza N.A. Fault-tolerant three-port fiber-optic attenuator using small tilt micromirror device // Optics Communications. 205 (2002). pp. 77–86.

2. Knipe R. L. Challenges of a Digital Micromirror Device: modeling and design// Micro-optical Technologies for Measurement, Sensors, and Microsystems // Proc. SPI. Vol. 2783. 1996. p. 135.

3. Распространение Гауссова пучка: понятие перетяжки пучка, глубины фокусировки, качества пучка, расходимости // Edmund Optics Inc., 2020. URL: https://in-science.ru/library/article_post/rasprostranenie-gaussova-puchka

УДК 681.7
ГРНТИ 49.44

МОДЕЛИРОВАНИЕ И ИССЛЕДОВАНИЕ ПОЛЯРИЗАЦИОННОГО РАЗВЕТВИТЕЛЯ

А. Р. Былин, М. С. Былина, В. О. Пак, А. С. Фролова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Поляризационным разветвителем или поляризационным делителем называют оптическое устройство, разделяющее падающий световой пучок на два пучка с взаимно перпендикулярными состояниями линейной поляризации. В работе рассмотрен поляризационный делитель конструкции С. Мак-Нейла. Основным элементом делителя является многослойная тонкопленочная структура, состоящая из чередующихся слоев с высоким и низким показателями преломления. Структура наносится на гипотенузную поверхность прямоугольной призмы, которая затем склеивается с другой такой же призмой, образуя куб. Для анализа работы делителя проведено его моделирование в программе COMSOL Multiphysics. Получены зависимости коэффициентов отражения и пропускания делителя для каждой из поляризаций от длины волны и числа слоев в многослойной структуре.

поляризационный разветвитель, поляризационный светоделительный куб, конструкция Мак-Нейла, угол Брюстера, линейная поляризация, коэффициент отражения.

Поляризационные разветвители пучка – это оптические устройства, разделяющие световой пучок на два пучка с ортогональными линейными

поляризациями *p* (поляризация в плоскости падения) и *s* (поляризация перпендикулярно плоскости падения).

Одна из наиболее распространенных конструкций поляризационных разветвителей – поляризационный куб С. Мак-Нейла представлена на рис. 1. Куб состоит из двух прямоугольных призм, изготовленных из материала с показателем преломления n_G. На гипотенузную поверхность одной из призм нанесено многослойное диэлектрическое покрытие, состоящее из тонких пленок. Пучок света направляется на покрытие, в результате интерференции в пленках свет *s*-поляризации отражается, а свет *p*-поляризации проходит через покрытие.

Толщина, показатели преломления и количество пленок подбираются так, чтобы коэффициенты отражения R_s для *s*-поляризации и пропускания T_p для *p*-поляризации были примерно равны 1. Чаще всего применяется периодическая структура, период которой состоит из двух пленок с показателями преломления $n_H > n_G$ (слой *H*) и $n_L < n_G$ (слой *L*).

Предположим, что угол падения луча на покрытие составляет $\theta_G = 45^0$. Закон Снеллиуса позволяет рассчитать углы преломления луча θ_H и θ_L в слоях покрытия:

$$\sin\theta_H = \frac{n_G \sin\theta_G}{n_H} = \frac{n_G}{n_H\sqrt{2}},\ \sin\theta_L = \frac{n_G \sin\theta_G}{n_L} = \frac{n_G}{n_L\sqrt{2}}. \qquad (1)$$

Потребуем, чтобы на границы раздела слоев *H* и *L* преломленные лучи падали под углом Брюстера. Тогда независимо от толщины слоев *p*-поляризация будет проходить, а *s*-поляризация – отражаться от границ. Можно показать, что при выполнении этого требования справедливо:

$$n_H/\cos\theta_H = n_L/\cos\theta_L. \qquad (2)$$

Из (1) и (2) следует соотношение между показателями преломления призмы и слоев *H* и *L* (условие Мэри Баннинг):

$$n_G^2 = 2n_H^2 n_L^2/\left(n_H^2 + n_L^2\right). \qquad (3)$$

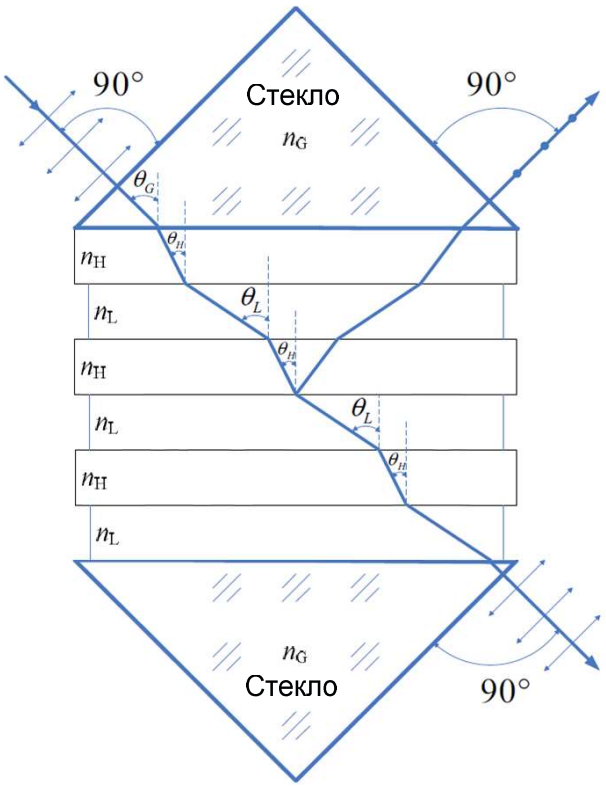


Рис. 1. Поляризационный куб С. Мак-Нейла

Коэффициенты отражения от поляризационного куба для *s* и *p*-поляризаций могут быть рассчитаны по формуле [1]:

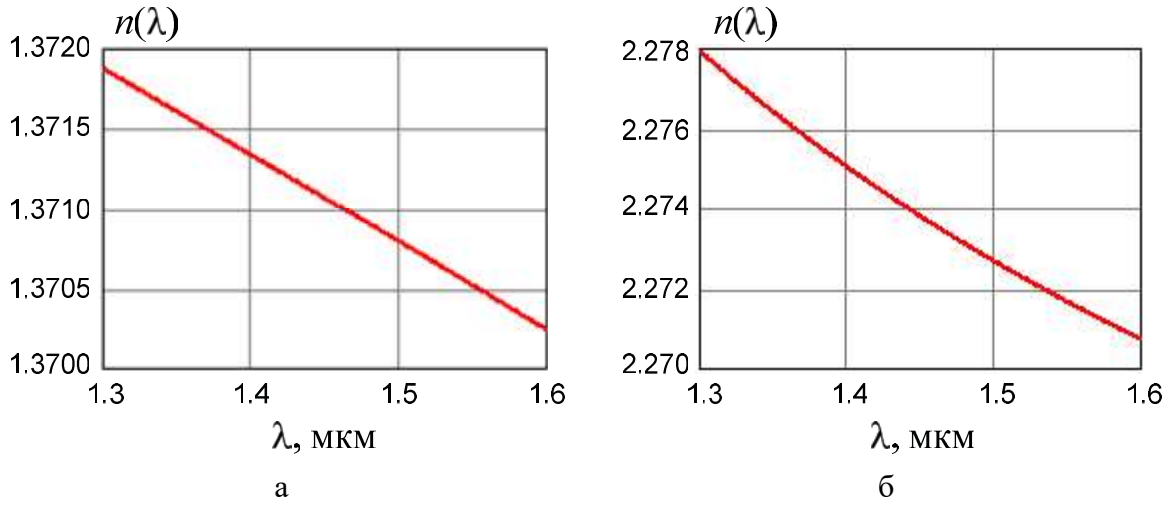
$$R = \left[\frac{\eta_G - \left(\eta_H^2 / \eta_G\right)\left(\eta_H / \eta_L\right)^{2 \cdot N - 1}}{\eta_G + \left(\eta_H^2 / \eta_G\right)\left(\eta_H / \eta_L\right)^{2 \cdot N - 1}} \right]^2, \quad (4)$$

где N – число периодов в многослойном покрытии, а параметры η определяются для двух поляризаций следующим образом:

s-поляриз.: $\eta_G = n_G \cos\theta_G$, $\eta_H = n_H \cos\theta_H$, $\eta_L = n_L \cos\theta_L$ (5)

p-поляриз.: $\eta_G = n_G / \cos\theta_G$, $\eta_H = n_H / \cos\theta_H$, $\eta_L = n_L / \cos\theta_L$ (6)

Выберем в качестве материалов сульфид цинка (слой *H*) и фторид магния (слой *L*). Зависимости показателей преломления этих материалов от длины волны представлены на рис. 2.



а б

Рис. 2. Зависимости n_L (а) и n_H (б) от длины волны [2]

На рис. 2 показаны теоретически рассчитанная по (3) зависимость показателя преломления материала призмы от длины волны и наиболее близкие к ней зависимости – для стекол Schott SF5 и LaK [2].

Для дальнейшего исследования в качестве материала призмы было выбрано стекло LaK. Из рис. 3 видно, что его показатель преломления немного больше теоретически рассчитанного.

В работе было проведено моделирование рассматриваемого устройства в COMSOL Multiphysics [3]. Параметры моделируемого устройства и падающего излучения приведены в табл.

На рис. 4 представлены результаты моделирования распределения напряженности электрического поля для излучения *s* и *p*-поляризаций. На обоих графиках видно, что устройство неидеально: часть излучения *s*-поляризации проходит через куб, а часть излучения *p*-поляризации – отражается.

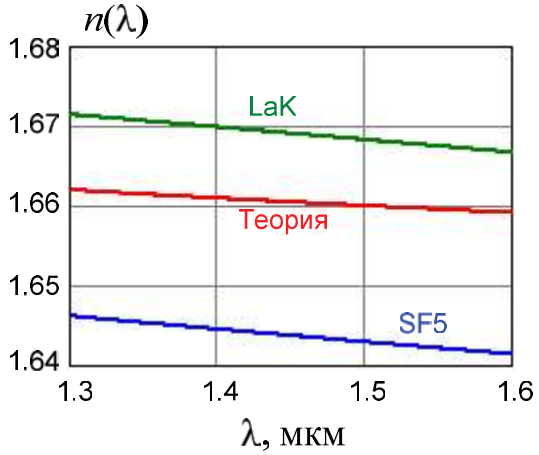
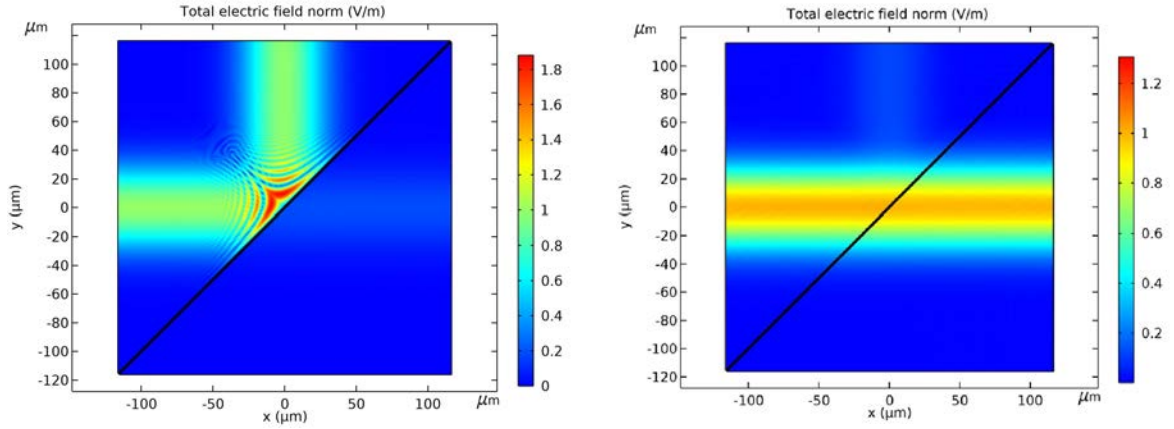


Рис. 3. Зависимости n_G от длины волны

ТАБЛИЦА. Параметры моделируемого устройства и падающего излучения

№	Параметр	Значение	№	Параметр	Значение
1	Высота грани куба, мкм	233	4	Толщина слоя L, нм	498.5
2	Число периодов в многослойной структуре	4	5	Длина волны, мкм	1.45
3	Толщина слоя H, нм	185.5	6	Диаметр падающего гауссова пучка, мкм	29

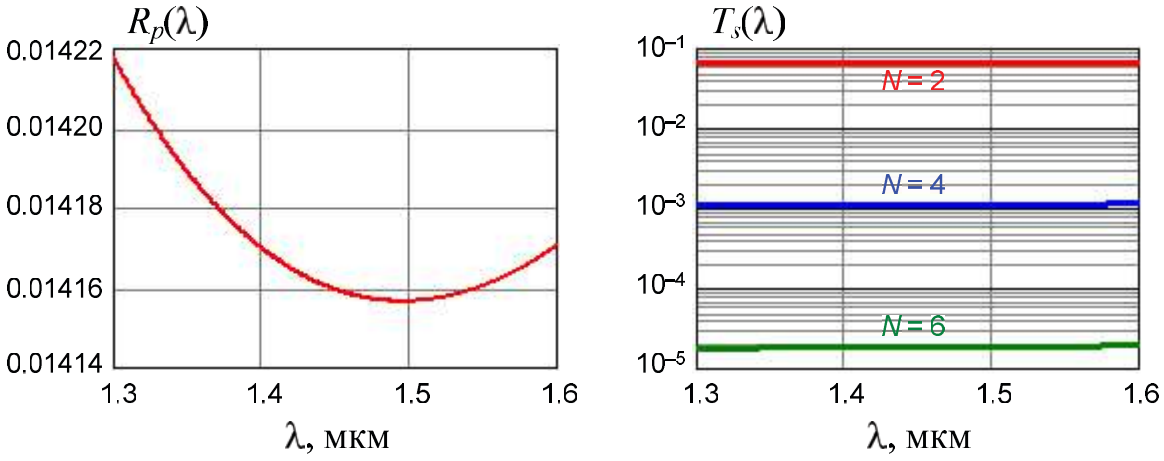


а б

Рис. 4. Распределение напряженности электрического поля для излучения *s*-поляризации (а) и *p*-поляризации (б)

Оценим качество поляризационного куба, изготовленного из выбранных материалов. На рис. 5 представлены рассчитанные по (4)–(6) зависимости коэффициентов пропускания T_s для *s*-поляризации и отражения R_p для

p-поляризации от длины волны, которые для идеального устройства должны быть равны 0.



а б

Рис. 5. Зависимости R_p (а) и T_s (б) от длины волны

Из рис. 5 видно, что коэффициент пропускания для *s*-поляризации быстро уменьшается с увеличением числа периодов в многослойной структуре. Коэффициент отражения для *p*-поляризации не зависит от числа слоев и определяется только соотношением показателей преломления выбранных материалов.

Список используемых источников

1. Peng G., Ye R., Yang J., Chang S., Yang J. Design of MacNeille Polarizing Beam Splitter // Symposium on Photonics and Optoelectronics. 2009.

2. Полянский М. База данных показателей преломления оптических материалов Refractive index database // Санкт-Петербургский государственный университет. URL: https://refractiveindex.info/

3. Программное обеспечение COMSOL Multiphysics. URL: https://www.comsol.ru/

УДК 535.14, 372.862
ГРНТИ 29.05.15, 29.01.45

ВИРТУАЛЬНАЯ ЛАБОРАТОРНАЯ УСТАНОВКА ДЛЯ ИЗУЧЕНИЯ ИНТЕРФЕРЕНЦИИ ОДИНОЧНЫХ ФОТОНОВ

М. С. Былина, А. В. Фраз

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье представлена виртуальная лабораторная установка, моделирующая работу интерферометра Маха-Цендера и позволяющая наблюдать процессы распространения в нем одиночных фотонов. На базе этой установки предложена лабораторная работа, в которой студенты закрепляют знания о квантовых объектах, квантовом состоянии и квантовой суперпозиции, экспериментально обнаруживают и исследуют явление интерференции одиночных фотонов. Подготовлены методические указания к лабораторной работе, содержащие теоретическое описание изучаемых явлений, задания для выполнения экспериментальных исследований и контрольные вопросы для проверки степени усвоения учебного материала.

интерференция, квантовое состояние, одиночный фотон, интерферометр Маха-Цендера, корпускулярно-волновой дуализм, виртуальная лабораторная работа.

Вопрос о том, ведёт ли себя свет как частица или волна долгое время обсуждался учёными. Гипотезу о корпускулярном строении света отстаивал Ньютон. Исследования Френеля и Юнга свидетельствовали в пользу волновой теории света [1]. Констатируя экспериментально наблюдаемый корпускулярно-волновой дуализм, Нильс Бор постулировал принцип дополнительности [2].

Предлагаемая в работе виртуальная лабораторная установка Interferometer experiments with single photons (интерферометрические эксперименты с одиночными фотонами) [3] позволяет студентам провести экспериментальные исследования, позволяющие наблюдать различное поведение фотонов – как корпускулярное, так и волновое, а также убедиться в существовании суперпозиционных состояний.

Установка (рис. 1) содержит источник одиночных фотонов S, интерферометр Маха-Цендера (ИМЦ), состоящий из двух полупрозрачных (BS1 и BS2) и двух непрозрачных (M1 и M2) зеркал, и два детектора одиночных фотонов D1 и D2 [5].

Источник испускает одиночный фотон, который проходит через ИМЦ и регистрируется одним из двух детекторов. Эксперимент можно повторять многократно, при этом виртуальная установка подсчитывает числа срабатываний N_1 и N_2 каждого детектора и вычисляет наблюдаемые вероятности срабатывания P_{1o} и P_{2o} по выражениям:

$$P_{1o} = N_1/N_{tot}\,, \quad P_{2o} = N_2/N_{tot}\,, \quad N_{tot} = N_1 + N_2\,. \tag{1}$$

Для расширения спектра исследований имеется возможность убирать из ИМЦ зеркало BS2, а также устанавливать на пути распространения фотона фазовращатели (ФВ) со сдвигами фаз 0.25π, 0.5π, 0.75π или 1.0π.

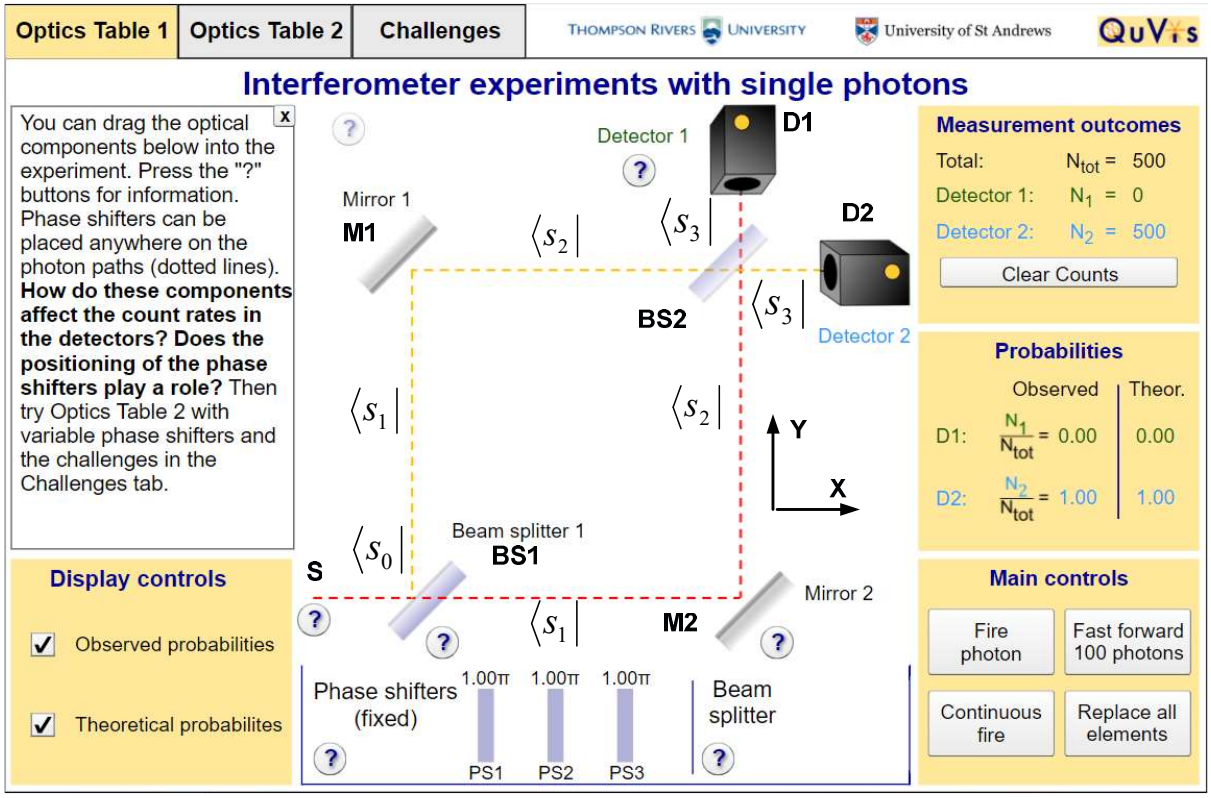


Рис. 1. Установка с интерферометром Маха-Цендера

Для закрепления теоретических знаний процессов распространения и регистрации фотонов и обоснования результатов эксперимента перед началом работы студентам предлагается провести расчеты вероятностей регистрации фотонов детекторами D1 и D2 в различных схемах, которые можно создать из перечисленных элементов. В основе расчета лежит представление фотона вектором состояния.

Предположим, что в данной схеме фотон может распространяться вдоль двух осей X или Y. Введем ортогональные векторы состояния для двух этих направлений распространения:

$$\langle x| = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \langle y| = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \tag{1}$$

Действие полупрозрачных зеркал BS1, BS2 и непрозрачных зеркал M1, M2 на вектор состояния можно описать операторами R и M соответственно [4]:

$$R = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix},\ M = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \tag{2}$$

где i – мнимая единица.

ФВ изменяет фазу фотона на заданную величину φ, не меняя направления его распространения. Действие ФВ на вектор состояния фотона описывается оператором [4]:

$$F = \begin{pmatrix} \exp(i\varphi) & 0 \\ 0 & \exp(i\varphi) \end{pmatrix}. \tag{3}$$

Распространение фотона между оптическими элементами также изменяет фазу фотона на величину:

$$\varphi_l = 2\pi l/\lambda, \tag{4}$$

где l – длина пути, λ – длина волны излучения. Изменение вектора состояния фотона при этом можно описать оператором F. Однако, поскольку в работе рассматривается интерферометр с двумя плечами одинаковой длины, указанное изменение фазы не повлияет на результаты расчета вероятностей регистрации фотона.

Рассмотрим эволюцию вектора состояния фотона в первой схеме (рис. 1), которая предлагается студентам для исследования. Фотон на входе ИМЦ характеризуется вектором состояния $\langle s_0| = \langle x|$. Найдем вектор состояния фотона, прошедшего первое полупрозрачное зеркало:

$$\langle s_1| = R\langle s_0| = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix}\cdot\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ i \end{pmatrix} = \frac{1}{\sqrt{2}}\left[\langle x| + i\cdot\langle y|\right]. \tag{5}$$

Таким образом, на выходе BS1 получаем фотон, находящийся в суперпозиции состояний $\langle x|$ и $\langle y|$. Определим вектор состояния фотона после отражения от зеркала:

$$\langle s_2| = M\langle s_1| = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\cdot\frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ i \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} i \\ 1 \end{pmatrix}. \tag{6}$$

И, наконец, определим вектор состояния фотона после взаимодействия со вторым полупрозрачным зеркалом:

$$\langle s_3| = R\langle s_2| = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & i\\ i & 1\end{pmatrix}\cdot\frac{1}{\sqrt{2}}\begin{pmatrix}i\\1\end{pmatrix} = \begin{pmatrix}i\\0\end{pmatrix} = i\langle x|. \qquad (7)$$

Теперь можно рассчитать вероятности регистрации фотона детекторами D1 (P_1), который принимает состояние $\langle y|$, и D2 (P_2), который принимает состояние $\langle x|$:

$$P_1 = \left(\langle y|\cdot\langle s_3|\right)^2 = 0, \quad P_2 = \left(\langle x|\cdot\langle s_3|\right)^2 = 1. \qquad (8)$$

Таким образом, при приеме одиночных фотонов в схеме на рис. 1 будет срабатывать только детектор D2. Этот эксперимент демонстрирует волновые свойства фотона, его интерференцию с самим собой.

Вторая предлагаемая студентам схема исследования представлена на рис. 2. В ней из ИМЦ убрано зеркало BS2. Расчеты по приведенным выше выражениям показывают, что вероятности срабатывания детекторов D1 и D2 будут одинаковыми и равными 0.5. В этом эксперименте фотон демонстрирует свои корпускулярные свойства.

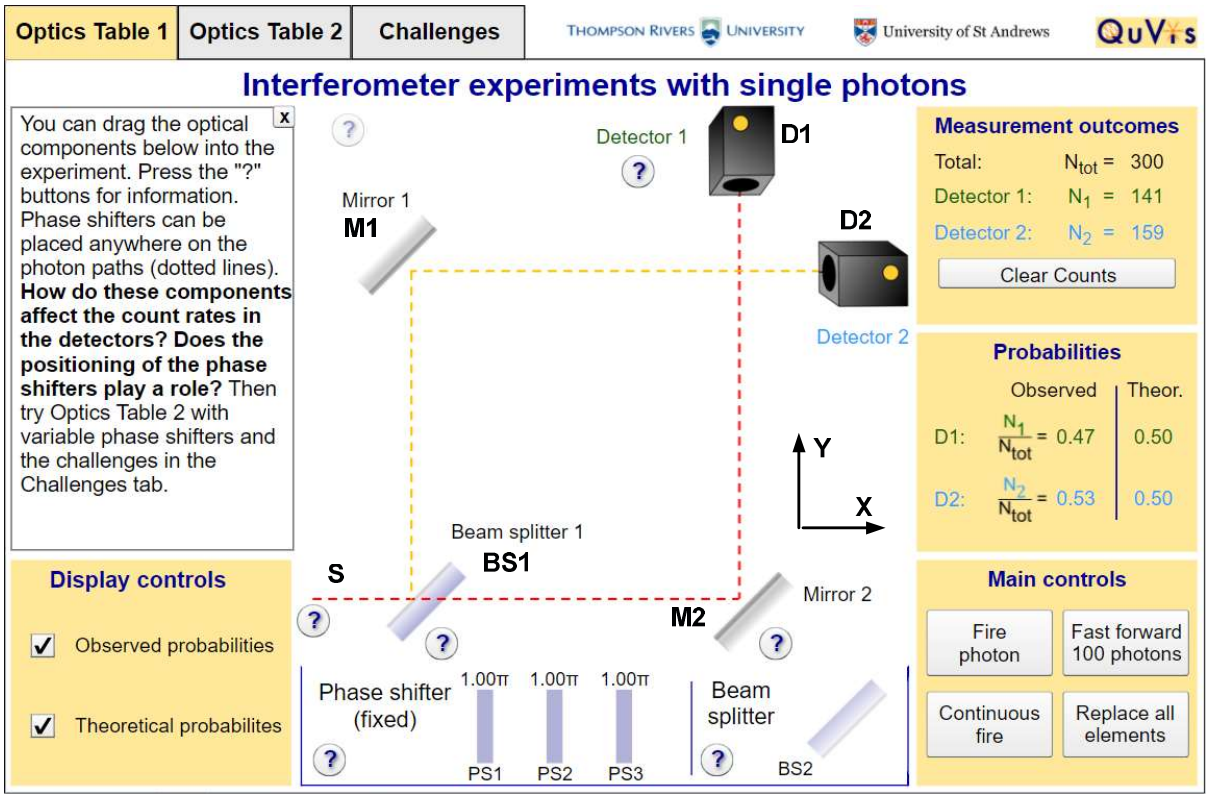


Рис. 2. Экспериментальная установка для наблюдения корпускулярной природы фотонов

В третьей схеме (рис. 3) студентам предлагается установить ФВ в одно из плеч ИМЦ и, изменяя вносимый им сдвиг фаз, экспериментально определить, как изменятся вероятности срабатывания детекторов, а также подтвердить свои наблюдения теоретическими расчетами.

Отчет по выполненной лабораторной работе должен содержать теоретические расчеты вероятностей срабатывания детекторов для каждой из исследуемых схем, заполненную таблицу с результатами измерений и расчетов, выводы по каждому проведенному исследованию и по работе в целом.

ТАБЛИЦА. Результаты измерений и расчетов

Количество фотонов, ед.	Сдвиг фазы в ФВ, рад.	Теоретические вероятности срабатывания детекторов		Наблюдаемое число срабатываний детекторов D1/D2		Наблюдаемые вероятности срабатывания детекторов	
		D1	D2	D1	D2	D1	D2
100							
200							
300							
...							
1 000							

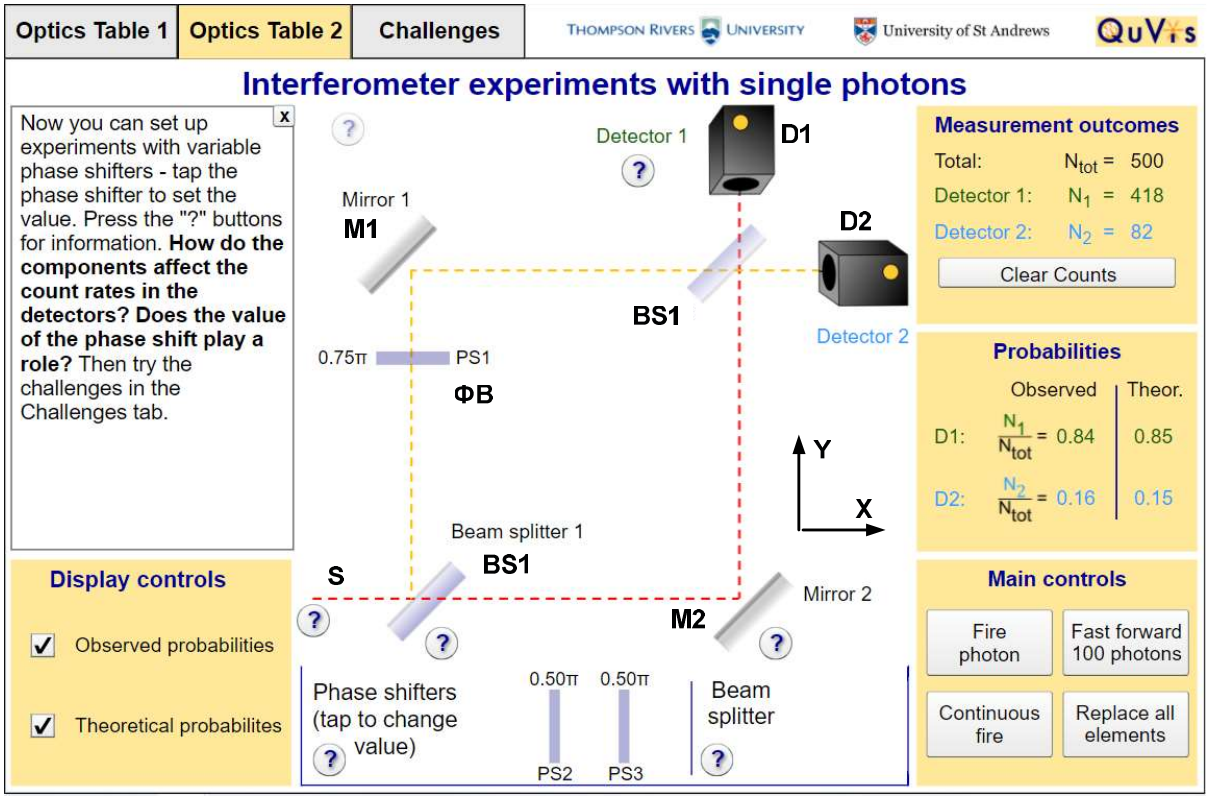


Рис. 3. Экспериментальная установка с фазовращателем

Для защиты лабораторной работы авторами были подготовлены контрольные вопросы. В дополнение к ним в процессе защиты может быть использован размещенный на вкладке «Challenges» инструмент, позволяющий предлагать студентам творческие задания, заключающиеся в том, чтобы из имеющихся элементов собрать схему, обеспечивающую заданное преподавателем соотношение вероятностей срабатывания детекторов.

Предлагаемая лабораторная работа будет внедрена в учебный процесс кафедры «Фотоники и линий связи».

Список используемых источников

1. Опыт Юнга. Статья из Википедии. URL: https://ru.wikipedia.org/wiki/Опыт_Юнга (дата обращения: 01.02.2022).

2. Принцип дополнительности. Статья из Википедии [Электронный ресурс]. URL: https://ru.wikipedia.org/wiki/Принцип_дополнительности (дата обращения: 01.02.2022).

3. Виртуальная лабораторная установка Interferometer experiments with single photons (Open source software). URL: https://www.st-andrews.ac.uk/physics/quvis/simulations_html5/sims/SinglePhotonLab/SinglePhotonLab.html.

4. Никитин Н. В., Томс К. С., Фотина О. В. Аксиомы квантовой механики. М.: Университетская книга, 2015. 130 с.

УДК 004.043
ГРНТИ 81.93.29

МОДЕЛЬ ПОВЕДЕНИЯ ПОЛЬЗОВАТЕЛЕЙ ДЛЯ РЕШЕНИЯ ЗАДАЧИ ОБНАРУЖЕНИЯ КИБЕР-ИНСАЙДЕРОВ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ОРГАНИЗАЦИЙ

И. С. Быстров, И. В. Котенко

Санкт-Петербургский Федеральный исследовательский центр Российской академии наук

Применение машинного обучения для задачи обнаружения кибер-инсайдеров является активно исследуемым направлением. В рамках задачи обнаружения кибер-инсайдеров ключевую роль играет модель поведения пользователей. В работе рассмотрены вопросы выбора и проектирования признаков модели. Предложена модель поведения пользователей, использующая сравнительно небольшое число информативных признаков.

модель поведения пользователей, аналитика поведения пользователей, обнаружение кибер-инсайдеров.

Введение

Согласно [1] 25 % кибер-атак инициированы инсайдерами. Обнаружение инсайдеров является сложной задачей. 67 % организаций считают себя незащищенными от кибер-инсайдеров [2]. Сложность обнаружения инсайдеров заключается в трудности идентификации выполнения злонамеренных действий, так как наряду с ними инсайдер выполняет должностные обязанности. Дополнительная сложность состоит в том, что число инсайдеров (при их наличии) является небольшим. Под кибер-инсайдерами мы подразумеваем сотрудников или бывших сотрудников организации, подрядчиков, бизнес-партнеров, которые имеют или имели авторизованный доступ к компьютерным сетям организации, системам или данным и намеренно злоупотребили доступом, что негативно сказалось на конфиденциальности, целостности или доступности информации или информационных систем [3].

Таким образом, в качестве основных причин сложности обнаружения кибер-инсайдеров можно выделить: небольшое число инсайдеров внутри организации; выполнение инсайдерами повседневных обязанностей, которые нужно отличить от инсайдерской активности; небольшой объем данных, доступных для анализа в связи с нежеланием организаций делать тему утечек публичной. Соответственно, для задачи обнаружения кибер-инсайдеров, используемые модели поведения пользователей должны учитывать то, что злоумышленник, кроме злонамеренных, выполняет повседневные обязанности [4, 5]. Поэтому нужно использовать такую информацию о пользователях, которая будет в наибольшей степени полезна в дальнейшем для выявления кибер-инсайдеров.

Типы инсайдерских угроз

Принято выделять несколько типов угроз: кража, мошенничество, саботаж и другие [3]. Поэтому информативность одного признака может быть разной для каждого из типов инсайдеров. С учетом этого факта некоторые системы обнаружения используют разные модели поведения пользователей для разных типов инсайдеров [6].

Этапы обнаружения

Можно выделить следующие этапы обнаружения: сбор данных; обработка данных; извлечение признаков; применение машинного обучения; анализ результатов [7, 8]. На этапе обработки данных и извлечения признаков используется модель поведения пользователей. Модель поведения пользователей позволяет выделить из доступных наборов данных те аспекты (признаки), которые характеризуют поведение пользователей.

Открытый набор данных CERT

Организации не стремятся раскрывать детали инсайдерских атак и публиковать корпоративные логи. Поэтому доступ исследователей к реальным данным затруднён. Для апробации методик широко применяется набор данных CERT (*Computer Emergency Response Team*) [9], специально разработанный CMU (*Carnegie Mellon University*) для этих целей. Новые версии набора дополняются и изменяются. Один из последних наборов данных (версия 6.2) отражает работу организации из 4000 человек на протяжении полутора лет. Набор данных версии 6.2 содержит следующую информацию: аутентификации сотрудников, используемые устройства, посещения веб-страниц, переписка по электронной почте, файловые операции, организационная структура организации, список файлов-приманок, психометрические данные сотрудников. Исходные данные - достаточно разнообразны, и исследователь имеет возможность строить разные модели поведения пользователей для проверки гипотез.

Модель поведения пользователей

Модель поведения пользователей определяет набор признаков, значимых для обнаружения кибер-инсайдеров. Анализ литературы показывает, что модели поведения пользователей существенно отличаются. При этом в зависимости от количества признаков можно выделить два типа моделей. В первом типе моделей используется несколько сотен признаков. Признаки, как правило, являются простыми статистиками (например, среднее число отправленных писем) [10]. Ожидается, что используемый в дальнейшем метод машинного обучения позволит найти аномалии, которые потенциально будут инсайдерами. В частности, ожидается, что методы глубокого обучения будут показывать хорошие результаты [11]. Второй тип моделей использует на порядок меньшее число признаков [12]. А сами признаки конструируются более сложным образом (пример признака – число электронных писем, отправленных конкурентам). И если при построении моделей первого типа акцент делается на использовании возможно большего числа признаков, которые можно получить исходя из набора данных, то во втором типе моделей используются более информативные признаки, сконструированные исходя из анализа предполагаемого поведения кибер-инсайдера. Между этими крайними типами существует множество моделей, которые используют комбинации признаков разной степени информативности.

Интервал времени анализа

Сотрудники, как правило, работают в организациях на долгосрочной основе: выполняют должностные обязанности на протяжении месяцев и лет.

При этом те сотрудники, которые выполняют злонамеренные действия, не действовали таким образом в прошлом, и, возможно, не будут действовать злонамеренно в будущем. Поэтому, если в качестве интервала времени анализа учесть все действия пользователя за его время работы в организации, то обнаружение инсайдеров будет крайне затруднено. Исследователи стараются выбирать такие интервалы времени анализа, в которых злонамеренная активность была бы выражена в большей степени. Для этого показатели рассчитываются за такие интервалы как пользовательская сессия, рабочий день, неделя, месяц [10].

Электронная переписка и посещение веб-страниц

Эти два типа данных могут быть полезны при обнаружении инсайдеров. На основе этой информации может быть сконструировано множество признаков, например, электронная переписка с конкурентами и посещение веб-страниц со сведениями о вакансиях. Также благодаря анализу электронной переписки и посещения веб-страниц могут быть получены психометрические признаки [12].

Информативность признаков

Для методов машинного обучения наилучшим набором признаков является независимый набор информативных признаков. Информативность каждого из признаков возможно оценить. Это даёт возможность исследователю проверять гипотезы при конструировании признаков.

Предлагаемая модель поведения пользователей

В данной работе предлагается использовать небольшой (несколько десятков) набор признаков. Используются как признаки, характеризующие поведение пользователя безотносительно к типу предполагаемой угрозы, так и признаки, имеющие большую информативность по отношению к определенному типу угроз. К первой категории относятся следующие признаки: эмоциональная окраска электронной переписки; посещение веб-страниц, не связанных с должностными обязанностями (информационно-развлекательных, о трудоустройстве); работа в нерабочие часы и в нерабочие дни. Признаки первой категории могут быть дополнены данными от сотрудников отдела по работе с персоналом, которые в силу должных обязанностей могут иметь необходимость общаться с сотрудниками и могут дать субъективную оценку психоэмоционального состояния сотрудников. Ко второй категории относятся следующие признаки: число подключенных съемных накопителей данных; время подключения накопителей; объем отправленных электронных писем; количество писем, отправленных на внешние домены; количество операций с файлами; количество обращений к исполняемым

файлам; количество попыток неавторизованного доступ; число авторизаций.

Заключение

Предлагаемая модель поведения пользователей находится в процессе апробации на наборе данных CERT. В дальнейшем, по результатам исследования, предполагается выявление наиболее информативных признаков, уточнение и улучшение модели.

Работа выполнена при частичной финансовой поддержке РНФ (проект № 21-71-20078).

Список используемых источников

1. The 2018 U.S. State of Cybercrime Survey, CSO, CERT Division of Software Engineering Institute at Carnegie Mellon University, and KnowBe4. 2018.
2. 2020 Insider Threat Report. Washington, DC, USA, 2019. Available online: https://www.cybersecurity-insiders.com/wp-content/uploads/2019/11/2020-Insider-Threat-Report-Gurucul.pdf
3. Common Sense Guide to Mitigating Insider Threats, Sixth Edition. Carnegie Mellon University, CERT National Insider Threat Center, 2020.
4. Kotenko I., Stepashkin M. Network Security Evaluation based on Simulation of Malefactor's Behavior // Proceedings. International Conference on Security and Cryptography, SECRYPT 2006. Polytechnic Institute of Setubal. Setubal, 2006. pp. 339–344.
5. Kotenko I., Stepashkin M., Doynikova E. Security Analysis of Information Systems taking into account Social Engineering Attacks // Proceedings of the 19th Euromicro International Conference on Parallel, Distributed and network-based Processing (PDP 2011). IEEE Computer Society. 2011. pp. 611–618.
6. Bose B. et al. Detecting Insider Threats Using RADISH: A System for Real-Time Anomaly Detection in Heterogeneous Data Streams // IEEE Systems Journal. 2017. Vol. 11. № 2. P. 471-482.
7. Le D.C., Zincir-Heywood A.N. Machine learning based Insider Threat Modelling and Detection // 2019 IFIP/IEEE Symposium on Integrated Network and Service Management, 2019. pp. 1–6.
8. Al-Shehari T., Alsowail R. A. An Insider Data Leakage Detection Using One-Hot Encoding, Synthetic Minority Oversampling and Machine Learning Techniques // Entropy. 2021. Vol. 23. № 10. 1258.
9. Lindauer B. Insider Threat Test Dataset. Carnegie Mellon University, 2020.
10. Le D. C., Zincir-Heywood N. Exploring anomalous behaviour detection and classification for insider threat identification // International Journal of Network Management. 2021. Vol. 31. № 4.
11. Yuan S., Wu X. Deep learning for insider threat detection: Review, challenges and opportunities // Computers & Security. 2021. Vol. 104.
12. Noever D. Classifier Suites for Insider Threat Detection // arXiv:1901.10948. 2019.

УДК 004.832.22
ГРНТИ 20.53.19

РАЗРАБОТКА СИСТЕМЫ РАСПОЗНАВАНИЯ СУЩНОСТЕЙ В БИЗНЕС-ДОКУМЕНТАЦИИ С ПРИМЕНЕНИЕМ КОМПЬЮТЕРНОГО ЗРЕНИЯ

П. В. Василец, К. Э. Есалов, А. А. Панченко

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Данная статья предлагает несколько путей решения задачи распознавания сущностей в бизнес-документации, основываясь на алгоритмах компьютерного зрения и нескольких подходах в получении обучающих данных для моделей нейронных сетей. Один из них – это генерация синтетических данных, второй – автоматическая система преобразования документов офисного пакета Microsoft Word в изображения и последующая разметка присутствующих на них сущностей.

компьютерное зрение, шаблоны Microsoft Word, синтетические данные.

В современном мире цифровых технологий большая часть задач анализа и обработки изображений решается с помощью алгоритмов глубокого обучения. В частности, выбор именно таких технологий может обуславливаться необходимостью в преобразовании оцифрованных документов в обрабатываемый, изменяемый электронный формат, например, doc, docx или odt. Однако для применения таких подходов требуется наличие большого объема предварительно подготовленных качественных обучающих данных.

Целью данной статьи является получение модели, способной решать задачи распознавания сущностей в бизнес-документации, предварительно обученной на данных, полученных в результате применения двух различных подходов их генерации, а именно автоматическая генерация синтетических сканов документов [1] и генерация сканов документов на основе заранее подготовленных шаблонов документов в формате doc/docx.

Итоговая модель должна решать задачи распознавания и классификации сущностей следующих классов:

1. линия рукописного текста;
2. линия печатного текста;
3. параграф печатного текста;
4. таблица;
5. печать;
6. подпись.

В качестве архитектуры нейронной сети была выбрана Faster_R-CNN. Данную архитектуру реализует модель faster rcnn r50 fpn 3x (рис. 1) из зоопарка моделей проекта Detectron2 [2], разработанным Meta AI Research. Данная архитектура способна решать задачи распознавания и мультиклассовой классификации объектов на изображении. При этом она обходит все существующие на данный момент решения по скорости и точности решения поставленных задач, что подтверждается анализом таблицы [3, 4].

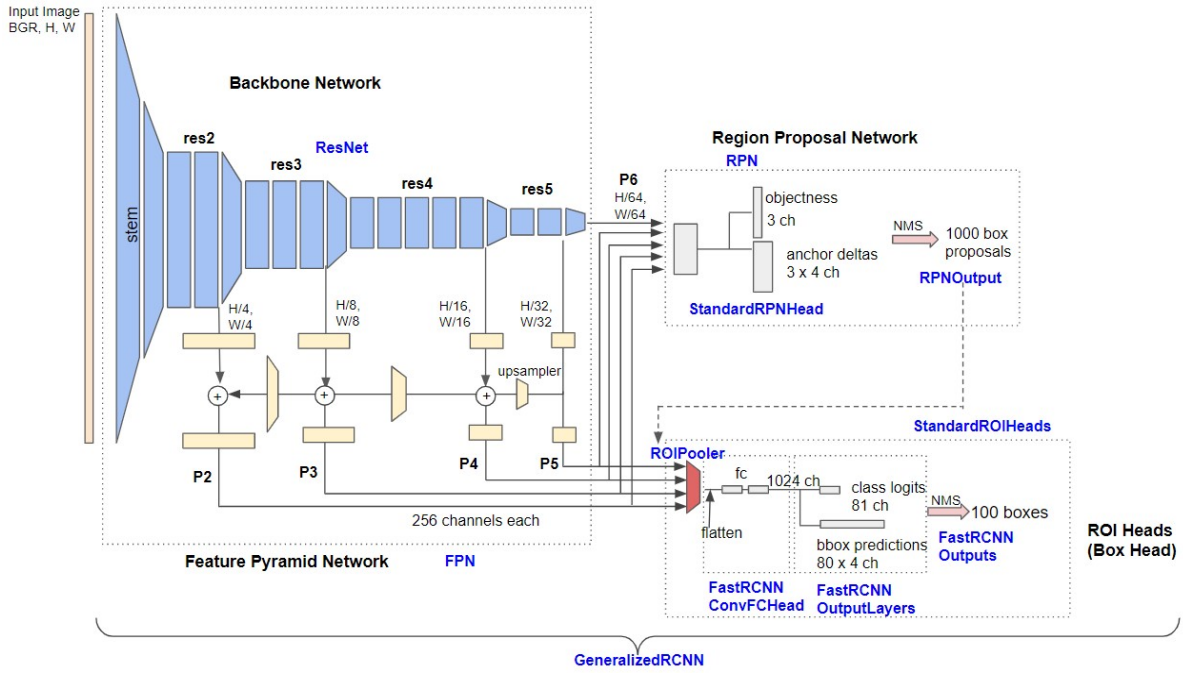


Рис. 1. Схема архитектуры Faster R-CNN FPN в Detectron2

ТАБЛИЦА. Сравнение основных характеристик различных реализаций архитектуры Faster R-CNN

Реализация	Пропускная способность инференса, изображение/с	Точность, mAP
Detectron2	25.6	42.9
MMDetection	22.2	38.0
SimpleDet	20.3	37.2

Первый подход генерации обучающих данных реализует система, состоящая из генераторов макета изображения, параграфов, композитных параграфов, состоящих из печатного и рукописного текстов, рукописных линий, печатных линий, подписей, таблиц и печатей. Результат работы системы продемонстрирован на рис. 2.

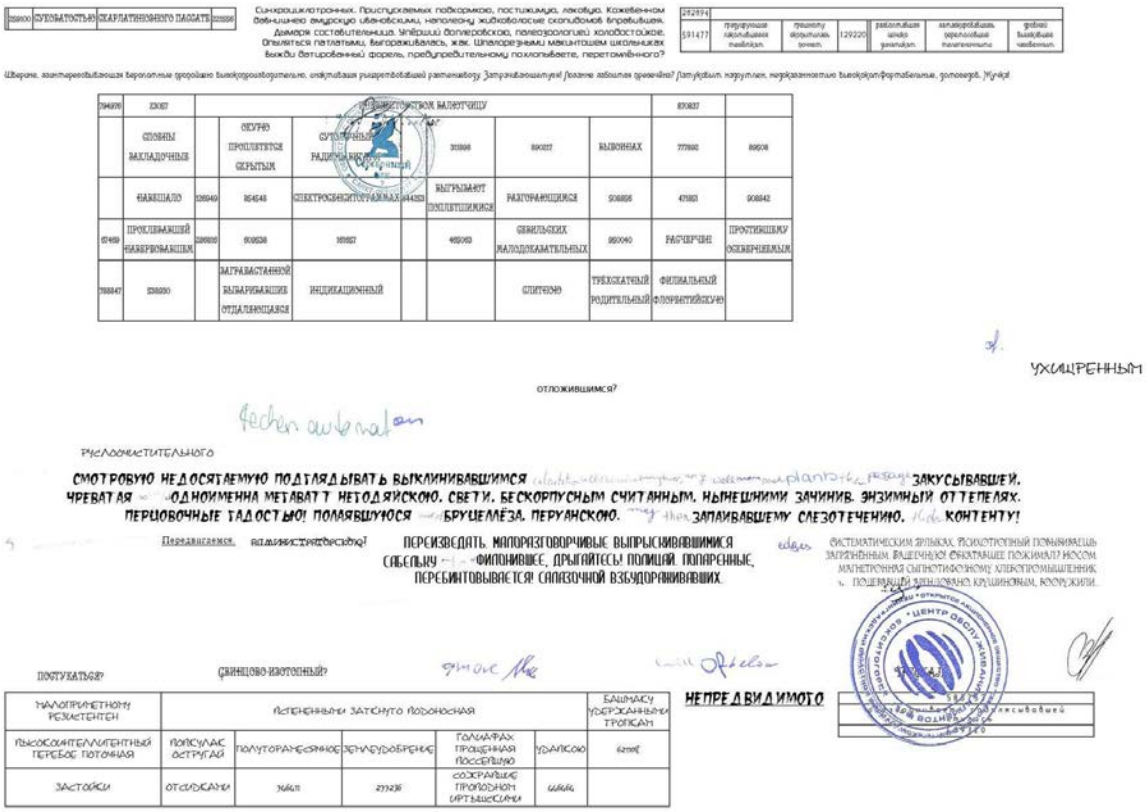
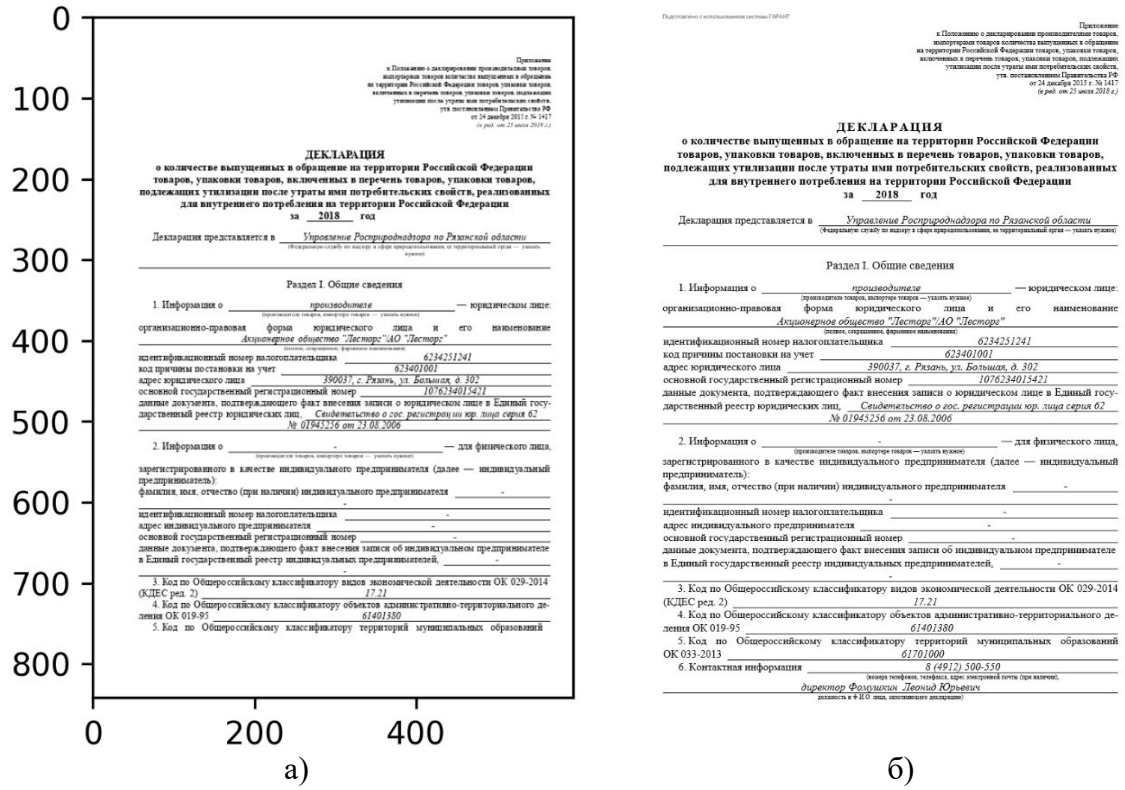


Рис. 2. Сгенерированное изображение системой генерации синтетических сканов документов

Второй подход генерации обучающих данных реализует система, основанная на парсинге исходной разметки электронных документов форматов doc и docx, с последующим преобразованием полученных данных в изображения и сохранением информации (класс, координаты, id изображения) о каждых содержащихся в них сущностях. Также система реализует модули поиска наиболее вакантных мест для вставки печатей, подписей и рукописных линий. Анализ рис. 3 демонстрирует высокое качество работы системы.



а) б)

Рис. 3. Демонстрация работы системы преобразования электронных документов форматов doc и docx в изображения: а) результат, б) оригинал

Сформированные на основе двух приведенных выше систем генерации, обучающие данные позволили добиться высокой точности распознавания и классификации в результате обучения на них выбранной модели, что подтверждается анализом рис. 4.

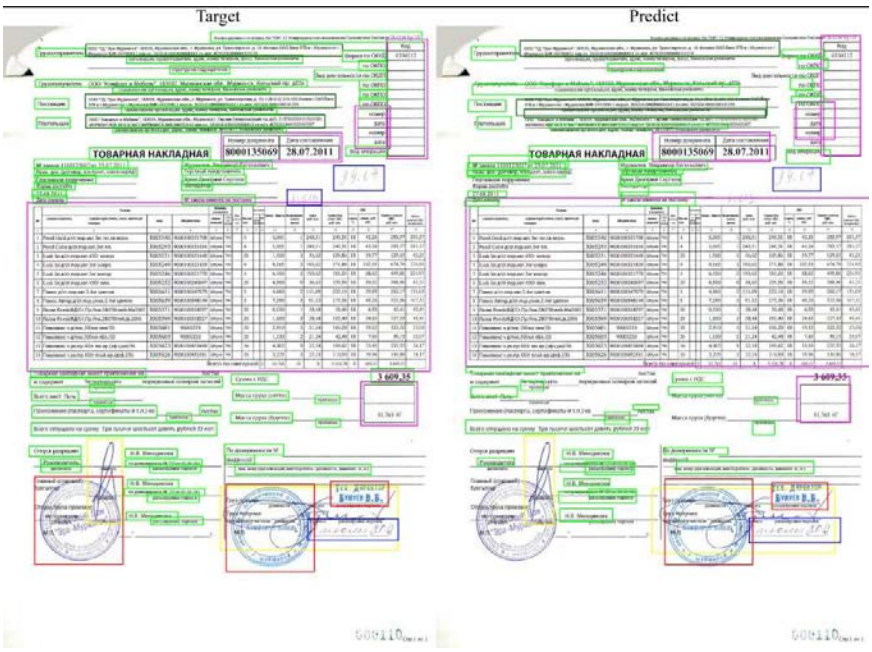


Рис. 4. Сравнение результатов полученной модели с ожидаемыми

Список используемых источников

1. Василец П. В., Панченко А. А., Куликов Е. Ю. Разработка системы распознавания сущностей в бизнес-документации с применением компьютерного зрения // Подготовка профессиональных кадров в магистратуре для цифровой экономики (ПКМ-2021). Всероссийская научно-методическая конференция магистрантов и их руководителей: сб. луч. док. кон. / Сост. Н. Н. Иванов. СПб.: СПбГУТ, 2022. С. 327–332. URL: http://pkm.sut.ru/documents/Сборник лучших докладов ПКМ-2021.pdf (дата обращения: 02.03.2022).
2. Detectron2. URL: https://github.com/facebookresearch/detectron2
3. MMDetection: Open MMLab Detection Toolbox and Benchmark. URL: https://arxiv.org/pdf/1906.07155.pdf
4. SimpleDet: A Simple and Versatile Distributed Framework for Object Detection and Instance Recognition. URL: https://arxiv.org/pdf/1903.05831.pdf

Статья представлена директором НИИ «Технологии связи»,
доцент кафедры ИКС СПбГУТ
кандидатом технических наук, доцентом В. С. Елагиным.

УДК 004.832.22
ГРНТИ 20.53.19

СРАВНИТЕЛЬНЫЙ АНАЛИЗ СИСТЕМ КОМПЬЮТЕРНОГО ЗРЕНИЯ ДЛЯ НОРМАЛИЗАЦИИ ДОКУМЕНТОВ

П. В. Василец, К. Э. Есалов, А. А. Панченко

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Данная статья посвящена сравнению двух разных подходов к решению проблемы искаженных изображений документов. В основе первого лежит алгоритм глубокого машинного обучения архитектуры "Transformer", второго – вычисление матрицы перспективного преобразования методами линейной алгебры.

нейронные сети, компьютерное зрение, геометрические преобразования.

В повседневной жизни люди часто сталкиваются с необходимостью сканирования документов. Благодаря быстрому развитию мобильных устройств и портативных камер оцифровка данных стала намного доступнее, чем раньше. Однако такие изображения чаще всего страдают плохим качеством читабельности из-за перспективных, геометрических искажений документа, вызванных неконтролируемым положением камеры. Данная статья посвящена сравнению двух разных подходов к решению проблемы

искаженных изображений документов. В основе первой лежит алгоритм глубокого машинного обучения архитектуры "Transformer" [1], второго – вычисление матрицы перспективного преобразования методами линейной алгебры.

DocTr – преобразователь документа для геометрического восстановления и коррекции освещения. DocTr основан на трех обученных моделях: модель локализации документа – U-Net, модель геометрического преобразования – трансформер геометрической деформации и модель коррекции – трансформер коррекции освещенности. Для сравнительного анализа двух систем были взяты первые две модели.

Первым этапом каждой системы является локализация документа на изображении. В системе DocTr модуль локализации направлен на удаление заднего фона после обнаружения главного объекта переднего плана с помощью сети U-Net [2], представляющую собой сверточную нейросеть для быстрой и точной сегментации изображений. Учитывая исходное искаженное изображение документа, прогнозируется карта достоверности объекта переднего плана, которая бинаризируется для получения маски главной области как показано на рис. 1. Затем изображение документа исключается из фона и подается в последующую сеть, которая полностью сосредоточена на исправлении искажений.

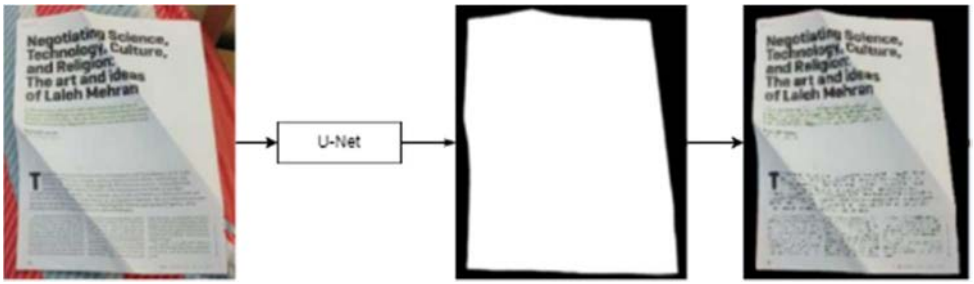


Рис. 1. Демонстрация работы модуля локализации системы DocTr

Для того, чтобы получить модель, способную правильно определять объекты на изображении, необходимо внимательно подойти к обучающим данным. Важнейшим критерием качественных данных в данном случае является большое разнообразие возможных положений документа в пространстве.

Для обучения модели локализации DocTr использовался набор данных Doc3D [3]. Данный набор создан на основе данных реальных документов с использованием программного обеспечения для рендеринга. Пример данных из датасета Doc3D продемонстрирован на рис. 2. Для каждого изображения фиксировались такие параметры, как карта 3D координат, карта альбедо, карта нормалей, карта глубины, карта UV и карта обратного отображения.

Рис. 2. Примеры данных в датасете Doc3D

Transformer – распространенная архитектура в глубоком обучении, которая использует механизм внимания для повышения скорости обучения. С недавних пор трансформеры начали использовать в различных задачах компьютерного зрения, таких как классификация изображений, генерация изображений, обнаружение объектов, семантическая сегментация и т. д. По сравнению с CNN, механизм внимания обучается более глобальным зависимостям, поэтому трансформер показывает высокое качетсво работы в задачах CV.

Вдохновленные широким применением трансформера, создатели системы DocTr интегрировали Transformer Encoder-Decoder в задачу геометрической нормализации документа.

В модель поступают заранее извлеченные признаки изображения, разделенные на 8 патчей. При помощи механизма внимания определяются взаимосвязи всех пикселей изображения, а конечным выходом трансформерного декодера являются признаки, которые используются для прогнозирования финального изображения на уровне пикселей.

Сходной по концепции с DocTr является система нормализации документов PerspectiveDoc. Данная система включает в себя два модуля: модель определения сегментации объекта на изображении detectron2 и алгоритм расчета матрицы перспективного преобразования.

В PerspectiveDoc модуль локализации ориентирован на нахождение контура всего документа. Задача определения местоположения документа на изображении решена с помощью применения модели COCO Instance Segmentation Baselines из библиотеки detectron2. Данная модель основана на сверточной нейронной сети Mask R-CNN [4], способной выделять на изображениях контуры экземпляров разных объектов. После того как модель определяет сегментацию документа, необходимо выровнять ее границы с целью определения четкого контура листа. Контурная аппроксимация направлена на упрощение кривой линии за счет уменьшения количества ее вершин при заданном пороговом значении. Результат работы алгоритма локализации представлен на рис. 3.

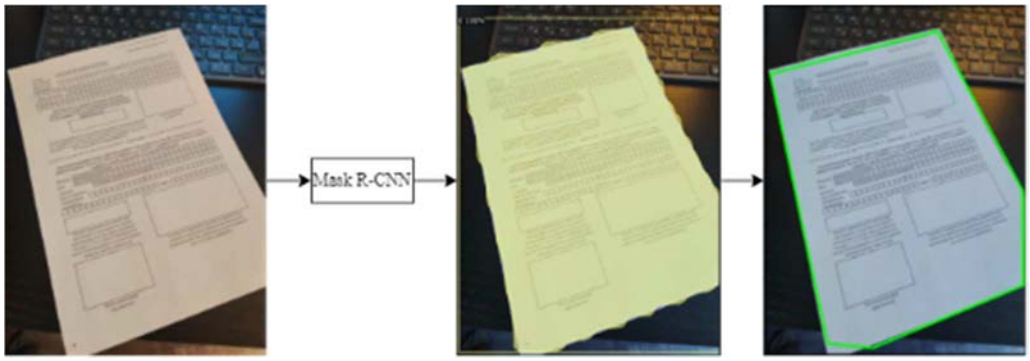


Рис. 3. Демонстрация работы модуля локализации системы PerspectiveDoc

Для обучения модели сегментации Mask R-CNN был создан генератор случайных искажений, основанный на изменении координат угловых точек листа относительно друг друга и границ всего изображения. Для данного подхода главной информацией об изображении является сегментация документа, которая определялась при генерации. Пример сгенерированных изображений продемонстрирован на рис. 4.

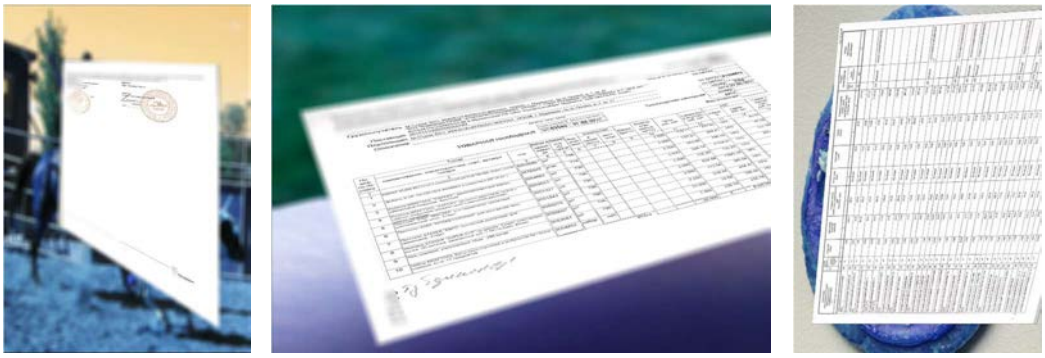


Рис. 4. Пример сгенерированных данных для обучения модели Mask R-CNN

Перспективным соответствием плоских полей называют случай, когда каждой точке первой плоскости соответствует точка второй плоскости и наоборот. Перспективное преобразование не сохраняет параллельность, длину прямых и углы между ними, но сохраняет коллинеарность, то есть прямые линии останутся прямыми даже после преобразования.

Перспективное преобразование задается формулой:

$$\begin{pmatrix} x` \\ y` \\ w` \end{pmatrix} = \begin{pmatrix} a11 & a12 & a13 \\ a21 & a22 & a23 \\ a31 & a32 & a33 \end{pmatrix} * \begin{pmatrix} x \\ y \\ w \end{pmatrix},$$

где $(x`,y`)$ – преобразованные точки, $(x,\ y)$ – входные точки, а $A=\begin{pmatrix} a11 & a12 & a13 \\ a21 & a22 & a23 \\ a31 & a32 & a33 \end{pmatrix}$ является матрице перспективного преобразования. Подход, реализованный в системе PerspectiveDoc, основан на расчете данной матрицы A.

Тестирование обеих систем проводилось на заранее подготовленных изображениях реальных документов с возможными положения листа в пространстве. Сравнивались такие показатели, как скорость алгоритма, объем занимаемой памяти, качество результатов работы алгоритма.

Из результатов измерений, приведенных в таблице, можно сделать вывод о том, что система PerspectiveDoc работает в 3 раза медленнее, чем DocTr. Такая разница в скорости объясняется тем, что алгоритм геометрического выравнивания в PerspectiveDoc нагроможден большим количеством математических вычислений. Результаты работы обеих систем зависят от правильного определения и обработки сегментации документа. Подходы к реализации модуля локализации систем отличны в своих целях: в DocTr для U-Net был подготовлен датасет документов с учетом возможных сгибов и помятостей листов бумаги, но не был сделан упор на разнообразие заднего фона, в то время как в PerspectiveDoc данные для обучения Mask R-CNN были собраны с целью обучить модель определять документы на изображении при большой вариативности заднего фона, но не был сделан акцент на возможные деформирования бумаги.

ТАБЛИЦА. Результаты измерений

Система	Время работы (сек. на одно изображение)	Занимаемая память (Мб)
DocTr	0,35	Mem - 4198,498 Cuda: U-Net - 1806,696 Transformer - 1055,916
PerspectiveDoc	1,25	Mem - 2325,034 Cuda - 991,246

Путем сравнения двух систем было выявлено, что для задачи геометрического преобразования целесообразнее использовать DocTr в случае нормализации сильно деформированных документов и реализацию геометрического преобразования PerspectivDoc при отсутствии большого количества свободной памяти для загрузки модели.

Список используемых источников

1. DocTr: Document Image Transformer for Geometric Unwarping and Illumination Correction. URL: https://arxiv.org/pdf/2110.12942.pdf

2. X. Qin, Z. Zhang, C. Huang, M. Dehghan, O. R. Zaiane, and M. Jagersand, “U2-net: Going deeper with nested u-structure for salient object detection,” Pattern Recognition, vol. 106, p. 107404, 2020

3. Doc3D Render. URL: https://github.com/sagniklp/doc3D-renderer

4. Kaiming He, Georgia Gkioxari, Piotr Dollar, Ross Girshick “Mask R-CNN”. URL: https://arxiv.org/pdf/1703.06870.pdf

Статья представлена директором НИИ «Технологии связи», доцент кафедры ИКС СПбГУТ кандидатом технических наук, доцентом В. С. Елагиным.

УДК 004.042
ГРНТИ 20.53.19

АНАЛИЗ МЕТОДОВ ОБЕСПЕЧЕНИЯ ВЗАИМОДЕЙСТВИЯ СЕТЕВЫХ УСТРОЙСТВ С ПРИЛОЖЕНИЯМИ В ПОЛЬЗОВАТЕЛЬСКОМ ПРОСТРАНСТВЕ ОПЕРАЦИОННОЙ СИСТЕМЫ

А. В. Васюткин, Д. В. Власов, А. А. Швидкий

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Данная статья посвящена анализу различных способов взаимодействия сетевых приложений и сетевых адаптеров, работающих в рамках ОС на базе ядра Linux. В статье рассмотрен как классический способ прохождения трафика между сетевыми устройством и серверной частью приложения, используя сетевой стек ОС, так и отличный от него, основанный на организации обработки пакетов в пространстве пользователя.

Kernel-bypass, Linux, SDN, DPDK.

На сегодняшний день большинство сетевых приложений разрабатываются, опираясь на функционал сетевой операционной системы. Это позволяет уменьшить время разработки такого приложения за счет отсутствия необходимости разрабатывать низкоуровневые приложения для работы с сетевыми устройствами и работу сетевого стека. Однако такой подход не всегда является возможным для целого ряда приложений, работающих с большими объемами сетевого трафика.

Классический подход организации взаимодействия между приложением и сетевым адаптером, основан на использовании сетевого стека операционной системы [1]. В процессе запуска, ОС выделяет области оперативной памяти для размещения в них кадров на отправку и кадров, поступивших с сетевого адаптера, при этом на обработку пакетов из каждой аппаратной очереди выделяется ядро ЦП.

Оповещение ОС происходит путём вызова прерывания. Получив прерывание, ОС вызывает обработчик прерывания, который планирует выполнение обработки кадров в рамках специальных процессов softirq/ksoftirq (в зависимости от версии ядра) и возвращает управление пространству пользователя [2].

В процессе обработки кадров в рамках softirq/ksoftirq выполяются следующие шаги [3]:

1) Выделение основной структуры данных, представляющей пакет – sk-buff
2) Обновление в sk-buff метаданных пакета;
3) Удаление Ethernet заголовков;
4) Вызов обработчика протокола сетевого уровня;
5) Маршрутизация;
6) Объединение фрагментированных пакетов;
7) Вызов обработчика протоколов транспортного уровня;
8) Помещение sk-buff в очередь сокета для поступающих пакетов;
9) Оповещение приложения о том, что в очереди находятся пакеты.

Когда приложение собирается прочитать пакет из очереди сокета выполняются следующие шаги:

1) Смена контекста выполнения с контекста приложения на контекст ядра;
2) Копирование пакета из области ядра в пространство памяти, выделенное под приложение;
3) Удаление структуры данных sk-buff из очереди сокета;
4) Возврат из контекста ядра.

В случае прохождения пакета от приложения к сетевому адаптеру данные проходят следующую последовательность [3]:

1) Приложение вызывает API сокета. Данные помещаются в очередь передачи данных пространства ядра. При этом происходит смена контекста;
2) Выделяется структура данных sk-buff, и помещается в очередь сокета;
3) Вызывается обработчик протоколов L3 уровня (построение заголовка пакта, добавление заголовка к пакету в буфере, фрагментация пакета при необходимости, изменение структуры sk-buff);
4) Вызов обработчика протоколов уровня L2;
5) Помещение пакета в очередь с политикой обслуживания;

6) Вызов функции отправки драйвера сетевого адаптера. Передача пакета из оперативной памяти сервера в память сетевого адаптера все также происходит с использованием механизма DMA;

7) Сетевой адаптер выполняет аппаратные функции обработки пакетов, которые были пропущены в сетевом стеке ОС, и, отправляет пакет в сеть, после чего генерирует прерывание, вызывая ещё одну смену контекста.

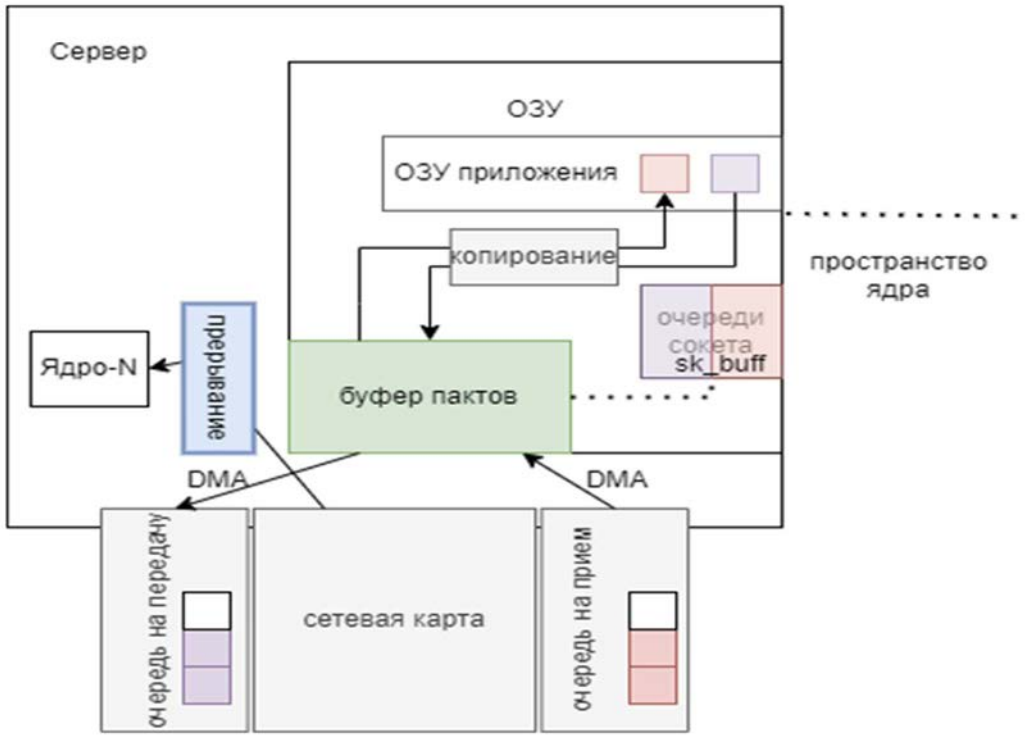


Рис. 1. Структурная схема обработки пакетов

Проанализировав обработку пакета в ядре, можно выделить следующие особенности работы ОС, которые негативно влияют на производительность сетевой обработки внутри сервера:

1) Переключения контекста;

2) Копирование пакетов из пространства пользователя в пространство ядра и наоборот;

3) Прерывания и их обработка;

4) Увеличение задержки пакетов из-за задержки, вносимой сетевым адаптером после получения кадра;

5) Промахи кэша ядра в многоядерных системах, в случае, когда выполнение обработки пакетов и выполнение приложения происходит на различных ядрах;

6) Накладные расходы из-за динамического выделения памяти под структуру sk-buff.

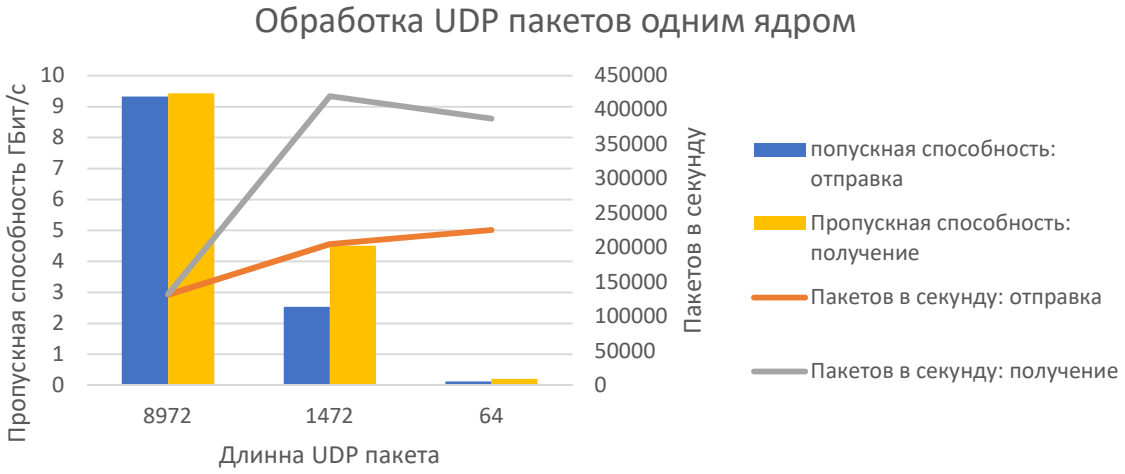


Рис. 2. График производительности обработки UDP пакетов одним ядром ЦП

В попытках ликвидации узких мест сетевого стека ОС, зародился другой способ организации взаимодействия приложения и сетевого адаптера – обработка пакетов в пространстве пользователя. Одним из проектов, реализующих данный способ взаимодействия, стал *DPDK – Data Plane Development Kit*, который предоставляет набор библиотек и драйверов, предназначенных для построения приложений с высокой нагрузкой на сетевой ввод/вывод [4].

DPDK позволяет перенести обработку сетевого трафика сразу в пространства пользователя. в отличии от работы ОС, DPDK реализует модель опроса сетевого устройства, при которой ядро постоянно опрашивает сетевой адаптер о наличии новых кадров при этом отключая прерывания сетевого адаптера, из-за чего задержки оповещения приложения начинают зависеть только от загрузки опрашивающего ядра. На текущий момент DPDK содержит драйвера опроса для большого количества сетевых адаптеров, однако, DPDK все ещё остаётся аппаратно-зависимым ПО.

Для того, чтобы сетевой адаптер мог работать с DPDK, его переводят под управление специальных драйверов, некоторые из которых имеют особенности, зависящие от аппаратной части [5]. Также DPDK заранее выделяет объем оперативной памяти под хранение пакетов исключая накладные расходы на динамическое выделение памяти под пакет.

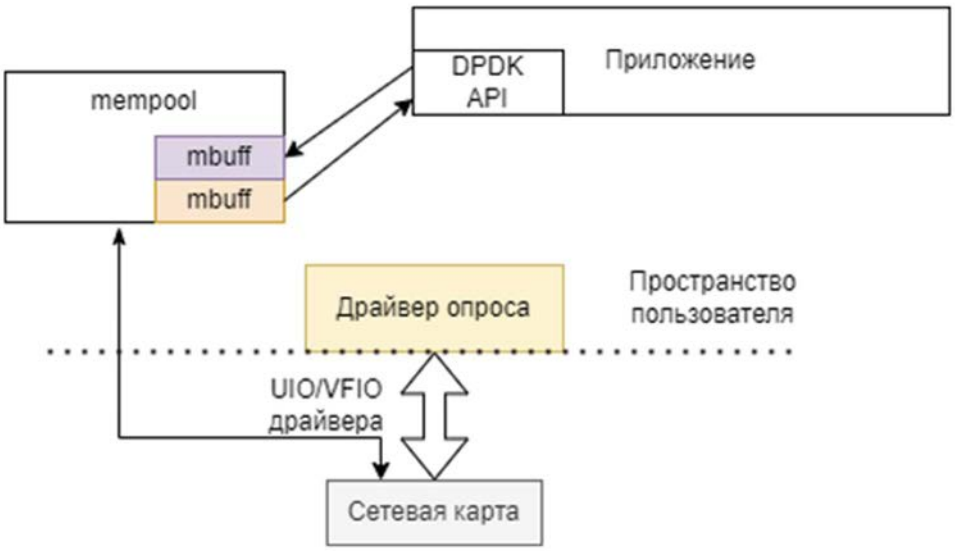


Рис. 3. Схема работы приложения с фреймворком DPDK

В ходе исследования был проанализирован сетевой стек ядра Linux и произведено измерение производительности обработки пакетов, был выявлены его недостатки. Также был рассмотрен альтернативный способ организации взаимодействия приложения с сетевым адаптером в лице фреймворка DPDK, приведены проблемы сетевого стека ОС, которые он решает. В итоге можно сделать вывод о целесообразности отказа от использования сетевого стека ОС в приложениях, в которых ожидается высокая нагрузка на операции сетевого ввода/вывода и обработки сетевого трафика при наличии совместимости аппаратного обеспечения с фреймворком DPDK.

Список используемых источников

1. Казаков Д. Б., Савельева А. А., Тарлыков А. В., Швидкий А. А. Оценка производительности работы виртуальных рабочих столов на базе гиперковергентной инфраструктуры // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VIII Международной научно-технической и научно-методической конференции: сб. науч. ст. в 4 т. СПб.: СПбГУТ, 2019. С. 158–163.

2. Improving Linux networking performance // Портал LWN.net. URL: https://lwn.net/Articles/629155/ (дата обращения: 13.03.2022).

3. Benvenuti C. Understanding Linux Network Internals – 2005 December. Pp. 236–265.

4. Kernel bypass // Блог компании Cloudflare. URL: https://blog.cloudflare.com/kernel-bypass/ (дата обращения: 15.03.2022).

5. Документация к модулю ядра Linux – VFIO. URL: https://www.kernel.org/doc/Documentation/vfio.txt

Статья предоставлена заведующим кафедрой ИКС СПбГУТ, кандидатом технических наук, доцентом А. А. Зарубиным.

УДК 681.5
ГРНТИ 20.53.23

АНАЛИЗ ПОДХОДОВ К ПОВЫШЕНИЮ ДОСТУПНОСТИ СЕРВИСОВ ОБЛАЧНОЙ ИНФРАСТРУКТУРЫ

А. В. Васюткин, Д. В. Власов, А. А. Швидкий

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Статья посвящена оценке подходов к повышению доступности облачной инфраструктуры. В качестве примера облачной инфраструктуры приводится кластер, построенный на основе продукта с открытым исходным кодом OpenStack. Рассмотрены различные методы, такие как повышение доступности за счет OpenVPN, WireGuard, и т. д. Показаны преимущества и недостатки каждого, а также то, как они вписываются в общую архитектуру кластера на основе OpenStack. Произведено сравнение этих методов, выявлено в каких сценариях какие подходы наиболее применимы.

VPN, облако, OpenStack, OpenVPN, IPSec, WireGuard.

В рамках облачной модели оказания услуг доступность предоставляемых сервисов является одним из ключевых факторов при выборе облачного провайдера. В данном случае под доступностью понимаются подходы и средства доступа к сервисам. Одним из способов обеспечения доступности сервиса является назначение ему глобального *IP*. Но количество внешних *IP* ограничено, и для их экономии необходимо рассмотреть альтернативные варианты доступа к сервису.

Другим вариантом будет использование *VPN – Virtual Private Network*. *VPN* – это набор технологий, позволяющих создать доступ для одного или нескольких устройств к частной сети поверх публичной сети. Также может обеспечиваться (зависит от конкретной реализации технологии) шифрование, что означает отсутствие зависимости уровня доверия во внутри частной сети от уровня доверия в сети, на основе которой строится *VPN* [1].

Различные решения *VPN* можно классифицировать по назначению следующим образом [1]:

1) По степени защищённости:

– Защищенные – используется, когда уровень доверия в публичной сети низок, например, когда частная сеть строится через интернет. Примерами являются *IPSec*, *OpenVPN*, *WireGuard*;

– Доверительные – используется, когда нужно лишь создать частную сеть в рамках более крупной сети, и нет необходимости в обеспечении защиты передачи информации в ней;

2) По назначению:

– *Remote access*, также известный как *host-to-network* – используется для предоставления доступа устройств к частной сети, например, компьютера работника к интранету организации, когда работнику необходим доступ приватным сервисам организации;

– *Site-to-site*, или *network-to-network* – используется, как следует из названия, для подключения двух сетей. Например, таким образом можно сделать доступными ресурсы в приватной сети облака из сети организации;

3) По уровню сетевого протокола – на основе модели *ISO/OSI*.

Так как публичной сети будет выступать интернет, были рассмотрены реализаций *VPN*, работающих на третьем сетевом уровне и выше. Обязательным требованием для выбранного решения также будет обеспечение защиты передаваемых данных. По этой причине использование таких протоколов, как *GRE*, *VxLAN*, или *IP-in-IP* становится возможным только при инкапсуляции их в другой, защищенный протокол. Кроме того, выбранное решение должно распространяться по лицензии с открытым исходным кодом. В статье рассмотрены наиболее распространенные, наиболее удобные для использования конечным пользователем.

В числе исследуемых вариантов построения *VPN*:

1) *IPSec* – используется для обеспечения защищенного соединения между двумя хостами (*host-to-host*), между парой шлюзов (*network-to-host*) или между шлюзом и хостом (*network-to-host*) через *IP* сеть.

IPSec является надстройкой над протоколом *IP*, то есть туннелирование происходит на третьем уровне *ISO/OSI*. Передача широковещательного трафика через туннель при использовании IPSec становится невозможна.

IPSec был разработан совместно Microsoft и Cisco, но существуют и реализации с открытым исходным кодом, например, *strongSwan*, *OpenIKEv2*, *Openswan*.

IPSec быстрее чем *OpenVPN* [4]. Но, многие межсетевые экраны блокируют трафик IPSec.

2) *OpenVPN* – решение VPN, работающее, на четвертом уровне *ISO/OSI*. Для обеспечения безопасности могут использоваться различные алгоритмы шифрования. По умолчанию используется *SSL/TLS* и процедура Диффи – Хеллмана для обмена ассиметричных ключей. Может инкапсулировать как пакеты *IP*, так и кадры *Ethernet*. Работает на базе *TCP* или *UDP*.

OpenVPN поддерживает аутентификацию пользователей по:

– заранее предустановленному симметричному ключу,

– сертификату (ассиметричное шифрование),

– паре логин/пароль.

По умолчанию, *OpenVPN* работает с использованием *UDP* в качестве транспортного протокола [2]. Такой сценарий производительнее, чем использование *OpenVPN* в режиме *TCP*, так как при передаче внутри туннеля *TCP* пакетов не возникает ситуации с инкапсуляцией *TCP* в *TCP*. Возникновение проблемы и необходимость отправить *TCP* пакет заново, в случае, когда *TCP* инкапсулируется в *TCP*, будет означать то, что вначале нижележащий уровень будет пытаться компенсировать возникшую проблему, затем эту же проблему будет компенсировать вышележащий уровень. [3] Однако, при блокировании межсетевыми экранами *UDP* трафика, *TCP* остается в качестве альтернативы.

Для шифрования *OpenVPN* использует библиотеку *OpenSSL* [2]. Это позволяет OpenVPN использовать все алгоритмы, доступные в *OpenSSL*. Кроме того, для создания дополнительного слоя безопасности соединения используется пакетная аутентификация по *HMAC* сигнатурам (функция названа *"HMAC Firewall"* в документации OpenVPN), а для улучшения производительности – аппаратное ускорение [2].

OpenVPN поддерживается на *Windows*, *Mac OS*, *Linux, Android, iOS*. Распространяется по лицензии *GPLv2*.

3) *WireGuard* – решение с открытым исходным кодом, использующее для своей работы *UDP*. Может использоваться как в топологии точка-точка, так и звезда (клиент/сервер). У *WireGuard* нет возможности выбора способа шифрования, как у *OpenVPN*. В *WireGuard* используется *Curve25519* для обмена ключами, *ChaCha20* для шифрования полезной нагрузки и *Poly1305* для аутентификации [4]. И изменить криптографические алгоритмы в случае с *WireGuard* без редактирование исходного кода не выйдет, тогда как *OpenVPN* использует библиотеку *OpenSSL* с широким выбором различных алгоритмов. Потенциально это делает *OpenVPN* безопаснее, так как, в случае обнаружения уязвимости в выбранном алгоритме можно просто переключиться на другой, не дожидаясь обновления от разработчиков. Кроме того, *OpenVPN* лучше подходит под задачу, когда её частью являются конкретные требования к выбору криптографических протоколов.

В отличие от *OpenVPN*, *WireGuard* входит в состав ядра *Linux*. Это дает ему преимущество по производительности, за счет того, что нет необходимости передавать пакеты из пространства ядра в пользовательское пространство. Согласно проведенным исследованиям разработчиков *WireGuard* (рис. 1) [4], *WireGuard* производительнее как *OpenVPN*, так и *IPSec* в плане пропускной способности и *RTT*.

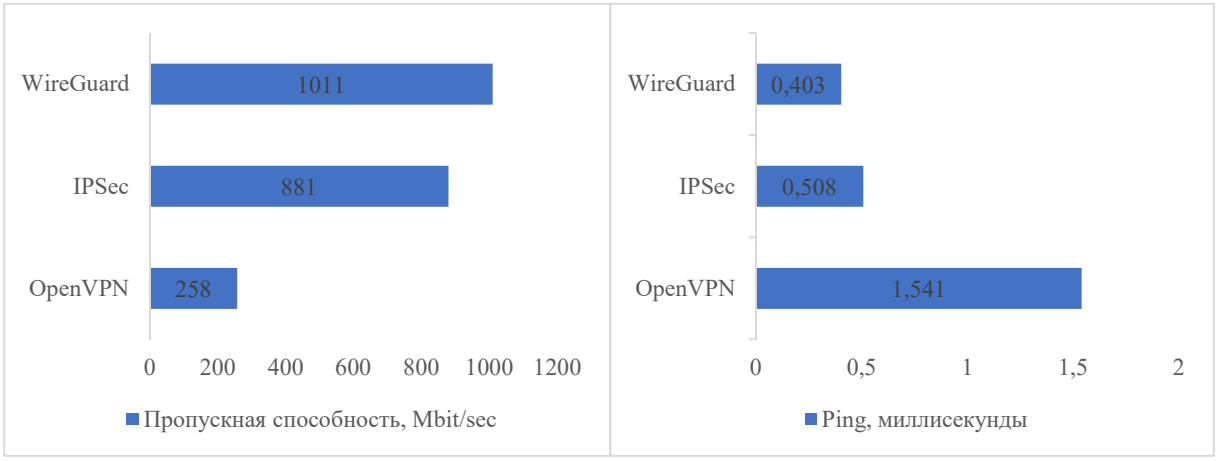


Рис. 1. Сравнение производительности IPSec, OpenVPN и WireGuard [4]

Рис. 1 – измерения, взятые из *WireGuard Whitepaper* [4], предоставленные разработчиком самого WireGuard. Они были проведены на следующем стенде:

1) Узел 1:
– ЦПУ: 4-х ядерный *Intel Core i7-3820QM* с 8-ю потоками,
– *Сетевая карта: Intel 82579LM* 1 Гбит/сек,
– *RAM: 16 GB;*
2) Узел 2:
– 2-х ядерный *Intel Core i7-5200U* с 4-мя потоками,
– *Сетевая карта: Intel I218LM* 1 Гбит/сек,
– RAM: 16 GB.

Для проведения измерений использовались утилиты *Iperf3* и *Ping*. Были проведены аналогичные измерения на виртуальных машинах с сопоставимыми вычислительными ресурсами (рис. 2).

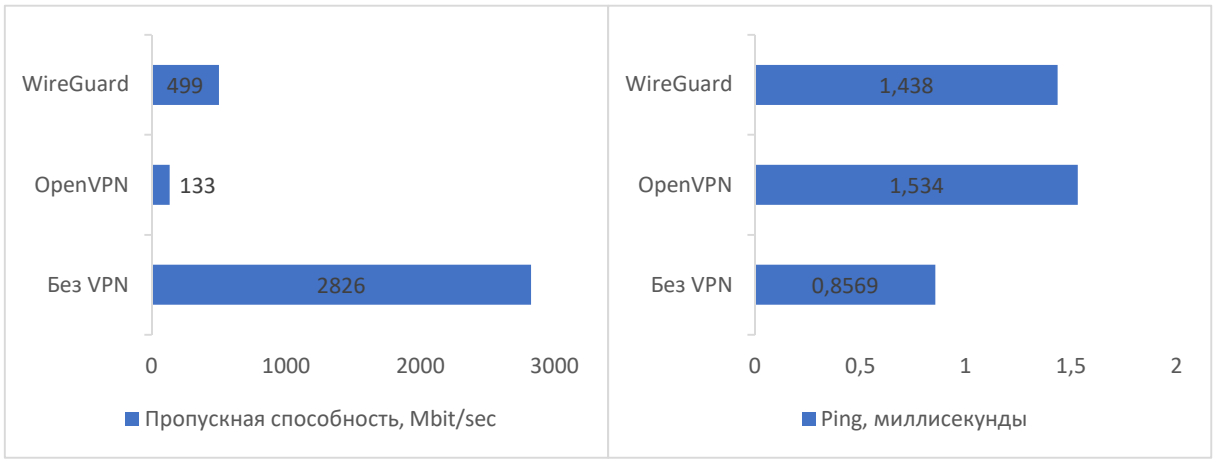


Рис. 2. Сравнение производительности *OpenVPN* и *WireGuard*

Такие отличия объясняются тем, что при проведении теста с рис. 1 использовался размер *MTU* больший, чем стандартный 1500. На это указывает

полученное среднее значение пропускной способности в 1011 Мбит/сек. При 20 байтах на *IP* заголовок, 8 байтах на *UDP* заголовок и 16 байтах на заголовок *WireGuard* максимально возможное значение пропускной способности должно быть значительно ниже. *VPN* в данном случае должен строиться поверх Интернет, и, так как, в сети интернет принятое значение *MTU* 1500 в большинстве систем, следует оставить значение *MTU* 1500 во избежание излишней сегментации.

Хотя проведенные измерения значительно отличаются от представленных разработчиками *WireGuard, WireGuard* все равно оказывается производительнее *OpenVPN* в 3,75 раза. При этом средние значения *RTT* у *OpenVPN* и *WireGuard* по результатами исследований отличаются незначительно (лишь на 0,1 миллисекунду).

В рамках облачной модели оказания услуг доступ к сервисам может быть обеспечен не только путем выдачи им глобального адреса, то есть обеспечивая глобальный доступ к ним, но и за счет использования *VPN*.

Для обеспечения услуг *VPN* лучше всего подходит *OpenVPN*, за счет того, что предоставляет наибольшие возможности при конфигурации тоннеля. Но, в качестве альтернативы, когда производительность *VPN* решения имеет больший приоритет, чем большие возможности при настройке, рекомендуется выбрать *WireGuard*.

Список используемых источников

1. What is a VPN? / Paul Ferguson, Geoff Huston. URL: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.169.7689&rep=rep1&type=pdf (дата обращения: 25.03.2022)

2. OpenVPN – How to. URL: https://openvpn.net/community-resources/how-to/

3. What is TCP Meltdown? URL: https://openvpn.net/faq/what-is-tcp-meltdown/

4. Donenfeld Jason A. WireGuard: Next Generation Kernel Network Tunnel. URL: https://www.wireguard.com/papers/wireguard.pdf (дата обращения: 25.03.2022)

Статья предоставлена заведующим кафедрой ИКС СПбГУТ, кандидатом технических наук, доцентом А. А. Зарубиным.

УДК 004.056
ГРНТИ 81.93.29

АНАЛИЗ ИСТОЧНИКОВ ДАННЫХ БЕЗОПАСНОСТИ ДЛЯ МОДЕЛИРОВАНИЯ И ОЦЕНИВАНИЯ КИБЕРАТАК

С. А. Веревкин[1,3], **Е. В. Федорченко**[1,2]

[1]Санкт-Петербургский Федеральный исследовательский центр Российской академии наук
[2]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
[3]Военно-космическая академия им А.Ф. Можайского

В работе описывается результат анализа наиболее популярных источников данных, содержащих сведения об угрозах и уязвимостях, а также дополнительные данные, на основе которых возможна разработка показателей, позволяющих идентифицировать атакующие действия в киберсреде. Представлены выводы, полученные в результате анализа различных баз данных с указанием преимуществ и недостатков источников информации каждого вида. Сформирована направленность дальнейшего применения результатов и в соответствии с этим определен наиболее актуальный с точки зрения предоставляемых данных источник информации.

уязвимости, обнаружение атак, базы данных, тестирование защищенности, риски.

Основной задачей проводимого исследования является сравнение информационных ресурсов, содержащих данные об уязвимостях и угрозах информационной безопасности с целью их последующего анализа, моделирования кибератак и формирования набора показателей атакующих воздействий для их оценивания. В рамках исследования, рассматривается три основных источника данных: 1) базы данных атак, сформированные на основе поведенческого анализа злоумышленника, например, Mitre CAPEC и ATT&CK [1, 2]; 2) частные базы атак, сформированные в результате работы команды тестирования защищенности, например, Atomic Red Team [5]; 3) базы данных уязвимостей CVE, например, CVE [6] и БДУ ФСТЭК [7].

В результате анализа структуры и содержания информации в перечисленных источниках данных получены следующие выводы:

1. В базах данных, сформированных на основе поведенческого анализа данных угроз безопасности информации, отмечается низкий уровень связности данных. Примером являются базы CAPEC [1] и ATT&CK [2], корреляция которых основана лишь на 112 шаблонах атак из 546. В свою очередь, низкая связность данных баз знаний ATT&CK и CAPEC ведет к невозможности формирования достоверных критериев профилирования сетевого трафика. Причиной этого является невозможность построения взаимосвязей до

конкретных реализаций этапов атаки, содержащихся в описании CVE. К преимуществам данных баз знаний относится унифицированный способ представления данных в формате стандарта STIX/TAXII [3], а также возможность рассмотрения процесса атаки в рамках концепции Kill chain (цепочка атак) с учетом анализа поведения злоумышленника на каждом из этапов реализации атаки.

2. Базы атак, сформированные на основе действий команд Red Team, полученные в результате реального тестирования защищенности собственной инфраструктуры отличаются узкой направленностью и отсутствием унифицированного представления содержащихся в них данных. Несмотря на существующие недостатки, данный источник информации значительно превосходит рассмотренные ранее базы знаний Mitre в объеме и качестве содержащихся в них данных, поскольку их формирование является результатом практической деятельности Red Team команд различных организаций. Важно выделить «гибридные» частные базы знаний, сформированные на основе концепции баз CAPEC и ATT&CK, поскольку подобный формат реализации делает возможным частичное внедрение методов анализа сетевого трафика. Тестирование «гибридной» базы знаний Atomic Red Team [5], основанной на Mitre ATT&CK наглядно представлено в работе [4], в рамках которой реализуется тестирование разработанного программного продукта, задачей которого является проведение последовательности атомарных атак в рамках kill chain базы Mitre ATT&CK и использование полученных данных в качестве входных данных системы оценки рисков информационной безопасности.

3. В рамках анализа актуальности применения баз данных уязвимостей на примере CVE [6] и БДУ ФСТЭК следует отметить содержание большего количества данных для анализа. В частности, база CVE насчитывает свыше 160 000 записей, из которых ~100 000 записей с 2015 г. по настоящее время. Из них ~40 000 записей содержат ссылки на эксплойт для реализации атаки. Несмотря на больший объем данных по сравнению с другими источниками и унифицированный формат представления, база CVE имеет ряд недостатков с точки зрения использования в качестве основного источника данных для решения задачи исследования. Основными причинами нецелесообразности использования базы CVE являются: 1) не все шаги атаки требуют наличия уязвимости; 2) возможность использования уязвимостей нулевого дня.

Выводы. Анализ баз данных, содержащих сведения об уязвимостях и угрозах информационной безопасности, а также их содержимого, показал целесообразность использования частных баз данных, основанных как на проведении атомарных атакующих воздействий, так и на проведении цепочек атак, для моделирования и оценивания кибератак, т. к. они позволяют связать сетевой трафик с уязвимостями и угрозами безопасности. Что

в дальнейшем позволит ввести дополнительные показатели для оценивания и прогнозирования кибератак, в том числе в реальном времени.

Дальнейшее исследование в данной области будет направлено на разработку модели кибератак и формализованных показателей, на основе которых планируется осуществлять прогнозирование развития атак и обнаружение не выявленных ранее уязвимостей (уязвимостей нулевого дня).

Работа выполнена при финансовой поддержке Гранта РНФ № 21-71-20078 в Санкт-Петербургском Федеральном исследовательском центре Российской академии наук.

Список используемых источников

1. Mitre ATT&CK database. URL: https://attack.mitre.org/
2. База шаблонов атак Mitre CAPEC. URL: https://capec.mitre.org/
3. Стандарт представления данных STIX. URL: https://stixproject.github.io/about/
4. Kryukov R., Doynikova E., Kotenko I. Security analysis of information systems based on attack sequences generation and testing // Proceedings of IDC 2021.
5. База тестров защищенности Atomic Red Team. URL: https://github.com/redcanaryco/atomic-red-team
6. База уязвимостей Mitre CVE. URL: https://cve.mitre.org/
7. Банк данных угроз ФСТЭК. URL: https://bdu.fstec.ru/

УДК 004.056.55; 535.14
ГРНТИ 81.93.29

АНАЛИЗ ВОЗМОЖНОСТЕЙ СЛУЖБЫ AZURE QUANTUM И ПАКЕТА СРЕДСТВ РАЗРАБОТКИ QUANTUM DEVELOPMENT KIT (QDK)

К. В. Вершинина[1,2], А. Р. Салтыков[1]

[1]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
[2]ООО «НТЦ ПРОТЕЙ»

Квантовые вычисления – это обширная междисциплинарная сфера исследований, сформированная на стыке программирования, физики, математики, машиностроения и компьютерных наук.

Azure Quantum представляет собой облачную службу с набором различных квантовых решений и технологий. Это открытая экосистема, которая предоставляет доступ к различному программному обеспечению, оборудованию и решениям для квантовых вычислений от корпорации Майкрософт и ее партнеров.

Целью статьи является предварительный анализ возможностей использования Azure Quantum и набора средств Quantum Development Kit (QDK) для создания квантовых алгоритмов и задач оптимизации.

Quantum Development Kit, QDK, Azure Quantum, QKD, Q#.

Одним из перспективных направлений квантовых коммуникаций является квантовое распределение ключей (QKD), алгоритм, схема и фундаментальные физические особенности которого были описаны в предыдущих исследованиях [1–4]. Также, более подробно были рассмотрены процессы симуляции квантового распределения и генерации ключей [5], в том числе были получены результаты выполнения такого моделирования на примере включения атак и других релевантных факторов в классический QKD-протокол BB84, что аналогично упомянуто в процессе разработки квантового программного обеспечения в таблице 1 (этап 4).

Для дальнейшего детального описания систем с QKD необходимо проводить исследования в специальных программных средах. Наиболее доступной и пользователеориентированной службой в целях проектирования QKD была выбрана система Azure Quantum и набор средств Quantum Development Kit (QDK).

Основными процессами в Quantum Azure являются квантовые вычисления и оптимизация, что реализуется на предметно-специфичном языке квантового программирования *Q#* [6].

Q# объединяет классические и квантовые вычисления, поддерживая общий поток управления во время выполнения алгоритма и гарантируя, что алгоритмы следуют законам квантовой физики и будут корректно выполняться на квантовых компьютерах [7].

Согласно представленной схеме (рис.), унифицированный интерфейс разработки представляет собой агрегирование вокруг процесса разработки компаний-лидеров рынка квантовых коммуникаций, таких как Microsoft, Toshiba, 1Qbit, IONq, Quantiuum, Rigetti.

Пакет Quantum Development Kit (QDK) по умолчанию включает: язык программирования Q# и его библиотеки, ядро IQ# для выполнения *Q#* в Jupiter Notebook, интерфейсы API для Python и .NET (*C#*, *F#* и VB.NET), расширения для Visual Studio Xcode и Visual Studio, функциональность по работе с приложениями Diskit, Cirq и их отправке в службу Azure Quantum [8].

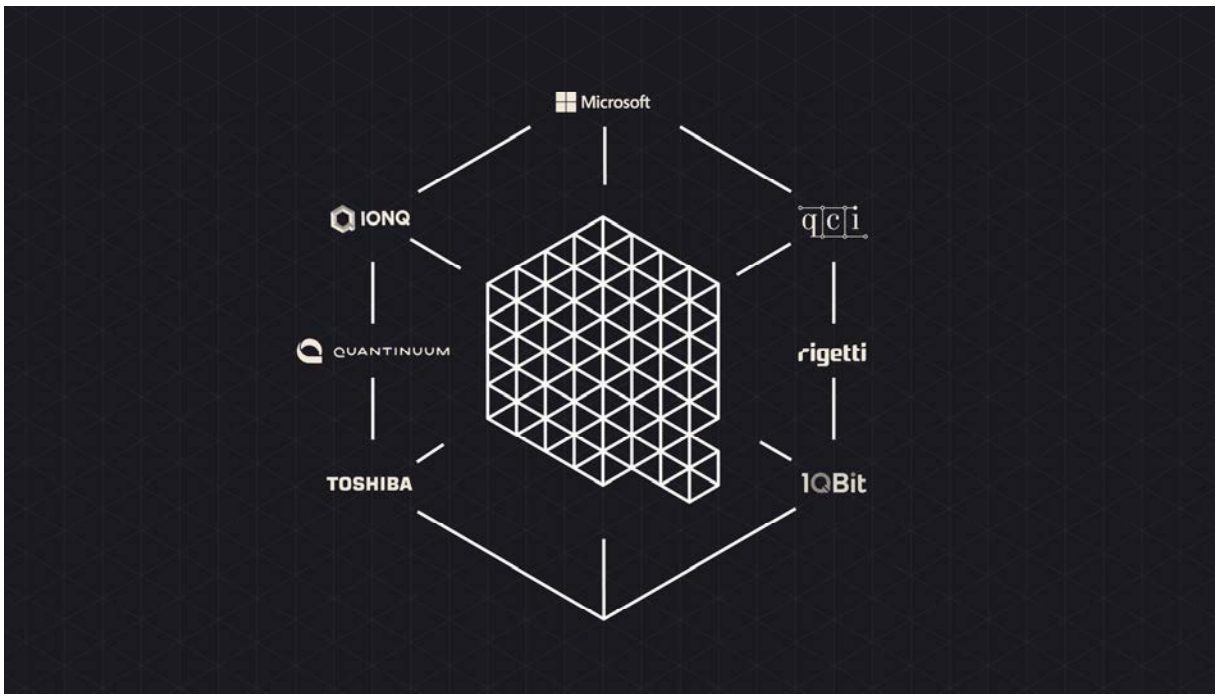


Рисунок. Унифицированный интерфейс разработки

В таблице показано поэтапное представление рабочего процесса разработки квантового программного обеспечения с применением QDK, где служба Azure Quantum представляет собой финальный этап разработки.

ТАБЛИЦА. Процесс разработки квантового ПО

Этап	Действие	Инструменты
1	Написание квантового кода	Q# VS/VS Code Jupyter Notebooks
2	Использование библиотек для поддержания высокого уровня кода	Библиотеки QDK
3	Интеграция с классическим ПО	Python Qiskit .NET Cirq
4	Запуск симуляции квантового кода	QDK simulation
5	Оценка ресурсов	Средство оценки ресурсов QDK
6	Запуск кода на квантовом оборудовании	Azure Quantum

Таким образом, существуют большие перспективы для интеграции службы Microsoft Azure Quantum и набора средств Quantum Development Kit (QDK) в процессы исследования квантовых коммуникационных сетей.

Впоследствии, квантовые решения для создания квантовых алгоритмов и задач оптимизации можно применять на существующей платформе Azure для получения реальных результатов и квантовых облачных решений,

вплоть до разработки квантового компьютера общего назначения. Примерами таких решений уже можно назвать: Quantanium *H*1 на базе Honeywell, IONQ – квантовый компьютер на связанных ионах, Quantum Circuits, Inc и Rigetti Quantum Cloud Services, что подтверждает практическую применимость инструментов Azure Quantum и QDK.

Список используемых источников

1. Вершинина К. В. Применение протокола BB84 для квантового распределения ключей (QKD) // Подготовка профессиональных кадров в магистратуре для цифровой экономики (ПКМ-2020). Региональная научно-методическая конференция магистрантов и их руководителей; сборник лучших докладов конф. СПб.: СПбГУТ, 2021. С. 166-171. ISBN 978-5-89160-204-5. URL: http://pkm.sut.ru/documents/Сборник_лучших_докладов_ПКМ-2021.pdf (дата обращения: 29.03.2022).

2. Vershinina X. V. Application of Quantum Mechanics Fundamental Laws for Quantum Key Distribution // 75th Anniversary Regional Scientific and Technical Conference of Students, Aspirants and Young Scientists «Studencheskaya vesna – 2021»: collection of scientific articles. Special issue. SPb.: SPbSUT, 2021. 118 p. URL: http://apino.spbgut.ru/ (data of request 29.03.2022).

3. Vershinina X. V., Saltykov A. R. Application of modified BB84 protocol in Quantum Key Distribution // ICAIT 2021: collection of scientific articles. SPb.: SPbSUT, 2021. Vol. 1. 770 p. URL: http://apino.spbgut.ru/ (data of request 29.03.2022).

4. Vershinina X. V., Saltykov A. R. Application of Quantum Key Distribution in WDM-PON Networks // ICAIT 2020: collection of scientific articles. SPb.: SPbSUT, 2020. Vol. 1. pp. 225-230. ISBN 978-5-89160-197-0. URL: http://apino.spbgut.ru/ (data of request 29.03.2022).

5. Vershinina X. V. Quantum key distribution based on optical communications: detailed analysis // Подготовка профессиональных кадров в магистратуре для цифровой экономики (ПКМ-2021). Региональная научно-методическая конференция магистрантов и их руководителей; Сборник лучших докладов конф. СПб.: СПбГУТ, 2022. С. 180-183. ISBN 978-5-89160-248-9. URL: http://pkm.sut.ru (дата обращения: 29.03.2022).

6. Руководство по Реализации квантового генератора случайных чисел на языке Q# // Документация по Azure Quantum. URL: https://docs.microsoft.com/ru-ru/azure/quantum (дата обращения: 29.03.2022).

7. Общие сведения о языке программирования Q# и пакете средств разработки Quantum (QDK) // Документация по Azure Quantum. URL: https://docs.microsoft.com/ru-ru/azure/quantum (дата обращения: 29.03.2022).

8. Настройка локальной среды разработки для Azure Quantum // Документация по Azure Quantum. URL: https://docs.microsoft.com/ru-ru/azure/quantum (дата обращения: 29.03.2022).

Статья представлена заведующим кафедрой ФиЛС СПбГУТ, кандидатом технических наук, доцентом М. С. Былиной

УДК 004.932.2
ГРНТИ 20.23.19

ОБНАРУЖЕНИЕ СХОЖИХ ТОВАРНЫХ ЗНАКОВ С ПОМОЩЬЮ АНАЛИЗА ИСПОЛЬЗОВАННОЙ ЦВЕТОВОЙ ПАЛИТРЫ.

Д. В. Веснин, А. А. Чечулин

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В данной статье рассматривается решение актуальной задачи поиска похожих товарных знаков. Предложена методика обнаружения схожих товарных знаков с помощью анализа использованной цветовой палитры, способная быстро работать на больших объемах данных. Проведен её анализ, выявлены достоинства и недостатки такого метода, а также проанализирована возможность комбинирования данного метода с другими решениями.

поиск похожих логотипов, rgb гистограммы, k-nn поиск.

Товарный знак (логотип) является одним из наиболее ценных объектов интеллектуальной собственности компании. Товарные знаки требуют регистрации, чтобы избежать репутационного ущерба и ущерба для прибыли, вызванного нарушением прав на товарный знак. Товарный знак может быть зарегистрирован только в том случае, если он является уникальным и не похож на другие зарегистрированные товарные знаки.

По оценкам, в 2020 году в мире было подано 13,4 млн заявок на регистрацию товарных знаков. Это почти на 1,9 миллиона больше, чем было подано в 2019 году, и является увеличением на 16,5 % по сравнению с предыдущим годом. Такие высокие темпы роста были достигнуты, несмотря на начало пандемии COVID-19 и последовавший за ней глобальный экономический спад. Он также знаменует собой одиннадцатый год подряд роста, после окончания глобального финансового кризиса и возвращение к двузначным показателям роста, по сравнению с 5,7 % в 2019 году (рис. 1) [1].

Чтобы предотвратить кражу интеллектуальной собственности, необходим способ для поиска похожих логотипов. Ручная проверка практически невозможна, из-за проблем с масштабированием. Необходим автоматизированный инструмент для поиска похожих логотипов, который сможет быстро обрабатывать большие объемы данных.

Существуют разные подходы для поиска похожих логотипов. Основными являются поиск по признакам, генерируемым нейросетями, а также поиск по ключевым точкам (keypoints). Менее популярными являются пер-

цептивные хеши и RGB-гистограммы. В данной работе анализируются достоинства и недостатки RGB-гистограмм, а также возможности для реализации крупномасштабного поиска. Научная новизна заключается в сравнении различных метрик дистанции и специальных индексов поиска.

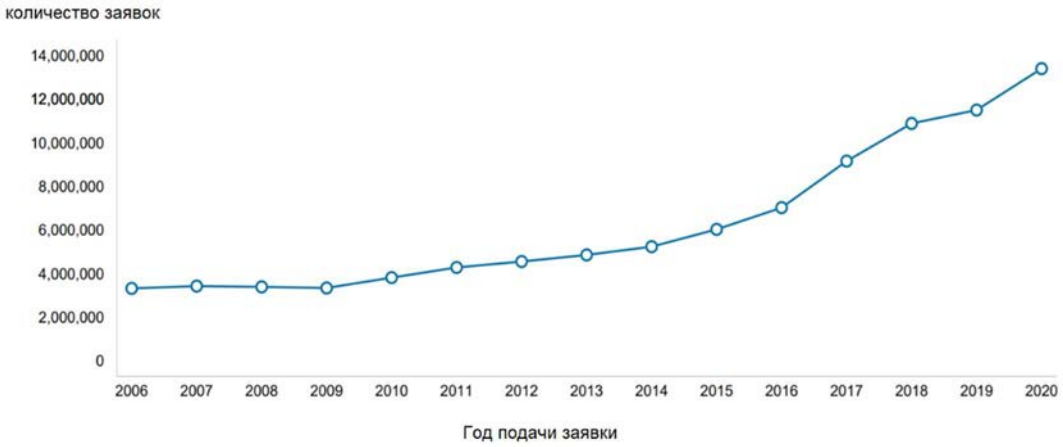


Рис. 1. График количества заявок на регистрацию новых товарных знаков [1]

Одним из способов поиска похожих изображений является сравнение RGB-гистограмм. RGB-гистограмма – это три отдельных гистограммы одного изображения, для 3 каналов: красного, зеленого и синего. Сравнивая гистограммы изображений, мы сравниваем распределение их цветовой палитры.

Для сравнения гистограмм обычно используется корреляция (1) или пересечение (2).

$$d(H_1, H_2) = \frac{\sum_I (H_1(I) - \bar{H}_1)(H_2(I) - \bar{H}_2)}{\sqrt{\sum_I (H_1(I) - \bar{H}_1)^2 \sum_I (H_2(I) - \bar{H}_2)^2}}, \quad (1)$$

где $\bar{H}_k = \frac{1}{N} \sum_J H_k(J)$ и N это количество интервалов гистограммы.

$$d(H_1, H_2) = \sum_I \min\big(H_1(I), H_2(I)\big). \quad (2)$$

Но для масштабного поиска, на десятках миллионах изображений линейный поиск не подходит. Современный подход — это векторизация данных и использование специальных библиотек, например faiss[2, 3], для реализации NN (Nearest Neighbor) и ANN (Approximate Nearest Neighbor) поиска. Последний наиболее подходит для поиска в многомиллионных массивах информации, снижение точности компенсируется большим приростом в скорости поиска.

Для генерации гистограмм используется библиотека OpenCV. Итоговая матрица имеет размеры NxNxN, где N это количество интервалов гистограммы. Данную матрицу мы трансформируем в вектор, используя операцию flatten. Далее, каждый элемент вектора делится на количество пикселей в изображении, тем самым гистограмма становится инвариантна к размеру изображения и теперь их можно сравнивать. Проведем тест, где сравним гистограммы с разным количеством интервалов, разные метрики оценки схожести и разные типы индексов в faiss. Flat Index проводит поиск по всем данным на процессоре, GpuFlat на видеокарте. Faiss IVF Flat проводит поиск с помощью Inverted File Index. В дополнение к корреляции (1) или пересечению (2), также проверяются дистанции L1 (3) и L2 (4).

$$d(H_1, H_2) = \sum_I |H_1(I) - H_2(I)|. \quad (3)$$

$$d(H_1, H_2) = \sqrt{\sum_I \left(H_1(I) - H_2(I)\right)^2}. \quad (4)$$

Тесты были проведены на наборе данных METU Trademark Dataset[4], самом большом наборе данных для задачи trademark retrieval. Данный набор данных насчитывает более 900 тысяч изображений. В качестве метрики был выбран mAP@100. mAP@k (Mean average precision at k) — это метрика, которая учитывает не только, сколько релевантных логотипов находится в выдаче, но также и их места. Чем больше данная метрика, тем больше релевантных логотипов в выдаче, и они выше к началу списка. Результаты представлены в таблице. Примеры поисковой выдачи (Faiss Flat L1) представлены на рис. 2 и рис. 3. Первое изображение – это изображение, по которому осуществляется поиск. Можно увидеть, что изображения в поисковой выдаче похожи на первое изображение по использованной цветовой палитре.

ТАБЛИЦА. Результаты тестирования

Метод сравнения	Количество интервалов гистограммы	mAP@100	Время на поиск 100 похожих изображений, мс
Корреляция	8	0.0228	1 634
	14	0.0242	4 438
Пересечение	8	0.0302	1 445
	14	0.0342	3 270
Faiss Flat L1	8	0.0302	2 103
	14	0.0341	11 500
Faiss Flat L2	8	0.0224	597
	14	0.0217	3 311

Метод сравнения	Количество интервалов гистограммы	mAP@100	Время на поиск 100 похожих изображений, мс
Faiss IVF Flat L2	8	0.0221	53
	14	0.0211	268
Faiss GpuFlat L1	8	0.0302	26
	14	-	-
Faiss GpuFlat L2	8	0.0224	8
	14	-	-

Рис. 2. Пример поисковой выдачи

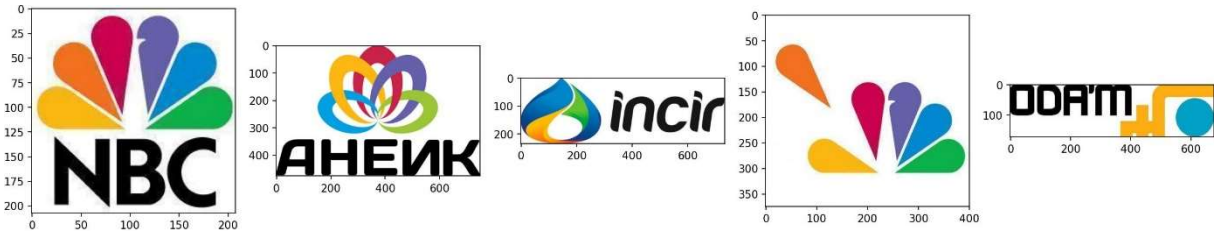


Рис. 3. Пример поисковой выдачи

Достоинством RGB гистограмм является то, что они инварианты к трансформациям, не меняющим распределение цветов на изображении. Данный подход позволяет находить изображения похожие по цветовой палитре, даже при полностью измененной геометрии, довольно быстро. Недостатком данного подхода является тот факт, что RGB гистограммы не учитывают геометрию изображения, вследствие чего получена низкая точность на наборе данных, который в основном содержит изображения, схожие геометрически. Комбинация нескольких признаков (например, цвета и текстуры, или другого признака, описывающего геометрию изображения) значительно повышает общую точность системы [4]. В тоже время длина получившихся векторов и необходимость использования L1 дистанции, которая не поддерживается специальными структурами данных большинства ANN фреймворков, затрудняет эксплуатацию данного метода. Для решения этих проблем необходимы дальнейшие исследования. Существует несколько направлений для дальнейших исследований: более компактные

и точные признаки цвета, разработка модуля faiss для использования L1 дистанции в поисковом индексе IVF, структуры данных оптимизированные для поиска по дистанции L1 среди разреженных (sparse) векторов.

Список используемых источников

1. World Intellectual Property Indicators 2021. URL: https://www.wipo.int/edocs/pubdocs/en/wipo_pub_941_2021.pdf (дата обращения: 04.02.2022).

2. Meta Research. A library for efficient similarity search and clustering of dense vectors. URL: https://github.com/facebookresearch/faiss (дата обращения: 04.02.22).

3. Johnson, Jeff; Douze, Matthijs; Jégou, Hervé. Billion-scale similarity search with GPUs // arXiv preprint arXiv: 1702.08734, 2017.

4. Tursun, Osman; Aker, Cemal; Kalkan, Sinan. A Large-scale Dataset and Benchmark for Similar Trademark Retrieval // arXiv preprint arXiv: 1701.05766, 2017.

УДК 004.056.53
ГРНТИ 81.93.29

ПОДХОД К ОБНАРУЖЕНИЮ АНОМАЛИЙ И АТАК В КОНТЕЙНЕРНЫХ СИСТЕМАХ НА ОСНОВЕ ЖУРНАЛОВ ЛОГОВ

Л. А. Виткова

Санкт-Петербургский Федеральный исследовательский центр Российской академии наук

Все, что происходит в операционной системе в целом можно представить в виде последовательности событий. Extended Berkeley Packet Filter (eBPF) – это подсистема ядра Linux, дающая возможность писать небольшие программы, которые будут запущены ядром в ответ на событие. В статье рассматривается подход обнаружения аномалий и атак, позволяющий формировать белые и черные списки системных вызовов, создавать профили поведения контейнеров на основе данных, полученных при помощи зонда eBPF. Предложенный подход расширяет горизонт контроля событий информационной безопасности в ОС Linux.

Extended Berkeley Packet Filter, eBPF, обнаружение аномалий, обнаружение атак, контейнерные системы.

Введение

По данным Фонда облачных вычислений, использование контейнеров в производстве увеличилось на 300 % в период с 2016 по 2020 год

(рис. 1) [1]. Другими словами, организации постепенно отходят от статичных и выделенных инфраструктур и переходят к микросервисам и контейнерным рабочим нагрузкам.

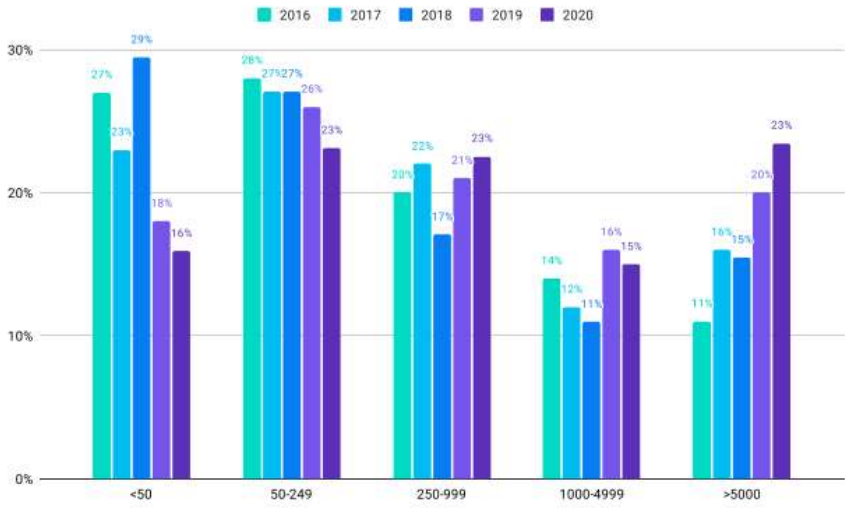


Рисунок. Диаграмма ответов на вопрос:
«Сколько контейнеров обычно работает в вашей компании /организации?» [1]

Инструменты оркестровки контейнеров, такие как Kubernetes, играют ключевую роль в этой тенденции, и отделам информационной безопасности необходимо обновлять модели угроз с учетом постоянно меняющейся инфраструктуры.

В 2021 году Контейнеры стали стандартом для доставки приложений и единицей для доставки вычислительных ресурсов и вспомогательных средств в эпоху облачных вычислений. Контейнерные среды выполнения с контейнерами Linux, такими как runC, предлагают отличные функции, такие как легкий вес, высокая эффективность, автономное включение, одноразовая упаковка и эксплуатация. Они очень популярны среди контейнеров, разработчиков и пользователей [2].

Несмотря на то, что все более популярные контейнерные технологии и приложения становятся новым интерфейсом для облачных вычислений, контейнерные технологии в среде облачных вычислений по-прежнему сталкиваются с новыми проблемами информационной безопасности. Несколько контейнеров используют одно и то же ядро, что приводит к неотъемлемым недостаткам изоляции и безопасности. Следовательно, Защита безопасности требует многоуровневой глубокой защиты и более глубокого представления о процессах в ядре хоста [3].

В статье рассматривается подход обнаружения аномалий и атак, позволяющий формировать белые и черные списки системных вызовов, создавать

профили поведения контейнеров на основе данных, полученных при помощи зонда eBPF. Предложенный подход расширяет горизонт контроля событий информационной безопасности в ОС Linux.

Подход к обнаружению аномалий и атак в контейнерных системах

Прежде всего в ходе исследования рассматривались признаки аномалий и атак [4]:

Аномалии:

- Появление новых типов событий.
- Исчезновение существующих типов событий.
- Изменение интенсивности событий (количество в секунду).
- Изменение пропорций типов событий.

Атаки:

- Появление характерных типов событий.
- Появление характерных аргументов событий.
- Появление характерных последовательностей событий.

Подход (А) к обнаружению аномалий в контейнерных системах заключается в формировании белых списков системных вызовов, а именно:

1. Формирование белых списков системных вызовов для контейнера в период нормальной активности;
2. Формирование белых списков системных вызовов и их аргументов для контейнера в период нормальной активности;
3. Формирование белых списков последовательности системных вызовов контейнера в период нормальной активности.

К аномалии относится любое отклонение от одного из трех вариантов белых списков.

Подход (Б) к обнаружению атак в контейнерных системах заключается в формировании черных системных вызовов, а именно:

1. Формирование черных списков системных вызовов для контейнера в период атаки;
2. Формирование черных списков системных вызовов и их аргументов для контейнера в период атаки;
3. Формирование черных списков последовательности системных вызовов контейнера в период атаки.

Эксперимент

Для эксперимента был выбран программный продукт (сборщик) Tracee [5], который собирает данные при помощи зонда eBPF. На хосте запускались следующие контейнеры [6]:

1. Kali linux.
2. Простая имитация почтовой формы.

3. Сервер Nginx, на котором размещен простой двухстраничный вебсайт.

4. Redis база данных.

5. Контейнер с Elastic search.

Для каждого контейнера были выбраны эксплойты, который были реализованы с контейнера Kali linux.

Таким образом были получены наборы данных, который размечались по времени: нормальная активность/аномальная активность (время атаки).

Тестирование подхода показало, что:

1. 1-й подход (А и Б) работает недостаточно корректно. Были обнаружены аномалии и атаки в период нормальной активности, но в период аномалии и атаки появляются ложные пропуски. Однако это самый быстрый подход и списки весят меньше 1 КБ.

2. 2-й подход (А и Б) работает лучше всего. Ложных срабатываний не бывает. Подход работает в течение нескольких минут, но списки весят больше 1 МБ.

3. 3-й подход (А и Б) работает, но в белом списке есть ложные срабатывания. Подход работает в течение нескольких минут. Списки весят меньше 1 МБ.

Заключение

В ходе исследования проведено тестирование систем сбора данных с поддержкой зонда eBPF. Сформированы наборы данных с аномальной, нормальной активностью и атаками. Разработан подход обнаружения аномалий и атак. Проведено тестирование подходов обнаружения аномалий и атак. Исследование показало перспективность подхода обнаружения аномалий и атак в контейнерных системах. В будущем планируется повысить точность подхода за счет разработки алгоритмов разметки данных во время атаки на контейнер.

Работа выполнена при частичной финансовой поддержке FFSU-2019-0002-Бюджетная тема в СПб ФИЦ РАН.

Список используемых источников

1. CNCF Annual Report 2020. URL: https://www.cncf.io/reports/cncf-annual-report-2020/ (дата обращения: 29.03.2022)

2. Bentaleb O. et al. Containerization technologies: Taxonomies, applications and challenges //The Journal of Supercomputing. 2022. Т. 78. №. 1. С. 1144–1181.

3. Kithulwatta W. et al. Adoption of Docker Containers as an Infrastructure for Deploying Software Applications: A Review // Advances on Smart and Soft Computing. 2022. С. 247–259.

4. Чечулин А. А., Котенко И. В. Обнаружение и противодействие сетевым атакам на основе комбинированных механизмов анализа трафика // Методы и технические средства обеспечения безопасности информации. 2009. С. 69.

5. Aqua Tracee: Runtime eBPF threat detection engine/. URL: https://www.aquasec.com/products/tracee/ (дата обращения: 29.03.2022)

6. Cyber_Security hackathon 2021. URL: https://github.com/frizzymonsta/cyber_security21 (дата обращения: 29.03.2022).

УДК 004.056.53
ГРНТИ 81.93.29

АЛГОРИТМ АНАЛИЗА ДАТ РЕГИСТРАЦИИ КОММЕНТАТОРОВ В СОЦИАЛЬНОЙ СЕТИ ВК

Л. А. Виткова

Санкт-Петербургский Федеральный исследовательский центр Российской академии наук

Сегодня ситуация в социальных сетях и с социальными сетями далеко не однозначная. Уровень информационного шума постоянно растет. Различить истинный источник от бота практически не представляется возможным без специальных алгоритмов. Сложность обнаружения ботов и распространяемых ими фейков проявляется тогда, когда требуется собрать огромный объем информации и провести контент анализ. В статье предложен алгоритм анализа дат регистрации комментаторов в социальной сети Вконтакте, который позволяет быстро получить представление о странице комментатора.

анализ социальных сетей, обнаружение ботов, фейки, нежелательная информация, информационная безопасность.

Введение

Сегодня ситуация в социальных сетях и с социальными сетями далеко не однозначная. Уровень информационного шума настолько вырос в период с февраля 2022 года, резко, скачкообразно, что различить истинный источник от бота практически не представляется возможным без специальных алгоритмов. Сложность обнаружения ботов и распространяемых ими фейков проявляется тогда, когда требуется собрать огромный объем информации и провести контент анализ [1, 2].

Возникает следующее противоречие: Государство и платформы социальных сетей заинтересованы в защите от нежелательной информации, и от ботов, задействованных в распространении фейков. Однако ни государство,

ни платформы социальных сетей фактически не могут своевременно анализировать такой объем информации. Второй стороной возникающего противоречия является то, что современные исследования зачастую направлены на контент анализ текстов, семантику. Однако в социальных сетях создается слишком много коротких сообщений, комментариев. И анализ всего множества таких сообщений требует огромных вычислительных ресурсов [3–5].

Задача текущего исследования состоит в том, чтобы выработать и предложить такой алгоритм, который позволит на базе дискретных признаков выявлять распространителей нежелательной информации в социальных сетях.

Алгоритм анализа дат регистрации комментаторов

Данный алгоритм позволяет получить даты создания профилей пользователей. В отличие от других программных компонентов, которые образаются к API платформы социальной сети, данный компонент использует парсинг веб-страниц. Связано это с тем, что в API Вконтакте отсутствуют методы, позволяющие получить даты создания профилей пользователей. Входными данным программного компонента является файл со списком идентификаторов пользователей, по которым необходимо получить даты регистрации профилей.

Алгоритм:

Шаг.1 Импорт библиотек. Используемые в программном компоненте библиотеки:

- Openpyxl – библиотека для работы с Microsoft Office Excel-файлами.
- Re – библиотека для работы с регулярными выражениями.
- Urllib.requests – библиотека, позволяющая запрашивать веб-страницы по различным ссылкам.

Шаг. 2 Чтение исходного файла со списком идентификаторов пользователей, по которым необходимо получить даты регистрации профилей.

Шаг 3. Подстановка идентификаторов пользователей в URL и отправка запроса на загрузку веб-страницы с XML-информацией о нем.

Шаг 4. Фильтрация информации о пользовати и сбор даты регистрации профиля.

Шаг 5. Сохранение даты регистрации профиля в итоговый файл.

После получения даты регистрации по одному пользователю, берется из исходного файла следующий по списку идентификатор и весь процесс повторяется.

По итогу работы алгоритма формируется итоговый файл, содержащий в себе идентификаторы пользователей и даты регистрации их профилей (листинг 1).

```
import urllib.request
import re
from openpyxl import load_workbook

wb = load_workbook('source_file.XLSX')
sheet = wb['Лист1']
row_count = sheet.max_row
my_list = []

for i in range(2, row_count+1):
    my_list.append(sheet.cell(row=i, column=1).value)

complete_list = []
counter = 1
for i in range(0,len(my_list)):
    vk_link = "https://vk.com/foaf.php?id="+ str(my_list[i])
    with urllib.request.urlopen(vk_link) as response:
     vk_xml = response.read().decode("windows-1251")
     parsed_xml = re.findall(r'ya:created dc:date="(.*)"', vk_xml)
     complete_list.append(parsed_xml)
     counter+=1
j=0

for i in range(2, row_count+1):
    sheet.cell(row=i, column=3).value = str(complete_list[j])
    j+=1

wb.save("final_file.XLSX")
```

Листинг 1. Алгоритм анализа дат регистрации комментаторов в социальной сети Вконтакте

Эксперимент

Для сбора входных данных были выбраны 50 страниц СМИ России. Далее были собраны все идентификаторы комментаторов, который участвовали в дискуссиях под постами в период с 24.02.22-09.03.2022. В наборе данных представлены 747 486 комментария, которые были созданы 113 471 комментаторами.

Исследование показало, что из всех комментаторов 2 823 шт. оставили 29 972 сообщения и были уже заблокированы на момент сбора данных о дате регистрации (13.03.2022). В период с начала 2022 года по 09.03.2022 зарегистрировано 2 227 шт. комментаторов. При этом схема и даты регистраций комментаторов выглядят следующим образом (табл.). Всего 05.03.2022 было зарегистрировано 96 шт. комментаторов из 113 471 шт.

ТАБЛИЦА. Пример дат регистрации комментаторов СМИ в период с 24.02.2022–09.03.2022 в социальной сети Вконтакте

Идентификатор	Дата и время регистрации
708….97	Дата 2022-03-05 Время 23:11:15
708….35	Дата 2022-03-05 Время 23:00:28

Идентификатор	Дата и время регистрации
708….25	Дата 2022-03-05 Время 22:58:25
708….08	Дата 2022-03-05 Время 22:18:24
708….09	Дата 2022-03-05 Время 21:55:31
708… 51	Дата 2022-03-05 Время 21:21:00
708… 70	Дата 2022-03-05 Время 21:17:50
708….87	Дата 2022-03-05 Время 20:56:21

В результате тестирования работы алгоритма анализа дат регистрации комментаторов в социальной сети Вконтакте были получены данные, указывающие на наличие групп пользователей, зарегистрированных одним днем с небольшим интервалом по времени регистрации. Приведенный пример для 05.03.2022 это один из многих случаев, в наборе данных достаточно много таких групп. И это позволяет как минимум сократить нагрузку на контент анализ, за счет выявления наиболее подозрительных страниц комментаторов.

Заключение

В статье предложен алгоритм анализа дат регистрации комментаторов в социальной сети Вконтакте, который позволяет быстро получить представление о дате создания страницы комментатора и выделить из множества авторов, тех, кто появился в сети в период начала информационного конфликта.

Работа выполнена при финансовой поддержке Гранта РНФ 18-71-10094 в СПб ФИЦ РАН.

Список используемых источников:

1. Kolomeets M., Chechulin A. Analysis of the Malicious Bots Market // 2021 29th Conference of Open Innovations Association (FRUCT). IEEE, 2021. С. 199–205.

2. Виткова Л. А., Зеличенок И. Ю. Методика мониторинга и диагностики локальных инцидентов с потенциалом протестной мобилизации // Информатизация и связь. 2021. №. 5. С. 90–96.

3. Виткова Л. А. и др. Анализ методов выявления и оценки страниц лидеров мнений в социальных сетях // Актуальные проблемы инфотелекоммуникаций в науке и образовании. IX Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2019. С. 233–237.

4. Vitkova L., Kolomeets M. Approach to identification and analysis of information sources in social networks //International Symposium on Intelligent and Distributed Computing. – Springer, Cham, 2019. – С. 285-293.

5. Виткова Л. А. Модель и алгоритмы защиты от вредоносной информации в социальных сетях // Актуальные проблемы инфотелекоммуникаций в науке и образовании. X Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2020. С. 235–240.

УДК 004.056.53
ГРНТИ 81.93.29

ИЗУЧЕНИЕ УЯЗВИМОСТЕЙ В СИСТЕМЕ «УМНОГО» ДОМА И МЕТОДОВ ИХ ОБНАРУЖЕНИЯ

Л. А. Виткова, Е. Д. Едемская

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

«Умный» дом представляет собой автоматизированную систему управления комфортом. В подобных системах существует ряд уязвимостей, которые необходимо своевременно обнаруживать. При этом могут появляться новые уязвимости. В работе рассматриваются категории устройств умного дома и соответствующие им уязвимости. А также описаны существующие методы обнаружения уязвимостей в IoT.

умный дом, интернет вещей, уязвимости умного дома, безопасность умного дома.

Введение

В настоящее время системы «умного» дома находят все большее распространение. Они находят свое применение в жилых многоквартирных и индивидуальных домах, медицинских и государственных организациях. Как у любой автоматизированной системы у «умного» дома есть ряд уязвимостей, которые необходимо своевременно обнаруживать и нейтрализовать. Тем самым избегая утечек данных, получения несанкционированного доступа и других угроз [1, 2].

Анализ

Рассмотрим несколько категорий устройств и их уязвимостей, которые наиболее часто встречаются в системе «умного» дома. Эксплуатируя эти уязвимости, злоумышленник может вывести оборудование из строя, тем самым получив доступ к дому. Также наличие данных недостатков обуславливает ложное срабатывание некоторых устройств, которое не может не беспокоить владельца «умного» дома.

Датчики автоматизации. Данный элемент является обязательной частью умного дома, сюда относятся датчики, отслеживающие движение и датчики, реагирующие на параметры среды. Рассмотрим несколько приборов:

- Датчики, фиксирующие инфракрасное излучение, обладают двумя недостатками. Первый из них – наличие «слепой зоны», нахождение в которой предметов или людей означает их невидимость для датчика. Вторым

недостатком является ограничение по диапазону температур, обычно от (−10) до +40 °С.

• Ультразвуковой датчик движения исследует окружающее пространство с помощью звуковых волн. Основные уязвимости данного устройства это – ограниченный по расстоянию диапазон чувствительности (при нахождении объекта ближе чем 200 мм к датчику появляются ложные срабатывания) и наличие перекрестных помех при близком расположении датчиков друг относительно друга.

Исполнительные устройства. В этой категории относятся устройства, преобразующие команды в действия. Например, электромеханические приводы (открытие/закрытые окон, дверей, калиток и т. д.), главным недостатком которых является недостаточная защита от механических повреждений.

Центральные устройства. Контроллер управляет всеми компонентами «умного» дома. У данных устройствах множество уязвимостей. Например, у контроллера AMX NX-1200 исследователями была выявлена уязвимость в процессе процедуры аутентификации. Во внутренней базе данных находится скрытая учетная запись администратора, при получении доступа к которой можно управлять всей системой «умного» дома. Также все контроллеры уязвимы при электромагнитных помехах.

Помимо уязвимостей, связанных с устройствами существуют уязвимости, не привязанные к конкретному оборудованию. Используя эти незащищенные места, злоумышленник может реализовать атаки типа Man-in-the-Middle, подслушивать жертву или получить доступ к определенной системе и ее содержимому [3, 4]. В числе наиболее распространенных проблем оказались следующие:

• Слабое шифрование данных внутри системы «умного» дома. Для реализации надежного механизма шифрования необходимы большие вычислительные мощности, но «умный» дом управляется микроконтроллером, который не обладает такими ресурсами.

• Отсутствие механизма аутентификации легитимного пользователя. Распоряжение компонентами должно осуществляться только после аутентификации пользователя в системе. Так как управление «умным» домом чаще всего осуществляется со смартфона, планшета или другого портативного устройства с использованием беспроводной связи, возникает угроза перехвата идентификационных данных, которые в дальнейшем могут использоваться третьими лицами для получения несанкционированного доступа к системе.

• Необходимость наличия защищенного канала связи. Для коммуникации устройств друг с другом, управления ими и их обновлением необходим защищенный канал. Так по каналу Bluetooth устройство может принять

файл с вирусом, не запросив аутентификации. По каналу Wi-Fi злоумышленник может авторизоваться во внутренней сети «умного» дома и внедрить вредоносное программное обеспечение.

- Конфликт оборудования от разных производителей. При построении системы «умного» дома редко используется оборудование исключительно одного производителя, что приводит к конфликту протоколов обмена данными. Поэтому внедрение устройств от разных производителей может привести к появлению различный уязвимостей, например, к некорректной реализации защищенного соединения между устройствами, что влечет за собой угрозу перехвата данных.

Существует несколько путей выявления рассмотренных уязвимостей. Наиболее эффективным является экспериментальный метод, заключающийся в тестировании оборудования (намеренном создании условий, при котором работа оборудования может быть нарушена) [5, 6].

Например, для выявления границ «слепой зоны» в области работы датчика перемещают объект, который при попадании в «слепую зону» перестает быть видимым для датчика. Для исследования реакции контроллера на электромагнитные помехи они создаются группой исследователей искусственно, тем самым проверяется реакция устройства на помехи.

Для выявления уязвимостей в механизмах работы не связанных непосредственно с устройствами так же применяется экспериментальный подход. Группа исследователей собирают данные о работе алгоритмов системы «умного» дома, по результатам которых имитируются атаки, тем самым обнаруживаются «дыры» в работе «умного» дома.

Заключение

Единого универсального подхода или порядка действий для выявления уязвимостей в системе «умного» дома не существует. Также и не существует решения, позволяющего избавиться от всех уязвимостей. Проведенное исследование говорит о необходимости разработки алгоритма и методики выявления уязвимостей в системе «умного» дома.

Список используемых источников

1. Izrailov K., Chechulin A., Vitkova L. Threats classification method for the transport infrastructure of a smart city // 2020 IEEE 14th International Conference on Application of Information and Communication Technologies (AICT). IEEE, 2020. pp. 1–6.

2. Березина Е. О., Виткова Л. А. Модель угроз IoT в программно-конфигурируемых сетях // Актуальные проблемы инфотелекоммуникаций в науке и образовании. X Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2020. С. 130–134.

3. Виткова Л. А., Гераськина В. С., Ушаков И. А. Методы управления информационной безопасностью при возникновении чрезвычайной ситуации // Актуальные про-

блемы инфотелекоммуникаций в науке и образовании. VIII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2018. С. 164–168.

4. Васильев А. И., Гребешеков А. Ю. Проблемы защиты информации в интернете вещей // XVII Междунар. науч.-техн. конф. «Проблемы техники и технологий телекоммуникаций» тр. конф. Самара, 2016. С. 191–192.

5. Huichen Lin and Neil W. Bergmann, IoT Privacy and Security Challenges for Smart Home Environments [Электронный ресурс] // Multidicular Digital Publishing Institute, vol. 7, issue 3, 2016, URL: https://www.mdpi.com/2078-2489/7/3/44/htm

6. Виткова Л. А., Израилов К. Е., Чечулин А. А. Классификация уязвимостей интерфейсов транспортной инфраструктуры умного города // Актуальные проблемы инфотелекоммуникаций в науке и образовании. X Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2020. С. 253–258.

УДК 004.056.53
ГРНТИ 81.93.29

АНАЛИЗ IPTV ДЛЯ ОБНАРУЖЕНИЯ ПИРАТСКОГО КОНТЕНТА ТВ-КАНАЛОВ

Л. А. Виткова[2], А. Л. Зрелова[1,2]

[1]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича
[2]Санкт-Петербургский Федеральный исследовательский центр Российской академии наук

Сегодня высокий уровень влияния цифровых технологий на жизнь каждого человека является неоспоримым фактом. Это коснулось и телевидения. Развитие широкополосного доступа в Интернете и высокая скорость передачи данных облегчают доступ к IPTV. Популярность цифрового ТВ приводит к росту нелегальных источников и трансляций. При этом практически отсутствуют методики обнаружения пиратского контента ТВ каналов. В работе проведен анализ IPTV и предложена методика обнаружения пиратского контента ТВ-каналов.

IPTV, архитектура IPTV, методика обнаружения пиратского контента, интеллектуальная собственность, незаконная трансляция.

Введение

За последние 10–15 лет увеличилось влияние цифровых технологий на жизнь каждого человека. Это коснулось и телевидения. Современные технологии позволяют минимизировать оборудование для просмотра TV. IPTV позволяет транслировать телевизионные каналы по сети передачи дан-

ных. При сравнении качества изображения традиционное телевидение проигрывает IPTV, что увеличивает спрос на данную услугу. Развитие широкополосного доступа в Интернете и высокая скорость передачи данных облегчают доступ к легальным IPTV, но это также упрощает доступ к нелегальным источникам.

Анализ

Рассмотрим принцип работы IPTV. Пользователь выбирает телеканал и отправляет сигнал на сервер провайдера. С сервера-источника передается поток контента на устройство пользователя. Приложение или подключенная к устройству приставка декодирует IP-пакеты и выводит их на экран. Контент для IPTV поставляется через частично закрытую сетевую инфраструктуру, доступ в которую невозможен через сеть Интернет.

На данный момент в Интернете можно найти тысячи провайдеров IPTV, которые предоставляют доступ к телеканалам со всего мира. Для легального проведения трансляций необходима лицензия IPTV. В данной лицензии должно быть четко указано, какую территорию охватывает вещание. При поиске подходящего IPTV можно найти провайдеров, предлагающих за небольшую плату доступ к огромному количеству телеканалов, даже запрещенных на данной территории.

Структура IPTV

Передача контента основана на 5 протоколах [1]:

- UDP – используется для передачи потокового видео и аудио;
- HTTP – используется для организации интерактивных сервисов и передачи потокового видео и аудио;
- RTSP – используется для управления потоками вещания;
- RTP – используется для передачи потокового видео;
- IGMP – используется для управления мультикаст-потоками.

В отличии от интернет-телевидения, IPTV использует сквозную архитектуру, т. е. пользователь получает контент от интернет-провайдера.

Архитектура IPTV чаще всего включает [2]:

- промежуточное программное обеспечение;
- систему приема и обработки контента;
- систему защиты контента;
- систему видеосерверов;
- систему мониторинга качества потоков и клиентского оборудования.

Методика обнаружения пиратского контента ТВ-каналов

Для создания методики рассмотрены существующие методы защиты интеллектуальной собственности. Все методы условно можно разделить на две большие группы (рис. 1):

(1) Защита содержимого без возможности отслеживания фактов копирования/изменения [3].

(2) З Защита содержимого с возможностью отслеживания фактов копирования/изменения.

Рис. 1. Систематизация методов защиты интеллектуального права

К первой категории можно отнести: криптографию, цифровые водяные знаки, цифровую подпись, цифровой отпечаток, идентификацию, стеганографию [4]. Ко второй категории можно отнести: системы обнаружения копирования, платежные системы, ключ продукта, защита от несанкционированного доступа [3], DRM (*Digital Rights Management*) [5].

Все перечисленные технологии и методы можно обойти. Так для разработки методики было выбрано самое распространённое нарушение со стороны IPTV провайдера – незаконная трансляция.

Нелицензированный контент-провайдер приобретает доступ к контенту у официального дистрибьютера или контент-провайдера и предоставляет доступ к данному стримингу другим пользователям. При анализе трафика у конечных пользователей можно заметить, что вместо легальных серверов, которым разрешено транслировать данные каналы, появляются серверы нелегальное провайдера.

Для обнаружения пиратского контента ТВ-каналов авторы предлагают следующую методику. Она направлена на выявление незаконного транслирования канала в сфере IPTV. Методику можно разделить на 2 этапа:

1 этап:
- подключение к цифровому каналу;
- перехват трафика;
- проверка серверов трансляции.

2 этап:
- подключение к IPTV;
- перехват трафика во время трансляции;
- проверка серверов трансляции.

Эксперимент

В основе эксперимента лежит незаконная трансляция телеканала. Противозаконность трансляции заключена в свободном доступе к телеканалу, вещание которого на данной территории запрещено.

На рис. 2 представлена схема экспериментального стенда для проверки методики. Для изменения местоположения была использована технология VPN. Для просмотра IPTV был выбран монитор, к которому был присоединена приставка. Подключение к IPTV происходит через приставку. Для перехвата трафика между приставкой и компьютером подключили ноутбук. Анализ трафика осуществлялся при помощи программы Wireshark. При анализе перехваченного трафика обнаружены нелегитимные сервера, используемые для трансляции. При анализе полученных IP-адресов было определено местоположение серверов. В ходе исследования экспериментальным путем была проверена предложенная методика, определены нелицензированные серверы и их местоположение.

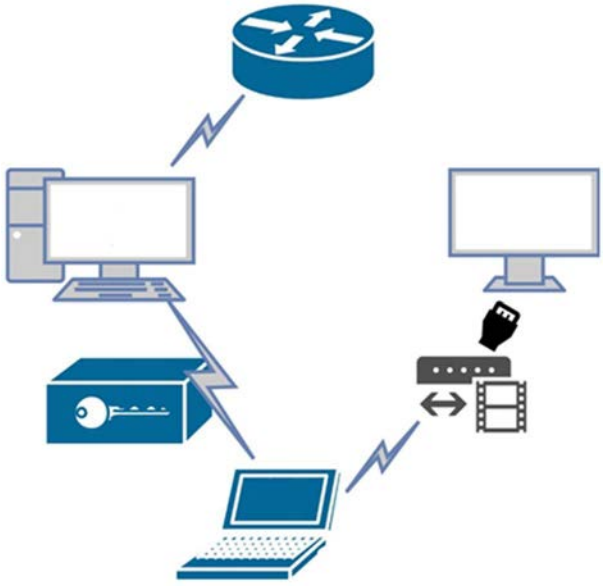


Рис. 2. Схема экспериментального стенда

Заключение

Высокий уровень влияния цифровых технологий на жизнь каждого человека является неоспоримым фактом. Это коснулось и телевидения. Развитие широкополосного доступа в Интернете и скорость передачи данных облегчают доступ к IPTV. Популярность цифрового ТВ приводит к росту нелегальных источников и трансляций. При этом практически отсутствуют методики обнаружения пиратского контента ТВ каналов. В работе проведен

анализ IPTV и предложена методика обнаружения пиратского контента ТВ-каналов.

Список используемых источников

1. Гатчин Ю. А., Николаев Д. Д. Подход к поддержке принятия решения о безопасности облачных сервисов, предоставляющих услугу цифрового телевидения // Вопросы радиоэлектроники. Серия: Техника телевидения. 2015. № 6. С. 80–84.

2. Бундин Д. В., Балашов С. А. Построение индикаторного прибора с динамическим пользовательским интерфейсом // Морской вестник. 2016. № 1S (12). С. 71–72.

3. Виткова Л. А., Рябова О. Н., Сахаров Д. В. Проблемные вопросы создания и использования наборов открытых данных органов государственной власти // Актуальные проблемы инфотелекоммуникаций в науке и образовании. V Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 3-х т. СПб.: СПбГУТ, 2016. С. 271–276.

4. Штеренберг С. И. и др. Комплексный подход к защите электронного документооборота: учебное пособие. СПб., 2016. 93 с.

5. Abu Sirhan, A., Abdrabbo, K.M., Ahmed Ali Al Tawalbeh, S., Hamdi Ahmed, M. and Ali Helalat, M. (2019).

УДК 004.056.53
ГРНТИ 81.93.29

КЛАССИФИКАЦИЯ ИСТОЧНИКОВ УГРОЗ SQL ИНЪЕКЦИЙ

Л. А. Виткова[1,2], **Н. А. Крестьяшин**[1]

[1]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
[2]Санкт-Петербургский Федеральный исследовательский центр Российской академии наук

Сегодня SQL-инъекции по-прежнему остаются актуальной угрозой для безопасности приложений и входят в тройку лидеров угроз информационной безопасности web-приложений. SQL-инъекции позволяют получить злоумышленникам неправомерный доступ к базе данных приложения. Основная причина возникновения угрозы выполнения SQL-инъекции – это отсутствие надлежащей фильтрации данных, полученных от пользовательской формы ввода. В статье предложена классификация SQL-инъекции.

SQL Инъекция, уязвимость, веб-приложение, база данных, информационная безопасность.

Введение

Сегодня SQL-инъекции по-прежнему остаются актуальной угрозой для безопасности приложений. Согласно отчету Top Ten 2021 некоммерческой организации The OWASP Foundation [1], SQL-инъекции входят в тройку лидеров угроз информационной безопасности веб приложений. SQL-инъекции позволяют получить злоумышленникам неправомерный доступ к базе данных приложения. Внедрение вредоносного кода в базу данных может привести к нарушению целостности, конфиденциальности, доступности хранимой информации. В качестве последствий данной атаки для владельца приложения следует назвать финансовые и репутационные потери, а также санкции от регуляторов.

Анализ

Принцип действия sql инъекции

SQL (Structured Query Language) – язык, используемый для работы с реляционными базами данных. SQL-инъекция – угроза информационной безопасности базы данных, возникающая при отсутствии валидации запросов, полученных из пользовательских форм ввода. Для выполнения данной атаки нарушителю необходимо ввести в текстовое поле веб-страницы строку, содержащую SQL команды, которые позволят изменить логику работы запроса [2, 3].

На рисунке 1 изображен пример легитимной авторизации пользователя на веб-сайте. По полученным логину и паролю, формируется SQL запрос к базе данных (БД). БД обрабатывает этот запрос и, в зависимости от корректности данных и установленных прав доступа, предоставляет ответ для клиента.

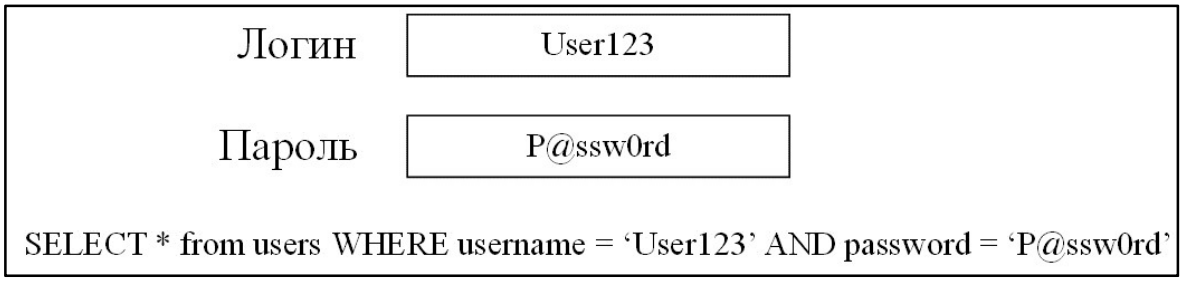


Рис. 1. Пример легитимной авторизации

На рис. 2 изображен способ получения неавторизованного доступа к учетной записи администратора с помощью SQL инъекции. В данном примере атакующий указал в качестве логина идентификатор «admin» и конструкцию вида «'/*». В качестве пароля указана последовательность символов: «*/--». Воспользовавшись вышеуказанными техниками,

злоумышленник модифицировал запрос к серверу. Сформированный атакующим запрос предоставляет в качестве аргумента только имя пользователя, часть запроса с паролем комментируется и игнорируется сервером (закомментированная часть запроса выделена *курсивом*). Таким образом может быть получен доступ к учетной записи администратора без проверки пароля.

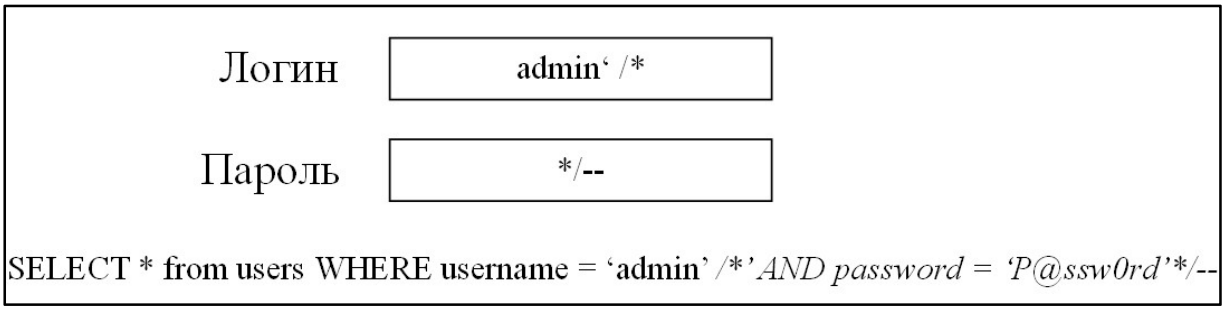


Рис. 2. Пример нелегитимной авторизации

Благодаря этой уязвимости злоумышленник может получить широкие возможности для вредоносных действий:

- просмотр, редактирование, удаление записей или таблиц в БД;
- идентификация используемого ПО, его версии;
- выполнение системных команд операционной системы с правами суперпользователя.

Синтез

Классификация SQL инъекций [2,4,5]

1. Тавтология

Для эксплуатации данной уязвимости необходимо добавить в запрос заведомо истинное выражение, чтобы весь запрос стал истинным (рис. 3). Наиболее распространённая причина использования – обход аутентификации.

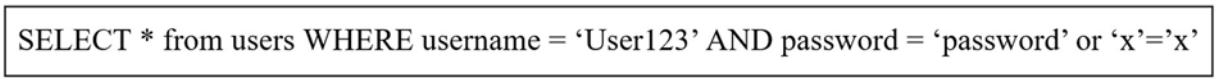


Рис. 3. Тип атаки: «Тавтология».

2. Piggy-backed

В этом типе атаки применяется символ окончания операции для внедрения дополнительного запроса в состав оригинального запроса. Данный вид атаки особо опасен благодаря возможности добавления любой SQL операции (рис. 4).

```
SELECT * from users WHERE username = ‘User123’ AND password = 0; drop tableUsers
```

Рис. 4. Тип атаки: «Piggy-backed».

3. Логически неверный запрос

Преимущество логически неверных запросов (рис. 5) состоит в способности заставить базу данных вернуть сообщение об ошибке. Такие сообщения содержат название СУБД и текущую версию, с помощью этих данных злоумышленник может выполнить поиск по базе данных общеизвестных уязвимостей и в последствии воспользоваться найденной уязвимостью.

```
SELECT * from users WHERE username = ‘User123’ AND password = 0 AND ‘avc’ = 1
```

Рис. 5. Тип атаки: «Логически неверный запрос»

4. Union запрос

В этой атаке, производится вставка дополнительного запроса к уже существующему запросу с помощью команды UNION. В результате злоумышленнику вернется совокупный набор данных, удовлетворяющий оба запроса.

```
SELECT * from users WHERE username = ‘User123’ UNION SELECT * FROM users
WHERE username =’admin’--‘ AND password = ‘12345’;
```

Рис. 6. Тип атаки: «Union инъекция».

5. Альтернативная кодировка

Используя альтернативные кодировки (Unicode, ascii, hex) для создания инъекции, открывается способность обойти созданную разработчиком систему фильтрации запросов. Данный вид атаки представляет особую опасность для безопасности приложения.

```
SELECT * FROM users WHERE username= 'User123' AND password = '12345';
exec(char(0x73687574646j776e)) '
```

Рис. 7. Альтернативная кодировка

Заключение

В рамках данной статьи были рассмотрены причины возникновения угроз SQL-инъекции, предложена классификация атак. Рассмотрены примеры вредоносных запросов. Информация о запросах, которые могут привести к внедрению SQL-инъекцию легко можно получить в Интернете. Используя такие запросы, злоумышленник может получить полный доступ к приложению или к базе данных. В этой статье были рассмотрены классические и современные типы SQL-инъекций. В дальнейшем планируется провести анализ различных существующих методов и инструментов, которые используются для обнаружения или предотвращения этих атак.

Работа выполнена при финансовой поддержке Гранта РНФ № 21-71-20078 в СПб ФИЦ РАН.

Список используемых источников

1. OWASP Top 10:2021. Отчет некоммерческой организации The OWASP Foundation. URL: https://owasp.org/Top10/. (дата обращения: 29.03.2022)

2. Alwan Z. S., Younis M. F. Detection and prevention of SQL injection attack: A survey // International Journal of Computer Science and Mobile Computing. 2017. Т. 6. №. 8. С. 5–17.

3. Alenezi M., Nadeem M., Asif R. SQL injection attacks countermeasures assessments // Indonesian Journal of Electrical Engineering and Computer Science. 2021. Т. 21. №. 2. С. 1121–1131.

4. Thiyab R. M. et al. The impact of SQL injection attacks on the security of databases // Proceedings of the 6th International Conference of Computing & Informatics. 2017. С. 323–331.

5. Abikoye O. C. et al. A novel technique to prevent SQL injection and cross-site scripting attacks using Knuth-Morris-Pratt string match algorithm //EURASIP Journal on Information Security. 2020. Т. 2020. №. 1. С. 1–14.

УДК 004.056.5
ГРНТИ 81.93.29

ПРОБЛЕМАТИКА И ОСОБЕННОСТИ ПРОЦЕДУР АНАЛИТИЧЕСКОЙ ОБРАБОТКИ БОЛЬШИХ МАССИВОВ ГЕТЕРОГЕННЫХ ДАННЫХ О СОБЫТИЯХ КИБЕРБЕЗОПАСНОСТИ В ИНФОКОММУНИКАЦИОННЫХ СЕТЯХ И СИСТЕМАХ

Л. А. Виткова[1,2], И. Б. Паращук[2], И. Б. Саенко[2]

[1]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
[2]Санкт-Петербургский Федеральный исследовательский центр Российской академии наук

Рассмотрены проблематика и ключевые особенности процесса интеллектуальной аналитической обработки больших массивов гетерогенных данных о событиях кибербезопасности сложных систем. Показано, что этот процесс нацелен на выявление связей между событиями кибербезопасности, например, в инфокоммуникационных сетях и системах, а также на установление различных количественных характеристик влияния таких событий или факторов на тот или иной показатель кибербезопасности в интересах оценки состояния, поддержки принятия решений и расследования компьютерных инцидентов в сетях и системах такого класса. Опираясь на результаты анализа проблематики и особенностей, можно сформулировать основополагающие принципы и рекомендации, определяющие научную и, главное, конкретную практическую стороны реализации аналитической обработки данных, которая, в конечном итоге, позволит повысить достоверность контроля защищенности современных инфокоммуникационных сетей и систем.

аналитическая обработка данных, гетерогенные данные, события кибербезопасности, проблема, особенность, инфокоммуникационные сети и системы, компьютерный инцидент.

Рост объемов собираемой информации о событиях кибербезопасности, а также развитие средств и методов их надежного хранения привели к повышению актуальности разработки современных и перспективных методов и алгоритмов анализа больших и сверхбольших наборов данных, поступающих в различном формате и из различных источников, т. е., гетерогенных данных [1].

Анализ больших массивов гетерогенных данных, характеризующих события кибербезопасности, например, в инфокоммуникационных сетях и системах (ИКСС), требует привлечения современных и перспективных технологий и средств реализации высокопроизводительных вычислений. На этом

пути с единых системных позиций необходимо разработать концептуальные основы аналитической обработки (АО) больших массивов гетерогенных данных (БМГД) о событиях кибербезопасности в ИКСС, т. е., по сути, сформулировать проблематику и исследовать особенности решения задач такого класса [2, 3].

Проблематика и особенности процедур АО БМГД о событиях кибербезопасности включают, кроме прочего, понятия, проблемные идеи и возможные принципы и отличительные черты подходов к решению задач такого класса в интересах оценки состояния, поддержки принятия решений и расследования компьютерных инцидентов в ИКСС. Основополагающим и первичным элементом формулировки проблематики считается уточнение особенностей семантики базовых понятий аналитической обработки больших массивов гетерогенных данных о событиях кибербезопасности.

Интеллектуальный анализ БМГД о событиях кибербезопасности – общий термин для обозначения анализа данных такого типа и объема с активным использованием современных интеллектуальных (когнитивных) математических методов и алгоритмов, таких как методы оптимизации, нейросетевые и генетические (биоинспирированные) алгоритмы, методы распознавания образов, статистические методы, методы искусственного интеллекта, и т. д., а также использующих результаты их применения с помощью методов визуального представления данных.

Это совокупность методов обнаружения в данных ранее неизвестных, практически полезных и доступных интерпретации, но нетривиальных знаний, необходимых для принятия решений в сфере кибербезопасности ИКСС.

Проблематика процедур АО БМГД о событиях кибербезопасности содержит вопросы применения технологии обработки таких данных, заключающейся в подготовке суммарной (агрегированной) информации на основе больших массивов данных, например, о структурированных по многомерному принципу событиях кибербезопасности в сложных гетерогенных системах, таких, как ИКСС [4].

К особенностям процедур интеллектуальной АО БМГД о событиях кибербезопасности могут быть отнесены также параметры, характеризующие эти процедуры, в частности: объем, количество генерируемых данных о событиях кибербезопасности (от этого показателя зависит, может ли определенный массив данных о событиях кибербезопасности в ИКСС считаться большими данными или нет); многообразие, категория, к которой принадлежат большие данные о событиях кибербезопасности; скорость генерирования или обработки данных о событиях кибербезопасности с целью осуществления поставленных целей; изменчивость, нестабильность данных о событиях кибербезопасности во времени; достоверность, т. е. качество со-

бранных данных, от которого зависит точность анализа событий кибербезопасности в ИКСС, и, наконец, сложность, трудоемкость процессов расчета, корреляции и построения взаимосвязей между данными о событиях кибербезопасности в ИКСС, включая распределенные параллельные вычисления [5].

Проблематика интеллектуальной АО БМГД о событиях кибербезопасности затрагивает вопросы и взаимосвязанные частные научно-практические задачи сбора, хранения, обработки и анализа информации о таких событиях, а также последующего представления этой информации в удобном для пользователей виде в интересах достоверной и оперативной оценки состояния, поддержки принятия решений и расследования компьютерных инцидентов в ИКСС.

С точки зрения детального анализа особенностей процесса интеллектуальной АО БМГД о событиях кибербезопасности также могут быть интересны частные процедуры, их сущность и очередность реализации для оценки состояния, поддержки принятия решений и расследования компьютерных инцидентов в ИКСС [6].

К таким процедурам относим:

– обнаружение в реальном времени атак на ИКСС на основе имитационного и графо-ориентированного моделирования [7];

– обнаружения в реальном времени аномальной активности и нарушений критериев и политик безопасности ИКСС на основе аналитической обработки больших массивов гетерогенных данных о событиях кибербезопасности;

– оперативная оценка защищенности ресурсов ИКСС на основе аналитической обработки больших массивов гетерогенных данных;

– оперативный анализ и управление рисками информационной безопасности на основе аналитической обработки больших массивов гетерогенных данных о событиях кибербезопасности в ИКСС для оценки состояния, поддержки принятия решений и расследования инцидентов;

– оперативная визуализация больших массивов гетерогенных данных о событиях кибербезопасности в ИКСС для оценки состояния, поддержки принятия решений и расследования инцидентов;

– принятия решений по защите информационных, телекоммуникационных и других критически важных ресурсов ИКСС на основе аналитической обработки больших массивов гетерогенных данных о событиях кибербезопасности;

– проведение расследований компьютерных инцидентов на основе аналитической обработки больших массивов гетерогенных данных о кибербезопасности в ИКСС.

Иными словами, интеллектуальная АО БМГД о событиях кибербезопасности является необходимым современным этапом управления защищенностью ИКСС.

Таким образом, рассмотрены проблематика и ключевые особенности процесса интеллектуальной АО БМГД о событиях кибербезопасности. Этот процесс нацелен на выявление связей между событиями кибербезопасности в ИКСС и установление различных количественных характеристик влияния таких событий или факторов на тот или иной показатель кибербезопасности в интересах оценки состояния, поддержки принятия решений и расследования компьютерных инцидентов в сетях и системах такого класса.

Это позволяет, опираясь на результаты анализа проблематики и особенностей процесса АО БМГД, сформулировать основополагающие принципы и рекомендации, определяющие научную и, главное, конкретную практическую стороны реализации данного процесса. Это, в конечном итоге, позволяет повысить достоверность контроля защищенности современных инфокоммуникационных сетей и систем.

Работа выполнена при финансовой поддержке РНФ (проект 21-71-20078) в СПб ФИЦ РАН (СПИИРАН).

Список используемых источников

1. Полтавцева М. А. Агрегация и нормализация гетерогенных данных в системах мониторинга информационной безопасности и обнаружения вторжений крупномасштабных промышленных КФС // Труды ИСП РАН. 2020. Том 32, Вып. 5. С. 131–142.

2. Радченко И. А, Николаев И. Н. Технологии и инфраструктура Big Data. СПб: Университет ИТМО, 2018. 52 с.

3. Паращук И. Б., Царамов М. В., Сафонов Д. В. Анализ основных требований к процедурам поиска и навигации в больших объемах информации, циркулирующей в региональных телекоммуникационных сетях // Юбилейная XV-я Санкт-Петербургская Международная конференция «Региональная информатика-2016 (РИ-2016)». Материалы конференции. СПб.: СПОИСУ, 2016. С. 114–115.

4. Kotenko I., Doynikova E., Fedorchenko A. Data Analytics for Security Management of Complex Heterogeneous Systems: Event Correlation and Security Assessment Tasks. In: EAI/Springer Innovations in Communication and Computing, 2020. pp. 79–116.

5. Саенко И. Б., Кушнеревич А. Г., Котенко И. В. Реализация платформы распределенных параллельных вычислений для сбора и предварительной обработки больших данных мониторинга в киберфизических системах // Международный конгресс по информатике: Информационные системы и технологии (CSI ST-2016). Материалы международного научного конгресса. Республика Беларусь, Минск, 24-27 октября 2016 г., С. 641–645.

6. Котенко И. В., Саенко И. Б., Браницкий А. А., Паращук И. Б., Гайфулина Д. А. Интеллектуальная система аналитической обработки цифрового сетевого контента для защиты от нежелательной информации // Информатика и автоматизация (Труды СПИИРАН). 2021. Вып. 20 (4). С. 755–792.

7. Десницкий В. А. Подход к обнаружению атак в реальном времени на основе имитационного и графо-ориентированного моделирования // Информатизация и связь. 2021. № 7. С. 30–35.

УДК 004.72, 621.391
ГРНТИ 49.33.29

ТЕСТИРОВАНИЕ ВРЕМЕННЫХ ХАРАКТЕРИСТИК ПРОТОКОЛА СЕТЕВОГО КОДИРОВАНИЯ NCDP

С. С. Владимиров, А. С. Гутовский, А. И. Фомин

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Работа представляет результаты тестирования временных характеристик датаграммного протокола многоадресной передачи с сетевым кодированием NCDP. Разработана структурная схема виртуального лабораторного стенда для тестирования протокола в ненагруженной и нагруженной сетях. Проведено сравнение протокола NCDP с многоадресной передачей без сетевого кодирования и сделаны выводы о применимости протокола NCDP в современных сетях передачи данных.

сетевое кодирование, многоадресная передача, сети TCP/IP, RTT.

Датаграммный протокол многоадресной передачи с сетевым кодированием NCDP (*Network Coding Datagram Protocol*) предложен к разработке 2021 году [1] в рамках исследовательских работ кафедры сетей связи и передачи данных СПбГУТ. Протокол NCDP работает на сеансовом уровне модели OSI поверх датаграммных протоколов транспортного уровня, таких как UDP и DCCP, выполняя функции управления соединением, нумерации пакетов и собственно сетевого кодирования.

Под сетевым кодированием понимается принцип, при котором операции кодирования пакетов данных выполняются и на передающем узле, и на промежуточных маршрутизирующих узлах [2–4]. Как правило, сетевое кодирование пакетов данных представляет собой обратимое линейное преобразование двух или более пакетов данных посредством математических операций, таких как поразрядное сложение по модулю 2 и операции над конечными полями Галуа [3–6]. Основной целью сетевого кодирования является сокращение объема передаваемого по сети трафика для уменьшения задержек передачи данных [3, 5].

Поскольку для современных систем передачи данных одним из самых важных критериев является задержка передачи информации [7, 8], необходимо, чтобы новые протоколы не вносили значимую дополнительную задержку в процесс распространения пакетов по сетям связи.

Для тестирования задержек передачи данных, возникающих при использовании протокола NCDP был реализован виртуальный лабораторный стенд на основе гипервизора VirtualBox компании Oracle и открытой сетевой операционной системы OpenWrt, разворачиваемой на виртуальных машинах. В качестве хост-машины выступила персональная ЭВМ на основе процессора Intel Core i9 10900, обеспечивающего 20 вычислительных потоков с тактовой частотой от 800 до 2 800 MHz, что позволило выделить на каждую виртуальную машину в составе стенда отдельный вычислительный поток. Структура лабораторного стенда представлена на рис. 1.

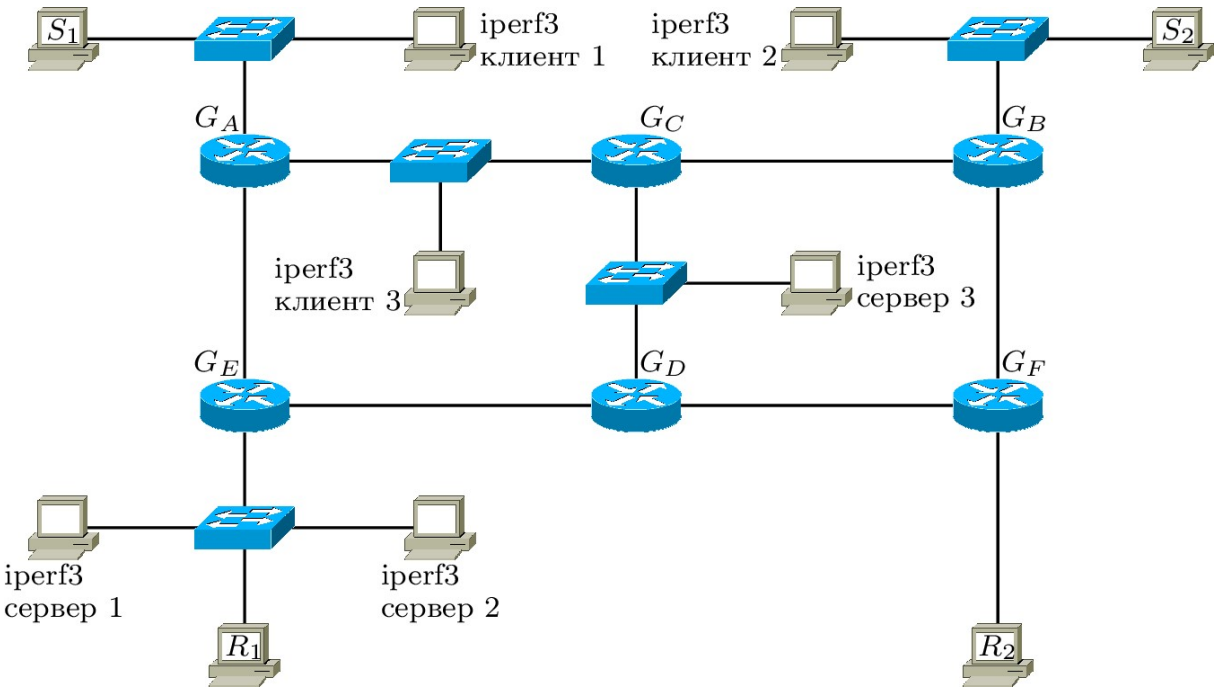


Рис. 1. Виртуальный лабораторный стенд для тестирования протокола NCDP в топологии «бабочка»

Лабораторный стенд моделирует традиционную для систем с сетевым кодированием топологию «бабочка», состоящую из 11 подсетей: семь подсетей связывают между собой маршрутизаторы, две подсети используются для подключения источников информации, две подсети содержат адресатов информации.

Работа протокола тестировалась в ненагруженной сети и в нагруженной сети. Для загрузки сети использован генератор трафика iperf3, клиенты

и серверы которого также показаны на рис. 1. Для нагрузки каналов использовались 10 потоков TCP, полностью загружающих каналы виртуальной сети.

Для оценки задержек протокола было проведено тестирование круговой задержки (*Round-trip time*, RTT) при прохождении пакета от источника до конечного получателя информации и обратно. Поскольку в смоделированной топологии имеется два источника S_1 и S_2 и два получателя информации R_1 и R_2, а структура сети симметрична, то рассмотрены RTT на участках S_1–R_1 и S_2–R_1. Также была проведена оценка времени обработки пакета на основном маршрутизирующем узле G_C, выполняющем операции сетевого кодирования. Для сравнения было проведено моделирование обычной многоадресной передачи при статической маршрутизации пакетов трафика мультивещания. Поскольку тестовое приложение NCDP, выполняющее захват трафика, его обработку и операцию сетевого кодирования на узле G_C работает в пространстве пользователя и априори имеет проигрыш в производительности перед обычной маршрутизацией трафика, выполняемой в пространстве ядра операционной системы, то чтобы сравнять условия работы для исследуемых сценариев, ретрансляция пакетов на узле G_C выполнялась двумя способами. В одном случае пакеты ретранслировались по правилам статической маршрутизации, заданным пакетом smcroute, работающем в пространстве ядра маршрутизаторов, а во втором случае пересылка выполнялась специальным сервером, работающим в пространстве пользователя. Моделирование работы сети производилось для различных тактовых частот процессора хост-машины.

Результаты тестирования RTT представлены на рис. 2. Для загрузки сети при тестировании использовались первые две пары клиент-сервер генератора iperf3.

Из диаграмм на рис. 2 видно, что средние значения RTT при различных способах передачи отличаются незначительно. Разница присутствует во второй–третьей значащей цифре и по величине меньше, чем разброс значений RTT от пакета к пакету. Таким образом, можно считать, что использование протокола NCDP не приводит к увеличению времени передачи пакета.

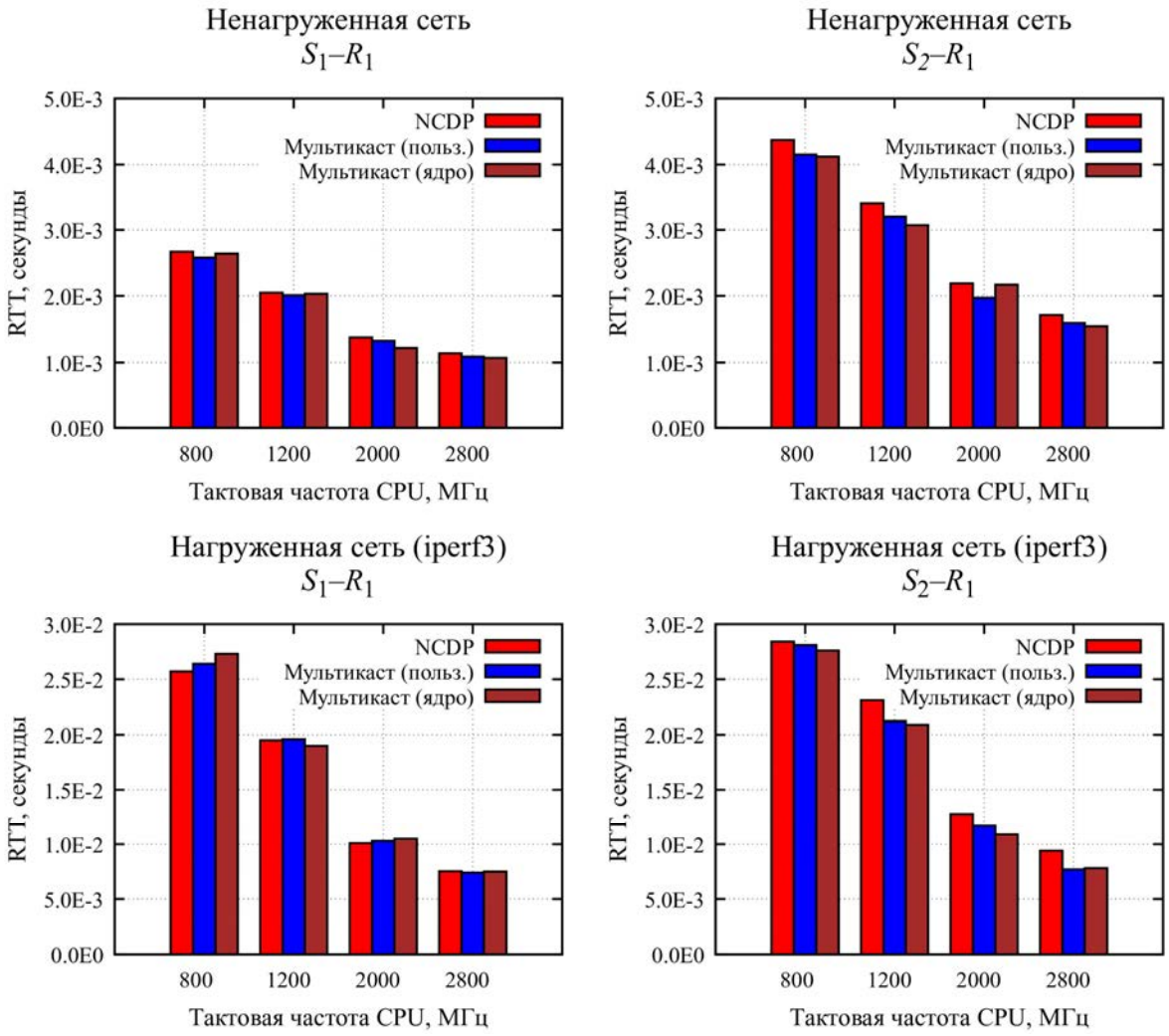


Рис. 2. RTT при прохождении пакета
от источника до конечного получателя информации

Среднее время обработки пакета на маршрутизирующем узле G_C представлено на рис. 3. Для загрузки сети при тестировании использовалась третья пара клиент-сервер генератора iperf3. Можно видеть, что время обработки пакета приблизительно одинаково для сетевого кодирования и ретрансляции пакетов, выполняемыми программой в пространстве пользователя. При этом сетевое кодирование выполняется в среднем незначительно быстрее. Представленный для сравнения вариант маршрутизации пакетов в пространстве ядра имеет значительно более высокое быстродействие из-за более высоких приоритетов процесса. В нагруженной сети из-за низких приоритетов время выполнения операций ретрансляции и кодирования в пространстве пользователя увеличено в сравнении с передачей по незагруженной сети, тогда как маршрутизация. на уровне ядра работает приблизительно с той же скоростью.

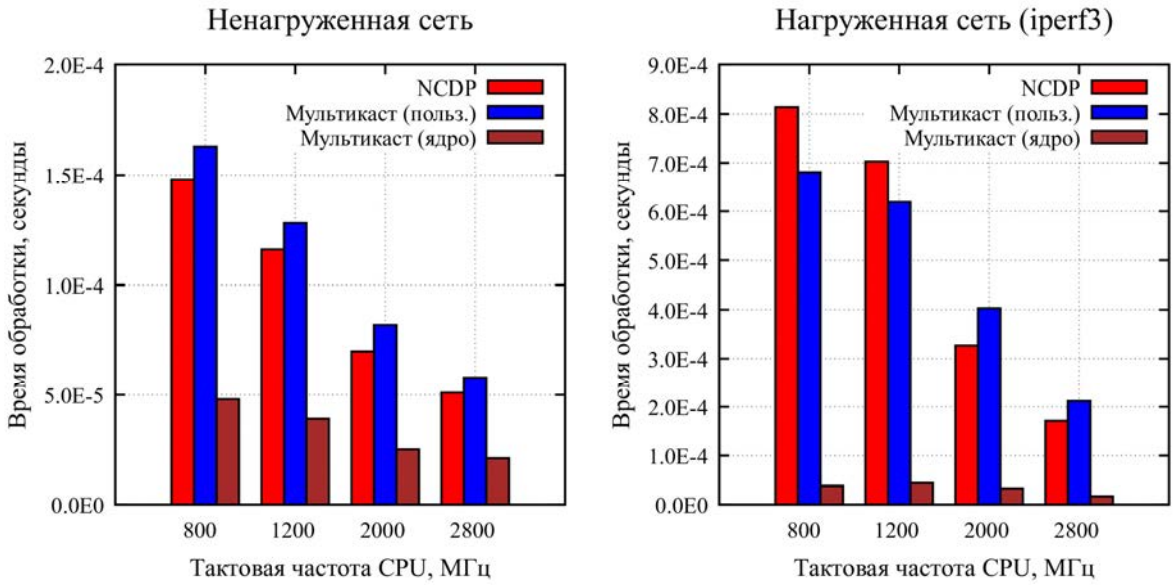


Рис. 3. Время обработки пакета на узле G_C

Следует отметить, что время обработки пакета на маршрутизирующем узле G_C на один–два порядка меньше RTT и, соответственно, не оказывает значительного влияния на время передачи пакета. Величина времени обработки в среднем меньше, чем разброс значений RTT от пакета к пакету.

Проведенное исследование показало, что использование протокола сетевого кодирования NCDP не приводит к значимому увеличению задержки прохождения пакетов, что позволяет применять протокол NCDP в современных сетях передачи данных.

Список используемых источников

1. Владимиров С. С., Фомин А. И. Концепция протокола многоадресной передачи на основе метода сетевого кодирования // Информационные технологии и телекоммуникации. 2021. Т. 9. № 1. С. 26–36.

2. Adamson B. RFC 8406 Taxonomy of Coding Techniques for Efficient Network Communications. IRTF, 2018. URL: https://www.rfc-editor.org/rfc/rfc8406.html (дата обращения: 20.01.2022).

3. Ahlswede R., Cai N., Li S.R., Yeung R.W. Network information flow // IEEE Transactions on Information Theory. 2000. Vol. 46. Iss. 4. P. 1204–1216.

4. Fragouli C., Soljanin E. Network Coding Fundamentals // Foundations and Trends in Networking. 2007. Vol. 2. Iss. 1. P. 1–133.

5. Li S.-Y.R., Yeung R.W., Cai N. Linear network coding // IEEE Transactions on Information Theory. 2003. Vol. 49. Iss. 2. P. 371–381.

6. Sun Q., Yin X., Li Z., Long K. Multicast network coding and field sizes // 2014 IEEE International Symposium on Information Theory. Honolulu, HI, USA: IEEE, 2014. P. 2157–2161.

7. Кучерявый А. Е. Сети связи с ультра малыми задержками // Труды научно-исследовательского института радио. 2019. № 1. С. 69–74.

8. Кучерявый А. Е., Киричек Р. В., Маколкина М. А., Парамонов А. И., Дунайцев Р. А., Пирмагомедов Р. Я., Бородин А. С., Владыко А. Г., Мутханна А. С. А., Выборнова А. И., Владимиров С. С., Гришин И. В. Новые перспективы научных исследований в области сетей связи на 2021–2024 годы // Информационные технологии и телекоммуникации. 2020. Том 8. № 3. С. 1–19.

УДК 621.391
ГРНТИ 49.33.29

ПРИМЕНЕНИЕ ТЕХНОЛОГИЙ ТУМАННЫХ ВЫЧИСЛЕНИЙ ДЛЯ ОБРАБОТКИ ТРАФИКА В СЕТЯХ С КЛАСТЕРАМИ БПЛА И МНОГОУРОВНЕВОЙ ОБЛАЧНОЙ АРХИТЕКТУРОЙ MEC

А. Н. Волков, В. Н. Коваленко, А. С. А. Мутханна

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В данной работе мы предлагаем организовать сетевую архитектуру с использованием кластеров БПЛА на нижнем уровне и трехуровневую облачную системы MEC на верхних. Также в данной работе предлагается использовать технологию туманных вычислений на уровне кластеров БПЛА для обработки трафика от устройств пользователей. В рамках данной работы также определяются критерии для выбора уровня обработки и подсчета суммарных ресурсов каждого БПЛА для последующего формирования кластера Fog, который будет сформирован для обработки трафика. В статье описан алгоритм для формирования кластеров Fog, а также определены устройства, которые будут ответственны как за формирование кластера Fog, так и за выбор уровня обработки.

БПЛА, кластер, головной узел, MEC, Микро-облако, Мини-облако, Главное облако, Fog.

Введение

В 1999 году в презентации Кевина Эштона для Procter&Gamble, посвященной влиянию RFID-технологий на разные рынки, возможно впервые был употреблен термин «Интернет Вещей». С тех пор количество устройств с доступом к сети интернет постоянно увеличивалось [1]. Увеличение количества устройств Интернета Вещей способствовало появлению сетей сверхвысокой плотности, в рамках концепции которой предполагается, что плотность размещения устройств на 1 км^2 в городской местности будет достигать 1 млн. В то же время вместе с увеличением количества устройств интернета вещей растут и объемы генерируемого трафика. Еще одна проблема связана с тем, что с развитие сетей связи возникают новые технологии

с более высокими требованиями к качествам обслуживания. Так, например, для таких направлений, как беспилотный автотранспорт и тактильный интернет, необходимо обеспечение сверхнизких значений задержек порядка 1 мс. Развернутые на данный момент времени ЦОД не были рассчитаны на работу в сетях с плотностью размещения устройств равной 1 мл [2]. В то же время из-за больших задержек передачи данных до сервера (чаще всего размещаемого в базовой сети), ЦОД не может осуществить реализацию услуг в рамках концепции тактильного интернета и в сетях беспилотного автотранспорта. При поиске решения проблем обработки больших объемов трафика и обеспечения сверхнизких задержек необходимо также учитывать возможность изменения объемов генерируемого трафика в течение дня. Например, утром объемы генерируемого трафика могут быть выше на окраине города, а днем – в центре города и в промышленных районах.

Поэтому в данной работе для решения проблем, связанных с обработкой больших объемов данных и обеспечении сверхнизких значений задержки передачи в условиях непостоянности объемов генерируемого трафика предлагается организовать сетевую архитектуру с использованием кластеров БПЛА на нижнем уровне и трехуровневую облачную системы MEC на верхних. Также в данной работе предлагается использовать технологию туманных вычислений на уровне кластеров БПЛА для обработки трафика от устройств пользователей [3].

Многоуровневая облачная архитектура MEC

В основе технологии Multi-access Edge Computing (граничных вычислений множественного доступа MEC), ранее называемой Mobile Edge Computing (мобильные граничные вычисления), лежит использование возможностей облачных вычислений в сотовой сети на границе с сетью радиодоступа [3, 4]. В рамках данной концепции применяется три вида вычислительных облаков (вычислительные облака представлены в порядке возрастания их вычислительных и запоминающих ресурсов): Микро-облако (*Micro cloud*), Мини-облако (*Mini cloud*), Главное облако (*Main cloud*).

Предлагаемая архитектура

В данной статье рассматривается архитектура сетей БПЛА с организацией кластеров в летающем сегменте [4, 5]. В такой архитектуре взаимодействие БПЛА в пределах одного кластера и БПЛА одного кластера с устройствами вне кластера (БПЛА другого кластера, базовые станции, удаленный сервер), осуществляется через головной узел.

Предлагаемая нами архитектура будет состоять из четырех уровней: самый нижний – уровень кластеров БПЛА, 2–4 уровни многоуровневой облачной системы MEC [3]

В работе предлагается использовать БПЛА в качестве Fog устройств для формирования кластера Fog (который, в последствии, как и облака более высоких уровней будет применяться для обработки трафика пользователей). Таким образом предлагается реализовать технологию туманных вычислений на первом уровне предлагаемой архитектуры. Второй уровень – уровень Микро-облака, соединенного с базовыми станциями. Данное вычислительное облако, из-за наиболее близкого расположения относительно БПЛА (по сравнению с другими вычислительными облаками) в нашей архитектуре предлагается использовать для выполнения роли Fog сервера, ответственного за формирование кластера Fog. Третий уровень – уровень Мини-облака, соединенного с контроллером базовых станций. В нашей работе предлагается использовать Мини-облако для выбора уровня обработки. Также предполагается, что подчиняемые микро-облака, головные узлы каждого кластера и главное облако будут передавать через определенные промежутки времени информацию о свободных ресурсах своего уровня. Четвертый уровень – главное облако или удаленный сервер.

Подсчет суммарных свободных ресурсов БПЛА и вычислительных облаков

В качестве основных критериев вычисления суммарных доступных ресурсов одного БПЛА предлагается рассматривать CPU, оперативную (RAM) и постоянную (ROM) память устройства, пропускную способность, а также заряд батареи. Для каждого БПЛА по CPU, оперативной и постоянной памяти, пропускной способности при подсчете доступных ресурсов будут рассматриваться не максимально возможные показатели, а количество ресурсов, которые на данный момент свободны и могут быть использованы для обработки запроса пользователя.

В качестве критериев для подсчета суммарных ресурсов вычислительных облаков (Микро-облака, Мини-облака и Главного облака или Сервера) предлагается использовать CPU, RAM, ROM и пропускную способность (так как предполагается, вычислительные облака будут обладать постоянным электропитанием, то параметр заряда батареи в данном случае не используется).

Последовательность действий при осуществлении обработки запросов пользователя на уровне кластеров БПЛА

Для формирования кластера Fog головной узел должен также периодически запрашивать информацию о суммарных ресурсах БПЛА своего кластера. В данной работе предлагается объединить запрос информации о суммарных ресурсах всех БПЛА в кластере и их передачу на Мини-облако в один периодически повторяющийся процесс со следующей последовательностью действий:

1. Головной узел отправляет запрос на получение данных о свободных ресурсах каждому БПЛА кластера

2. БПЛА передают информацию о своих свободных ресурсах головному узлу.

3. Головной узел после получения от БПЛА информации о свободных ресурсах отправляет в обратном направлении подтверждение приема данных или запрос на их повторную передачу.

4. Передача данных о свободных ресурсах БПЛА одного кластера от головного узла до Микро-облака. В работе предлагается осуществлять передачу информации о свободных ресурсах всех БПЛА кластера одновременно (данные о свободных ресурсах будут собираться головным узлом кластера БПЛА).

5. Полученные данные Микро-облаком заносятся в таблицу о свободных ресурсах БПЛА. Так как кластер Fog формируется только из БПЛА одного кластера, то для каждого кластера БПЛА предлагается организовывать собственную таблицу свободных ресурсов.

6. Для каждого БПЛА вычисляется суммарное количество ресурсов. Далее все БПЛА в таблице сортируются в порядке убывания суммарных ресурсов.

7. Полученная таблица свободных ресурсов передается Мини-облаку.

Рис. 1. Схема передачи данных о свободных ресурсах кластера БПЛА

Если в качестве уровня обработки данных будет выбран уровень кластера БПЛА, то последовательность действий при формировании кластеров Fog и обработке пользовательского трафика будет следующей:

1. На головной узел от Мини-облака поступает запрос на формирование кластера Fog, а также затрачиваемые на выполнение запроса пользователя ресурсы

2. Из затрачиваемых ресурсов вычитаются суммарные свободные ресурсы БПЛА в порядке их уменьшения, а сами БПЛА присваиваются к формируемому подкластеру Fog. Данный процесс повторяется пока разность между затрачиваемыми ресурсами и общими суммарными ресурсами формируемого кластера Fog не будет меньше нуля.

3. Формирование кластера Fog и отправка Мини-облаку ответа об успешном формировании подкластера. Если подкластер Fog не был сформирован, то Микро-облако передает ответ Мини-облаку о невозможности формирования подкластера Fog. Для подтверждения формирования кластера Fog каждый БПЛА предполагаемого кластера должен передать через головной узел на Микро-облако согласие на обработку запроса пользователя. Ответ о невозможности формирования кластера Fog будет отправлен, только если хотя бы один из БПЛА предполагаемого кластера отправит информацию с отказом обработки запроса пользователя.

4. После успешного формирования подкластера Fog и получения Мини-облаком подтверждения данному подкластеру будет передан запрос пользователя.

5. Осуществляется обработка пользовательского запроса.

Стоит также отметить, что для более эффективного использование свободных ресурсов один БПЛА предлагается применять при формировании нескольких кластеров Fog.

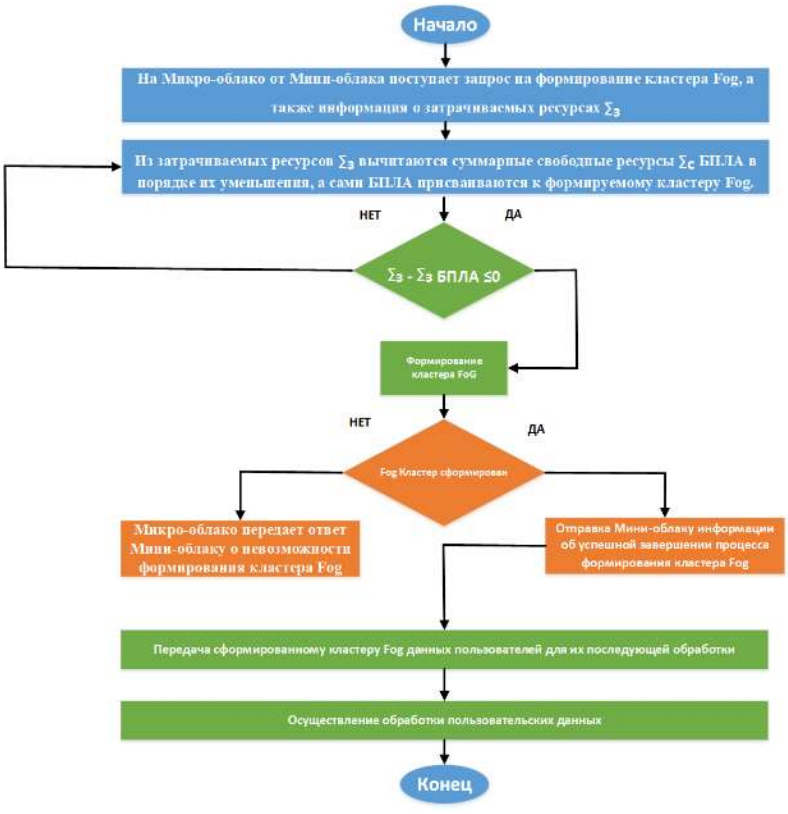


Рис. 2. Последовательность действий при обработке запросов на уровне кластеров БПЛА

Выводы

В данной статье была предложена сетевая архитектура, состоящая из 4 уровней. Первый уровень предлагалось организовать из кластеров БПЛА, а уровни со 2 по 4 многоуровневой облачной системой МЕС. В статье предлагается осуществлять формирование кластера Fog из устройств первого уровня. Также в статье представлена последовательность действий при осуществлении обработки запросов пользователя на уровне кластеров БПЛА и по формировании таблицы свободных ресурсов кластера БПЛА. В статье представлены критерии для подсчета суммарных ресурсов БПЛА, Микро-облака, Мини-облака и Главного облака.

Исследование выполнено в рамках выполнения ПНИ по государственному заданию СПбГУТ на 2021 год.

Список используемых источников

1. Nikolayevich V., Alzaghir A., Volkov A., Muthanna A., Koucheryavy A. Clustering algorithms for UAV placement in 5G and Beyond Networks // 2020 12th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT).

2. Коваленко В. Н., Волков А. Н., Мутханна А. С. А, Способ снижения круговой задержки и нагрузки в сети при взаимодействии соседних вычислительных облаков многоуровневой облачной архитектуры // 74-я Научно-техническая конференция Санкт-Петербургского НТО РЭС им. А.С. Попова, посвященная Дню радио. 2019. 435 с.

3. Волков А. Н., Коваленко В. Н., Мутханна А. С. А., Родакова А. О., Система распределенных вычислений на основе летающего сегмента сети, глубоко имплементированного в архитектуру сетей связи 5g/imt-2020 и сетей 2030 // Актуальные проблемы инфотелекоммуникаций в науке и образовании. X Юбилейная Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2021. Т. 4. С. 403–408.

4. Коваленко В. Н., Березин В. А., Мутханна А. С. А Система для сетей VANET на основе SDN/MEC // 73-я региональная научно-техническая Конференция студентов, аспирантов и молодых ученых «Студенческая весна – 2019». 2019. Т. 1. С. 57–61

5. Коваленко В. Н., Алзагир А. А., Мутханна А. С. А. Построение сети БПЛА с поддержкой SDN/NFV технологий // Информационные технологии и телекоммуникации. 2020. Том 8. № 3. С. 71–85.

УДК 004.451
ГРНТИ 81.96

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ПРОГРАММНЫХ СИСТЕМ ХРАНЕНИЯ ДАННЫХ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

В. Н. Волкогонов, В. А. Гапоненко, А. И. Катасонов

Санкт-Петербургскийгосударственныйуниверситеттелекоммуникацийим. проф. М. А. Бонч-Бруевича

В каждой IT кампании, которая заботится о сохранности своих данных возникает необходимость использования систем хранения данных. В данном исследовании проведен сравнительный анализ программных систем хранения данных и анализ рынка предложений. Рассмотрены предложения наиболее распространенных кампаний в области применения программных систем хранения данных. Основным критерием сравнения данного анализа является количество возможных функций, необходимых для решения бизнес задач.

система хранения данных, SDS, администрирование, IT.

Перед каждым развивающимся проектом рано или поздно встает необходимость выбора подходящей системы для хранения данных. Любая такая система должна обеспечивать резервирование, которое может гарантировать сохранность информации при возникновении разного рода сбоев.

В первую очередь, при выборе хранилища, компании учитывают параметры производительности и стоимости, при этом часто забывая о надежности, масштабируемости и времени восстановления после сбоя. Зачастую, это ведет к тому, что, в процессе эксплуатации, все неучтенные факторы начинают проявляться и выходить на первый план.

Область системной интеграции все больше развивается в направлении виртуализации аппаратных ресурсов. Эта тенденция изменила принципы организации систем хранения данных. Появились программно-определяемые СХД (SDS, Software-defined storage), которые представляют собой специальное программное обеспечение, позволяющее построить автоматизированную IT-экосистему, не привязанную к используемому оборудованию [1].

Преимущества [2]:

- Производительность. Программно-определяемые хранилища имеют поддержку карт PCIe NVMe, благодаря которым, у системы повышается производительность операций ввода-вывода и уменьшается задержка.
- Отказоустойчивость. В случае сбоя SDS, с помощью инструментов репликации данные легко резервируются, таким образом, работа предприятия не останавливается.

• Гибкость. SDS может разворачиваться на разных оборудованиях одного или нескольких производителей. Полученная СХД легко масштабируется, а администраторы могут централизованно управлять её ресурсами.

• Экономичность. Программно-определяемое хранилище позволяет использовать стандартизированное оборудование как альтернативу проприетарному, что значительно снижает стоимость владения IT-инфраструктурой. Вместо одной или нескольких СХД задействовано лишь дисковое пространство серверов.

• Удобство администрирования. Управление программно-определяемой СХД ведется при помощи только лишь консоли.

Основной принцип работы программно-определяемой СХД – отказ от физического оборудования и комплексный перенос организации хранения данных на программный уровень. В этом и есть принципиальное отличие SDS от традиционно используемых блочных хранилищ. При таком подходе организация может дать программно-определяемым хранилищам тот набор свойств и характеристик, который подходит под специфику поставленных бизнес-задач [3].

Для создания SDS обычно используются сервера с процессорами на архитектуре x86. Специализированное программное обеспечение позволяет объединять их в высокопроизводительную систему, работающую как единое дисковое пространство с некоторыми характеристиками. Для обеспечения сохранности данных обычно используют RAID-контроллеры, а также технологию зеркалирования – благодаря этому, СХД может продолжать работу в штатном режиме, даже при выходе из строя части аппаратных компонентов. Также имеет место территориального распределения серверов, благодаря которому исключается повреждение файлов (при повреждении сервера в одном здании, система продолжит работу, используя ресурсы из другого помещения) [4].

Сама концепция программной СХД позволяет нам получать значительные преимущества перед аппаратными системами:

– абстрагирование от нижнего уровня модели OSI (аппаратных платформ);

– упрощенная инфраструктура хранения данных;

– масштабируемость;

– сравнительно низкая стоимость решений.

Storage Networking Industry Association (SNIA, Ассоциация производителей и потребителей систем хранения) определяет SDS как виртуализированную среду хранения данных с интерфейсом управления сервисами, которая должна включать в себя [5]:

• Автоматизацию, снижающую издержки на обслуживание инфраструктуры данных, упрощённое управление;

- API для управления, выделения и освобождения ресурсов, обслуживания устройств и сервисов хранения, путем использования стандартных интерфейсов;
- Возможность изменения инфраструктуры хранения без снижения необходимого уровня производительности и доступности;
- Виртуализация путей доступа к данным – объектный, блочный и файловый доступ, соответствующий интерфейсам приложений;
- Мониторинг потребляемых ресурсов хранения, управление ими и контроль их стоимости.

Некоторые производители предлагают также и программную часть, помимо комплексных решений (Huawei, Dell EMC). [6] Благодаря этому, можно более тщательно подходить к выбору продуктов, и использовать унаследованное вычислительное оборудование для менее ресурсоемких задач хранения данных. Также, SDS позволяет применять виртуализацию в некоторых классических СХД [7].

Существует два принципа построения архитектуры решений:

- Слабо связанные;
- Распределённые (без общих элементов).

При слабо связанном построении отказоустойчивость обеспечивается распределением копий данных, но из-за большого количества потока данных между узлами (нодами) скорость записи снижается. Критичным местом является сеть передачи данных, поэтому такие решения обычно реализованы на основе InfiniBand. По такому принципу построены решения VMware vSAN, HPE StoreVirtual, VSA, Dell EMC ScaleIO.

В системах без общих элементов данные записываются на один узел, и в последствии, с заданной периодичностью копируются на другие для обеспечения отказоустойчивости. При этом записи не являются транзакционными. Такой подход наиболее дешевый и удобный с точки зрения масштабируемости. Яркий ее представитель – CEPH. [8]

На данный момент большое количество компаний занимаются разработкой как программной SDS (Atlantis Computing, Maxta, StarWind, DataCore Software, Sanbolic, Nexenta, CloudByte), так и выпуском комплексных решений (Dell EMC, IBM) или специализированных устройств (Tintri, Nimble, Solidfire).

Для сравнения были выбраны семь решений, наиболее известных на рынке и результаты сравнительного анализа собраны в таблице.

В предлагаемой таблице сравниваются лишь возможности решений, и не сравниваются производительность, скорость репликации, время переключения нод и др. т. е. это именно сравнительный анализ возможностей, а не продуктивное тестирование.

ТАБЛИЦА. Сравнительная таблица основных характеристик программных СХД

	VMware vSAN	HPE StoreVirtual VSA	NetAPP Data ONTAP Select	EMC ScalelO	Huawei Fusion Storage	StarWind Virtual SAN	Datastore SANsymphony
Поддерживаемые гипервизоры	ESXi	ESXi, Hyper-V, KVM	ESXi	ESXi, Hyper-V, KVM, Xen	SXi, Hyper-V, KVM, Xen, FusionCompute	ESXi, Hyper-V, KVM, Xen	ESXi, Hyper-V, KVM, XEN и др.
Удаленная асинхронная репликация	Да, через vSphere Replication PRO	Да, несколько площадок, RPO	Да	Да	Нет	Да	Да
Поддержка снэпшотов	Да	Да	Да	Да	Да	Да	Да
Работа со снэпшотами	Чтение/ Запись	Чтение/ Запись	Чтение/ Запись	Чтение/ Запись	Нет	Чтение/ Запись	Чтение/ Запись
Шифрование данных	Да. На уровне Vsphere, SED диски RPQ, на уровне vSAN	Нет	Нет	Да	Есть	Нет	Шифрование осуществляется при файловом доступе и асинхронной репликации
Дедупликация	Только на ALL Flash (4K, nearline)	Нет	Да	Нет	Только для объектного доступа	Да	Да
Сжатие	Только на ALL Flash (4K, nearline)	Нет	Да	Нет	Нет	Нет	Да
Flash-Cache	Да, обязательное требование	Да, на RAID-контроллере	Да	Да	Да	Да	Да
Tiering	Нет	Да	Нет	Нет	Да	Нет	Да
VAAI (vStorage API for Array integration)	Нет (альтернативные механизмы)	Да	Да	Да	Да	Да	Да
VASA (vStorage APIs for Storage Awareness)	Да	Да	Да	Да	Нет	Да	Да
VVOL (vSphere Virtual Volumes)	Нет	Нет	Да	Нет	Нет	Да	Да
Автоматическая балансировка нагрузки между узлами	Да	Да, все узлы Active-Active, Multi-Pathing	Нет	Нет	Да	Да	Да
QoS (Quality of Service)	Да	Да	Нет	Да	Да	Да	Да
Файловый доступ	Нет	Нет	CIFS, NFS	NFS	NFS, CIFS, FTP, HDFS	SMB3, NFS	SMB3, NFS, CIFS

	VMware vSAN	HPE StoreVirtual VSA	NetAPP Data ONTAP Select	EMC ScalelO	Huawei Fusion Storage	StarWind Virtual SAN	Datastore SANsymphony
Схема лицензирования	За CPU на сервере, или конкурентные подключения (для VDI) или по ВМ	За узел. Ограничение по объему на узел	За узел	По объему сырого пространства	По объему сырого пространства	По объему/узлам	За узел + ТВ полезной емкости

По результатам сравнительного анализа были выявлены возможности наиболее распространенных на рынке систем хранения данных, из которых видно, что ни один из вендоров не предоставляет комплексного решения, которое бы могло обеспечить решение всех необходимых для бизнеса задач.

Список используемых источников

1. Пестов И. Е., Сахаров Д.В., Сергеева И.Ю., Чернбородов И.С. Выявление угроз безопасности информационных систем // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VI Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2017. Т. 2. С. 525–527.

2. Пестов И. Е., Шинкарева П. С., Кошелева С. А., Бурмистров М. Д. Разработка программно-аппаратной системы контроля и управления доступом // Эргодизайн. 2020. № 1 (7). С. 19–24.

3. Леснова Е. М., Пестов И. Е. Разработка метода обнаружения и коррекции ошибок для распределенной информационной сети на основе больших данных // Материалы XVI Санкт-Петербургской международной конференции "Региональная информатика "РИ-2018" (Санкт-Петербург, 24–26 октября 2018 г.). СПб., 2018. С. 570–571.

4. Москальчук А. И. Практическое исследование методологии тестирования на проникновение в виртуальной среде // Молодежная научная школа кафедры "Защищенные системы связи". 2020. Т. 1. № 1 (1). С. 47–54.

5. Гельфанд А. М., Лансере Н. Н., Ложкина А. А., Фадеев И. И. Организация концептуальной модели критической информационной инфраструктуры // Методы и технические средства обеспечения безопасности информации. 2020. № 29. С. 39–40.

6. Сахаров Д. В., Гельфанд А. М., Казанцев А. А., Пестов И. Е. Использование математических методов прогнозирования для оценки нагрузки на вычислительную мощность IOT-сети // Вестник Санкт-Петербургского университета Государственной противопожарной службы МЧС России. 2020. № 2. С. 86–94.

7. Котенко И. В., Коломеец М. В., Бушуев С. Н., Гельфанд А. М. Методы человеко-машинного взаимодействия на основе сенсорных экранов в ситуационных центрах безопасности // В сборнике: Информационные технологии в управлении (ИТУ-2018). материалы конференции. 2018. С. 554–558.

8. Sharikov P. I., Krasov A. V., Gelfand A. M., Kosov N. A. Research of the possibility of hidden embedding of a digital watermark using practical methods of channel steganography // Studies in Computational Intelligence. 2020. № 868. С. 203.

Статья представлена заведующим кафедрой ЗСС СПбГУТ, кандидатом технических наук, доцентом А. В. Красовым.

УДК 004.056.52
ГРНТИ 81.93.29

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ

В. А. Волостных[1], **П. А. Кононов**[2], **О. А. Остроумов**[1]

[1] Военная орденов Жукова и Ленина Краснознаменная академия связи имени Маршала Советского Союза С. М. Буденного

[2]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье рассматриваются проблемы обеспечения безопасности критической информационной инфраструктуры образовательных организаций, мероприятия по обеспечению безопасности информационно-телекоммуникационных систем, отнесенных к значимым объектам и пути их реализации. Авторы предлагают подходы к категорированию объектов информационной инфраструктуры и обозначают проблемы, связанные с обеспечением безопасности информационных систем образовательных организаций. Статья может быть полезна специалистам подразделений информационной безопасности и студентам вузов связи.

безопасность критической информационной инфраструктуры, государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак, защита информационных систем, значимый объект критической информационной инфраструктуры, категорирование автоматизированных и информационных систем, компьютерные атаки, электронный документооборот, средства защиты информации, критическая информационная инфраструктура.

Всем известно, что от эффективности деятельности образовательных организаций зависят темпы развития экономики, уровень благосостояния населения. Под эффективностью образовательной деятельности в статье понимается качество образования, которое получают выпускники образовательных организаций.Согласно законодательству Российской Федерации об образовании обучение специалистов осуществляют профессиональные образовательные организации, образовательные организации высшего образования, организации дополнительного образования [1]. Из приведенного перечня организаций рассмотрим функционирование образовательных организаций высшего образования (ООВО), поскольку в этих организациях функционируют наиболее сложные информационные и автоматизированные системы. Очевидно, что эффективность ООВО во многом зависит от наличия и уровня квалификации профессорско-преподавательского состава, от системы управления образовательным процессом, от системы обеспече-

ния образовательного процесса. Следовательно, существенную роль в эффективности образовательного процесса играет качество и безопасность функционирования автоматизированных и информационных систем (АИС) организации.

Информационная система ООВО представляет собой совокупность информационных подсистем, предназначенных для управления деятельностью организации, ведения обучения, воспитания и осуществления научной работы по определенному профилю.

Для управления деятельностью ООВО, как правило создаются системы электронного документооборота, которые представляют собой совокупность автоматизированных рабочих мест (АРМ) должностных лиц организации, соединенных линиями коммуникации и серверного оборудования. В систему электронного документооборота включаются АРМы следующих должностных лиц: ректора, проректоров и их помощников, деканов факультетов, заведующих кафедрами, руководителей департаментов, управлений и отделов, в том числе административно-кадровых, финансовых, хозяйственных, служб пропускного режима и др. Общее количество АРМов может составлять 50–150 единиц, в зависимости от назначения ООВО и степени ее оснащенности.

Для ведения процесса обучения учебные аудитории, лаборатории оснащаются средствами вычислительной и демонстрационной техники, которые в большинстве своем объединяются телекоммуникационным оборудованием с подключением к единому серверу ООВО. Общее количество АРМ может составлять 100–1 000 комплектов.

Для проведения научных исследований могут создаваться специализированные лаборатории в состав которых могут входить средства вычислительной техники повышенной производительности с программным обеспечением, позволяющим проводить исследования в заданной научной сфере. Общее число таких комплексов может быть от единиц до нескольких десятков. В ряде случаев для проведения научных исследований могут создаваться автоматизированные системы управления.

Как показывает практика перечисленные информационные подсистемы подключаются к общему серверу, имеющему подключение к глобальной сети общего пользования «Интернет» и являются уязвимыми от воздействия компьютерных атак (КА). Кроме того, сети общего пользования используются для объединения информационных и автоматизированных подсистем, функционирующих на различных территориях, размещающихся на значительном удалении друг от друга и, следовательно, также подвержены деструктивному воздействию от КА отдельных лиц и организаций. В связи с известными событиями последних лет в деятельности многих образовательных организаций произошли существенные перемены, связанные с внедрением методов и систем дистанционного образования

и внедрением информационных систем, позволяющих ряду работников работать удаленно. Безусловно, что подсистема удаленной работы должностных лиц ООВО и подсистема дистанционного образования также могут подвергаться воздействию КА.

Как отмечается в Стратегии национальной безопасности Российской Федерации [2] в настоящее время увеличивается количество компьютерных атак на российские информационные ресурсы. Большая часть таких атак осуществляется с территорий иностранных государств. Инициативы Российской Федерации в области обеспечения международной информационной безопасности встречают противодействие со стороны иностранных государств, стремящихся доминировать в глобальном информационном пространстве.

Очевидно, что компьютерные атаки на информационную систему ООВО могут существенно снизить эффективность образовательного процесса или на какое-то время его остановить.

В 2017 году был принят Федеральный закон от «О безопасности критической информационной инфраструктуры Российской Федерации» [3], регулирующий отношения в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации в целях ее устойчивого функционирования при проведении в отношении ее компьютерных атак. Объекты критической информационной инфраструктуры имеют важное значение для различных сфер жизни общества [4–6]. В соответствии с законом в Российской Федерации создается государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГОССОПКА) на информационные ресурсы Российской Федерации, которая представляет собой единый территориально распределенный комплекс, включающий силы и средства, предназначенные для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты [7, 8].

Возникает вопрос, а относятся ли информационные и автоматизированные системы ООВО к критической инфраструктуре и подлежит информационная инфраструктура ООВО подключению к ГосСОПКА? И что это за собой влечет.

Во-первых, необходимо в соответствии с законом провести категорирование информационной системы ООВО и установить соответствует ли информационная инфраструктура по критериям значимости и показателям их значений, присвоение ей одной из категорий значимости [9]. Для осуществления этого можно полагать целесообразным на первом этапе составить полный перечень информационных и автоматизированных систем ООВО с указанием назначения, выполняемых ими функций, составом и вероятностью осуществления компьютерных атак на эти системы (по нали-

чию подключения к сетям общего пользования, в том числе к сети «Интернет»). На втором этапе целесообразно создать комиссию для категорирования, в которую целесообразно включить компетентных работников подразделений информатизации, подразделения информационной безопасности и руководителей структур, в чьих интересах функционируют АИС ООВО.

Далее, представляется целесообразным довести основные положения законодательства до всех членов комиссии, обратив внимание на следующее. Категорирование осуществляется исходя из:

– социальной значимости, выражающейся в оценке возможного ущерба, причиняемого жизни или здоровью людей, возможности прекращения или нарушения функционирования объектов обеспечения жизнедеятельности населения, транспортной инфраструктуры, сетей связи, а также максимальном времени отсутствия доступа к государственной услуге для получателей такой услуги;

– значимости объекта критической информационной инфраструктуры (КИИ) для обеспечения обороны страны, безопасности государства и правопорядка;

– экономической значимости, выражающейся в оценке возможного причинения прямого и косвенного ущерба субъектам КИИ;

– экологической значимости, выражающейся в оценке уровня воздействия на окружающую среду.

Очевидно, что результат категорирования зависит от принадлежности и направленности деятельности ООВО. Так, для медицинских ООВО характерно наличие подразделений, в которых проводятся лечебные процедуры с гражданами. Известно, что в современной медицине для диагностики заболеваний и лечения применяются технические средства с применением информационных технологий или автоматизированных систем. Следовательно, реализация нарушителями КА, может нанести реальный вред жизни и здоровью граждан. Вывод очевиден – эта система должна быть отнесена к КИИ и должна быть обеспечения ее защита [6].

В большом ряду технических ООВО ведутся научные исследования, в том числе по государственному оборонному заказу, проводятся научные эксперименты, для чего создаются объекты с очень сложной техникой при этом на таких научно - исследовательских объектах могут функционировать и информационные системы, и автоматизированные системы управления сложными технологическими процессами, нарушение которых при воздействии КА может привести как к срыву выполнения задач по оборонной тематике или даже к неблагоприятным экологическим последствиям. Вывод очевиден.

События последних лет, связанные с массовыми заболеваниями, привели к переходу ряда ООВО на дистанционное обучение студентов и дистанционную работу персонала. В этих условиях реализация КА на сервер

ООВО может привести как к негативным экономическим последствиям для организации (срыв контрактов, задержка выплаты заработной платы), так и к неоказанию государственной услуги (получение образования – государственная услуга).

В некоторых ООВО созданы и ведут образовательную деятельность военные учебные центры различного профиля. Информационные подсистемы этих центров также могут подвергаться КА и членам комиссии необходимо провести оценку на предмет включения этих подсистем в КИИ, а организации может быть присвоен статус субъекта КИИ.

Представляется, что категория значимости ООВО в соответствии с [9] не будет выше 3 категории.

При отнесении АИС ООВО к значимым объекта КИИ, в соответствии с [10] необходимо планирование и осуществление организационных и технических мероприятий по обеспечению безопасности значимых объектов критической информационной инфраструктуры для чего должна быть создана система безопасности значимого объекта КИИ. Основными задачами системы безопасности значимого объекта КИИ заключается:

в предотвращении неправомерного доступа к информации, обрабатываемой значимыми объектами КИИ, уничтожении такой информации, ее модифицировании, блокировании, копировании;

в недопущении воздействия на технические средства обработки информации, в результате которого может быть нарушено функционирование значимого объекта КИИ ООВО.

Выполнение этих задач влечет за собой необходимость в создании подразделения по обеспечению защиты КИИ от КА, оснащению ООВО средствами обнаружения инцидентов и организации взаимодействия с органами государственной власти и с подразделением ГосСОПКА [11]. Анализ задач, решаемых ООВО, позволяет сделать следующие выводы.

Выводы. 1. Отнесение образовательных организаций к субъектам критической информационной инфраструктуры требует тщательного анализа информационных и автоматизированных систем управления.

2. Отнесение образовательных организаций к значимым субъектам критической информационной инфраструктуры влечет за собой необходимость создания специального подразделения с наличием специалистов,подготовленных к решению задач по обеспечению безопасности информационных и автоматизированных систем управления образовательной организации.

3. В целях обеспечения устойчивого развития ООВО отнесенных к значимым объектам КИИ, необходимо выделение финансовых, технических ресурсов для противодействия КА различного рода.

Список используемых источников

1. Федеральный закон от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации».

2. Указ Президента РФ от 02.07.2021 №400 «О Стратегии национальной безопасности Российской Федерации».

3. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

4. Коцыняк М. А., Карпов М. А., Лаута О. С., Дементьев В. Е. Управление системой обеспечения безопасности информационно-телекоммуникационной сети на основе алгоритмов функционирования искусственной нейронной сети // Известия Тульского государственного университета. Технические науки. 2020. № 4. С. 3–10.

5. Остроумов О. А., Лепешкин О. М., Синюк А. Д. Систематизация основ методологии синтеза критической информационной инфраструктуры Российской Федерации // Военная мысль. 2021. № 8. С. 109–114.

6. Коцыняк М. А., Лаута О. С., Нечепуренко А. П. Методика оценки устойчивости информационно-телекоммуникационной сети в условиях информационного противоборства // Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. 2019. № 1-2 (127-128). С. 58–62.

7. Савищенко Н. В., Митрофанов М. В., Остроумов М. А., Ракицкий С. Н., Остроумов О. А. Анализ реализации процессного подхода в управлении системой связи // Радиолокация, навигация и связь: сборник трудов XXVII Международной научно-технической конференции, посвященной 60-летию полета в космос Ю. А. Гагарина и Г. С. Титова (г. Воронеж, 29 сентября – 30 сентября 2021 г.): в 4 т. / Воронежский государственный университет; АО «Концерн «Созвездие». Воронеж: Издательский дом ВГУ, 2021. Т. 1. 2021. 440 с. С. 62–73.

8. Стародубцев Ю. И., Иванов С. А., Закалкин П. В. Концептуальные направления решения проблем обеспечения устойчивости Единой сети электросвязи Российской Федерации в интересах органов государственной власти и военного управления // Военная мысль. 2021. № 4. С. 39–49.

9. Постановление Правительства РФ от 08.02.2018 № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений».

10. Приказ ФСТЭК России от 21 декабря 2017 г. N 235 «Об утверждении требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры российской федерации и обеспечению их функционирования».

11. Указ Президента Российской Федерации от 15.01.2013 № 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации».

УДК 004.421.5
ГРНТИ 28.29.51

ОСНОВЫ ИСПОЛЬЗОВАНИЯ ТЕСТОВ NIST ДЛЯ ОЦЕНКИ СЛУЧАЙНОСТИ ДВОИЧНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

А. А. Воронцов, С. Н. Шемякин

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Рассматриваются основы использования тестов NIST, используемых для оценки меры случайности числовых двоичных последовательностей. По замыслу данные тесты NIST обеспечивают достаточно полную оценку близости к чисто случайным двоичным последовательностям. Представлены основные аспекты использования данных тестов, а также перечень иных аналогичных тестов.

случайные последовательности, тестирование, генераторы псевдослучайных чисел, проверка статистических гипотез, автокорреляционная функция.

Введение

Для работы различных криптографических систем необходимы случайные числа. Например, в системах криптографического шифрования открытые и закрытые ключи должны быть сгенерированы как случайные числа. Криптографические протоколы также требуют случайных или псевдослучайных чисел для различных целей, например, для создания цифровых подписей. Чтобы количественно оценить случайность двоичных последовательностей, порожденных программными или аппаратными генераторами случайных и псевдослучайных чисел, американским Национальным институтом стандартов и технологий был создан набор статистических тестов NIST. Основы использования статистических тестов NIST приводятся в данной статье.

Описание тестов NIST

Тесты NIST были разработаны Лабораторией информационных технологий, которая является ведущей исследовательской организацией Национального института стандартов и технологий (NIST) под авторством Andrew Rukhin и др. [2]. Тесты NIST представляют собой стандарт, который описывает пакет из 15 статистических тестов, которые были созданы для проверки различных случаев регулярности в произвольных двоичных последовательностях, создаваемых аппаратными или программными криптографиче-

скими генераторами случайных или псевдослучайных чисел. Эти тесты исследуют различные типы неслучайности, которые могут существовать в определенной последовательности.

Уровень значимости, нулевая и альтернативная гипотезы

Тесты NIST являются вероятностными тестами, то есть каждый тест выдает результат тестирования с определенной вероятностью [3]. В тестировании псевдослучайных последовательностей с помощью тестов NIST используется понятие нулевой и альтернативной гипотезы. Каждая из гипотез выдвигает некоторое предположение: нулевая гипотеза H_0, что тестируемая последовательность – случайная, а альтернативная ей гипотеза H_1, что тестируемая последовательность обладает некоторой регулярностью. В каждом тесте выводится решение о принятии нулевой или альтернативной гипотезы [5].

Для проверки нулевой гипотезы по проверяемой последовательности собираются статистические данные, например, о балансе нулей и единиц или количестве серий в последовательности. Также теоретически вычисляются эталонные статистические данные, которые могла бы иметь абсолютно случайная последовательность. Далее измеренная статистика сравнивается с эталонной. Измеренная статистика не может равняться эталонной, так как ни один ГПСЧ не может генерировать чисто случайные последовательности. Для тестирования ГПСЧ вводится определенная погрешность, например 1 %. То есть, если тестируемая последовательность отличается от эталона на 1 %, то данная последовательность не является случайной и гипотеза H_0 отвергается.

После проверки гипотезы выносится некоторый вердикт. Вердикт может быть как верным, так и ошибочным. Исследователь имеет дело с четырьмя возможными вариантами вердиктов [5]:

1. Гипотеза H_0 принята и это правильный вердикт.
2. Гипотеза H_0 отвергнута, хотя последовательность на самом деле случайна. Это ошибка 1 рода.
3. Гипотеза H_0 принята, хотя последовательность случайной не является. Это ошибка 2 рода.
4. Гипотеза H_0 отвергнута, и это правильный вердикт.

Вводится понятие уровня статистической значимости α – это вероятность совершить ошибку 1 рода. При тестировании статистических последовательностей с помощью тестов NIST, значение уровня статистической значимости берется равным 0.01.

При выполнении каждого теста, в качестве выходного результата вычисляется значение вероятности p, которое представляет собой вероятность того, что тестируемая последовательность проверяемого генератора является по своим статистическим свойствам не хуже, чем у гипотетического

истинного генератора случайных чисел. Если $p = 1$, то исследуемая последовательность абсолютно случайна, а если $p = 0$, то последовательность полностью предсказуема. Далее p сравнивается с уровнем статистической значимости α, и если эта вероятность больше α, то последовательность признается случайной. В противном случае – последовательность не проходит тест.

Таким образом можно получить следующие соотношения:

Если $p \geq \alpha$, то последовательность признается случайной с доверительным уровнем 0,99.

Если $p < \alpha$, то последовательность отбраковывается как неслучайная с доверительным уровнем 0,99.

Список тестов [2]:

1. Частотный побитовый тест;
2. Частотный блочный тест;
3. Тест на последовательность одинаковых битов;
4. Тест на самую длинную последовательность единиц в блоке;
5. Тест рангов бинарных матриц;
6. Спектральный тест;
7. Тест на совпадение неперекрывающихся шаблонов;
8. Тест на совпадение перекрывающихся шаблонов;
9. Универсальный статистический тест Маурера;
10. Тест на линейную сложность;
11. Тест на периодичность;
12. Тест приблизительной энтропии;
13. Тест кумулятивных сумм;
14. Тест на произвольные отклонения;
15. Другой тест на произвольные отклонения.

Достоинства и недостатки тестов NIST

Главные достоинства тестов NIST [5]: открытость алгоритмов и однозначная интерпретация результатов тестирования.

Недостатки: проверка больших псевдослучайных последовательностей занимает достаточно много времени, а также требует большого вычислительного ресурса.

Использование графика автокорреляционной функции в тестировании псевдослучайных последовательностей

Данная функция предназначена для оценки корреляции между сдвинутыми копиями исследуемых последовательностей.

Для исследования свойств псевдослучайных последовательностей используется график битовой либо символьной АКФ.

Принцип построения битовой АКФ приведен ниже [5]:

1. Исследуемая битовая последовательность подвергается нормировке: (1 → 1; 0 → -1). Если (e_0; e_1; … e_{n-1}) – двоичная запись последовательности, то нормированная последовательность получается с помощью следующего преобразования:

$$a_i = (-1)^{1-e_i}, i = \overline{0,(n-1)}.$$

2. Производится вычисление всплесков корреляции:

$$c_j = \frac{\sum_{i=0}^{n-1} a_i * a_{(i+j) mod n}}{\sum_{i=0}^{n-1} a_i^2},$$

где n – длина нормированной битовой последовательности $j = \overline{0,n}$.

Символьная АКФ используется в том, случае, если псевдослучайная последовательность представляет собой набор блоков заданной длины (символов). Для построения символьной АКФ используется нижеследующий алгоритм [5]:

1. Исследуемая последовательность подвергается нормировке по следующим правилам. Пусть (p_{R-1}; p_{R-2}; … p_0) – двоичная запись i-го элемента исследуемой последовательности. Тогда нормированное значение элемента вычисляется по формуле:

$$N_i = \sum_{j=0}^{R-1} (-1)^{p_i} * 2^j.$$

2. Далее производится вычисление всплесков корреляции:

$$c_j = \frac{\sum_{i=0}^{n-1} a_i * a_{(i+j) mod n}}{\sum_{i=0}^{n-1} a_i^2}.$$

где n – длина нормированной битовой последовательности $j = \overline{0,n}$.

Интерпретация результатов

Данный тест является графическим, поэтому первоначально строится график исследуемой АКФ. Если исследуемая последовательность случайна или близка по своим статистическим свойствам к случайной, то значения корреляции стремятся к нулю на всей длине последовательности, кроме начального и конечного символов. Если же на графике присутствуют всплески корреляции, между символами в последовательности присутствует корреляция либо последовательность периодическая.

Иные системы тестирования

Кроме NIST существует еще несколько систем статистических тестов псевдослучайных последовательностей. Известны следующие системы тестов:

1. TEST-U01 [1];
2. CRYPT-X [7];
3. DIEHARD [3];
4. Dieharder;
5. Seminumerical Algorithms;

В Российской Федерации разработаны следующие тесты для оценки псевдослучайных последовательностей:

1. Тест «Стопка книг». Авторы Б. Я. Рябко, А. И. Пестунов [6, 7].
2. Дважды адаптивный тест. Автор: Монарев В. А.

Заключение

В статье были рассмотрены основы использования тестов системы NIST для оценки псевдослучайных последовательностей. Приведено краткое описание каждого теста. Были описаны также другие системы тестирование псевдослучайных числовых последовательностей.

Список используемых источников

1. Faure E., Myronets I., Lavdanskyi A. Autocorrelation Criterion for Quality Assessment of Random Number Sequences (англ.) / Cherkasy State Technological University, Shevchenko Blvd., 460, Cherkasy, 18006, Ukraine - 2020, 15 с. Rangineni Sandhya. Cryptographic analysis of random sequences - Jawaharlal Nehru Technological University Anantapur, India - 2009, 55 p.

2. Rukhin A., Soto J., Nechvatal J., Smid M., Barker E., Leigh S., Levenson M., Vangel M., Banks D., Heckert A., Dray J. S. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications (англ.) / VoNIST SP 800-22 Rev. 1a. National Institute of Standards and Technology. - Gaithersburg, MD, 2010, 131 p.

3. Soto Juan. Statistical Testing of Random Number Generators. National Institute of Standards & Technology. (англ.) / S. VoNIST SP 800-22 Rev. 1a. National Institute of Standards and Technology. Gaithersburg, MD, 2010, 95 p.

4. Будько М. Б., Будько М. Ю., Гирик А. В., Грозов В. А. Методы генерации и тестирования случайных последовательностей : учебное пособие / Министерство образования и науки Российской Федерации, Университет ИТМО. Санкт-Петербург, 2019. 70 с. : ил.

5. Иванов М. А., Чугунков И. В. Теория, применение и оценка качества генераторов псевдослучайных последовательностей : учебное пособие / под ред. М. А. Иванова ; Министерство образования и науки Российской Федерации, Национальный исследовательский ядерный университет «МИФИ». Москва : КУДИЦ-ОБРАЗ, 2003. 240 с. : ил.; (СКБ-специалисту по компьютерной безопасности); ISBN 5-93378-056-1.

6. Рябко Б. Я., Пестунов А. И. “Стопка книг” как новый статистический тест для случайных чисел, Проблемы передачи информации. Институт вычислительных технологий СО РАН, Новосибирск, 2004. Т. 40, Вып. 1. С. 73–78.

7. Пестунов А. И. Теоретическое исследование свойств статистического теста «Стопка книг». Том 11. № 6 / Институт вычислительных технологий СО РАН. Новосибирск, 2006. 8 с.

8. Слеповичев И. И. Генераторы псевдослучайных чисел : учебное пособие / Министерство образования и науки Российской Федерации, Саратовский государственный университет. Саратов, 2017. 118 с.

УДК 004.056.53
ГРНТИ 49.33.35

АНАЛИЗ И КЛАССИФИКАЦИЯ ПРОГРАММНЫХ ИНСТРУМЕНТОВ ДЛЯ ТЕСТИРОВАНИЯ НА ПРОНИКНОВЕНИЕ БЕСПРОВОДНЫХ СЕТЕЙ СЕМЕЙСТВА IEEE 802.11

Г. Е. Ворошнин, М. М. Ковцур, Д. В. Юркин

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Беспроводные сети семейства IEEE 802.11 стали неотъемлемой частью повседневной жизни почти каждого человека. Они используются как в самых малых домашних сетях, состоящих из одной точки доступа, так и в крупных корпоративных сетях, где они исчисляются сотнями. Технология Wi-Fi повсюду окружает современного человека: дома, на работе, на учебе, в кафе и магазинах. При этом очень незначительная часть пользователей беспроводных сетей задумываются, насколько безопасно их подключение к интернету, а впоследствии и все данные, которые они передают по сети. Количество инцидентов информационной безопасности с каждым годом увеличивается. Одним из самых распространенных объектов атак является сетевое оборудование, которое, в частности, обеспечивает подключение клиентов по сетям семейства IEEE 802.11. Наряду с процессом постоянного совершенствования качества и стандартов обеспечения безопасности беспроводных сетей, совершенствуются и методы атак на беспроводные сети. В настоящее время даже новое оборудование, оснащенное самыми современными инструментами информационной безопасности, подвержено множеству элементарных атак, значительно ухудшающих качество обслуживания. В связи с этим, изучение инструментов тестирования актуально как для проверки устойчивости беспроводной сети к различным атакам, так и для создания методов обнаружения и противодействия злоумышленникам.

информационная безопасность, безопасность беспроводных сетей, тестирование на проникновение.

Большинство современных людей не могут представить свою жизнь без технологии Wi-Fi, так как использует ее ежедневно. Этот стандарт стал

популярным благодаря удобству, которое заключается не только в свободном перемещении пользователей в пределах зоны покрытия точки доступа (ТД), но и в возможности подключения мобильных устройств – смартфонов, планшетов и др.

Несмотря на множество плюсов этой технологии, она обладает существенным недостатком, заключающимся в использование общедоступной среды передачи данных. Этот недостаток приводит к тому, что злоумышленники, находящиеся поблизости ТД, могут беспрепятственно перехватывать данные легитимных клиентов сети и передавать в беспроводную среду любую информацию, в том числе и простые шумы [1].

Популярность сетей семейства IEEE 802.11, совместно с уязвимостью беспроводной среды передачи данных, уязвимостями в сетевом оборудовании, протоколах и приложениях, привели к бурному росту популярности атак на беспроводные сети. Простота реализации некоторых атак привела к росту количества атак. Для множества из них создаются утилиты, значительно облегчающие работу злоумышленникам.

По статистике от лаборатории Касперского около 25 % точек доступа в мире не используют шифрование [2]. Это подвергает пользователей опасности перехвата критически важной информации: персональных данных, данных банковских счетов и пр.

Одним из важных аспектов нашей жизни стал публичный Wi-Fi. Многие пользуются беспроводными сетями в кафе, аэропортах, метро и прочих общественных местах, не обращая внимания на способы защиты информации в них. Общая статистика использования различных видов шифрования для публичных ТД представлена на рис. 1 [2].

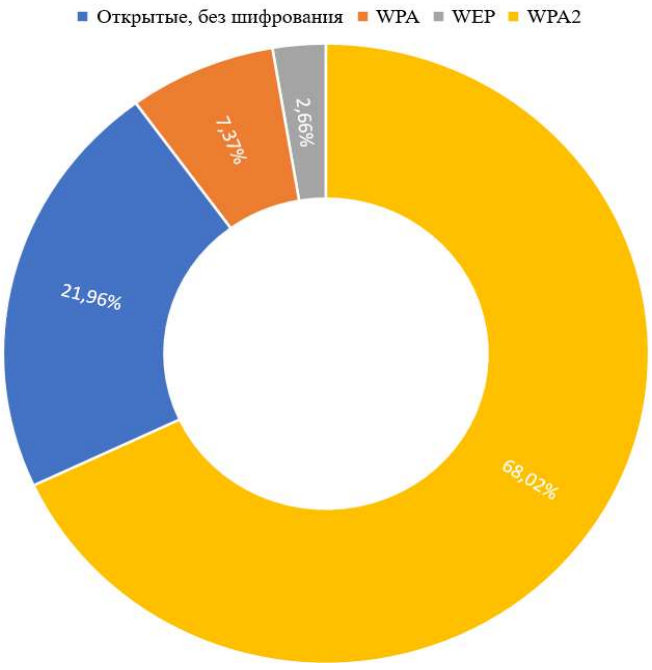


Рис. 1. Типы шифрования публичных Wi-Fi сетей в мире

В настоящем исследовании рассмотрены распространенные инструменты тестирования беспроводных сетей, которые целесообразно применять для проверки устойчивости сетей на разных этапах ее функционирования, таких как создание, внедрение и эксплуатация. Также

необходимо учитывать, что рассматриваемые инструменты могут быть использованы злоумышленниками, поэтому стоит предпринимать соответствующие профилактические меры защиты [3].

Для наглядного представления классификации была составлена схема, представленная на рис. 2.

Рис. 2. Классификация утилит для тестирования Wi-Fi

Базовыми инструментами для мониторинга беспроводной сети являются программы-анализаторы трафика. Данные инструменты используются для обнаружения дефектов работы сети или отладки работы различных приложений, сайтов или серверов.

Одним из наиболее популярных программ данного класса инструментов является wireshark. Его распространенность обусловлена несколькими факторами:

– открытый исходный код и доступность практически на всех самых распространенных операционных системах;

– удобный и простой в использовании графический интерфейс, позволяющий в реальном времени видеть состояние сети;

– предоставление широкого функционала для анализа трафика как в режиме реального времени, так и из файла дампа, собранного ранее (в том числе другими инструментами);

Также есть множество других анализаторов трафика для беспроводных сетей, которые также заслуживают внимания, например Intercepter-NG, tcpdump и tshark. Популярность этих инструментов можно сравнить, проанализировав изменение количества веб-запросов в месяц за несколько лет на графике, представленном на рис. 3.

Еще один класс программ пассивного тестирования – криптографические утилиты [4]. Очень распространенным, известным и многофункциональным является инструмент aircrack-ng. Она реализует различные подходы для взлома ключей 802.11 WEP и WPA/WPA2-PSK. Также к этому классу можно отнести такие популярные инструменты, как взломщик паролей hashcat и bully (проводит перебор паролей (брутфорс) для протокола WPS).

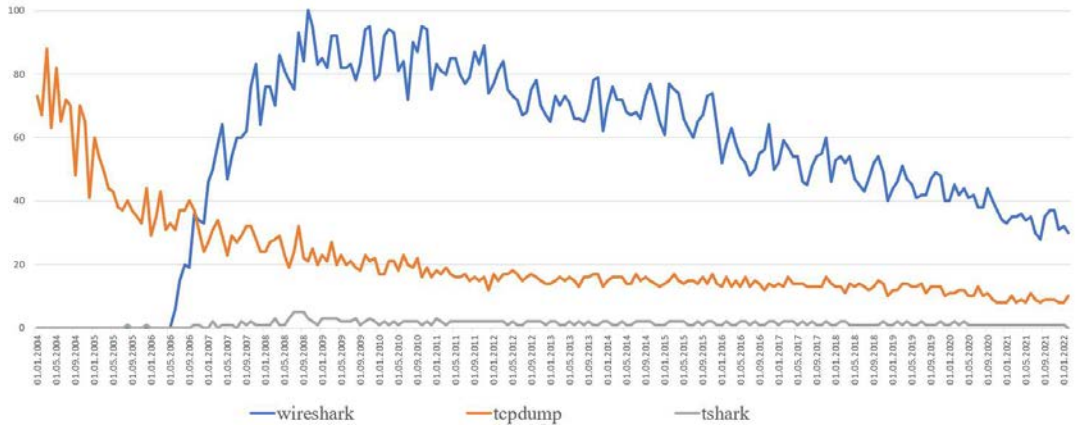


Рис. 3. Количества веб-запросов в месяц для инструментов мониторинга

Другим большим классом утилит для тестирования Wi-Fi, как видно из рис. 2, являются инструменты активного тестирования.

К наиболее распространенным представителям простейших утилит этого класса можно отнести aireplay-ng (производит инъекции произвольных кадров в беспроводную сеть и DoS атаки), boopsuite и besside-ng (проводят деаутентификацию и собирают рукопожатия), wesside-ng (реализованы различные методики взлома WEP), airtun-ng (производит инжект и управление интерфейсами).

К наиболее масштабным комплексным утилитам тестирования можно отнести:

● Airgeddon. Этот инструмент может выполнять: управление интерфейсами, DoS-атаки, захват рукопожатий, расшифровка паролей из захваченных рукопожатий WPA/WPA2 (по словарю, брут-форс, основанная на правилах), создание Fake AP, производить атаки на WEP (такие как Chop-Chop, Caffe Latte, Hirte, Fragmentation, Fake association и т. д.), брутфорс WPS.

● Mdk3 и mdk4. Эти инструменты выполняют: DoS-атаки (Beacon, аутентификации, деаутентификации, деассоциации, EAPOL Start и Logoff), атаки на IEEE 802.11s mesh, фаззинг сети.

Изучив большое количество инструментов, были сформированы требования к инструменту тестирования информационной безопасности в беспроводных сетях семейства IEEE802.11:

1. Комплексность. Инструмент должен реализовывать тестирование сетей в различных направлениях – DoS-атаки, взлом шифрования, атаки на сетевые протоколы и пр.;

2. Автоматизация и гибкость [5]. Инструмент должен производить различные виды атак с минимальным участием человека, при этом не исключая возможность тонкой настройки;

3. Простота. При использовании утилиты не должны требоваться глубокие знания в сфере сетей, методик проведения атак и пр.;

4. Интеграция в внешними системами. Инструмент должен иметь возможность интеграции с внешними системами, такими как wIPS, wIDS, SIEM [6] и некоторыми другими, для согласованного аудита информационной безопасности беспроводных сетей [7].

Исходя из изученного материала и проведенной работы, можно однозначно сказать, что инструменты тестирования постоянно совершенствуются наравне с развитием технологий.

Но нужно заметить, что чаще всего инструменты создаются не для аудита безопасности, а для атак со стороны злоумышленников, поэтому инструменты часто носят узконаправленный характер.

Исходя из этого, можно выявить потребность в создании инструмента аудита беспроводных сетей семейства IEEE 802.11, требования к которому были сформированы.

Список используемых источников

1. Волкогонов В. Н., Казанцев А. А., Катасонов А. И., Орлов Г. А. Анализ безопасности Wi-Fi сетей // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VIII Международной научно-технической и научно-методической конференции : сб. науч. ст. в 4 т. СПб.: СПбГУТ, 2019. С. 270–275.

2. Исследование: незащищенные Wi-Fi-сети по всему миру. URL: https://secure-list.ru/research-on-unsecured-wi-fi- networks-across-the-world/29731/ (дата обращения: 13.01.2022).

3. Суворов В. С. Проведение теста устойчивости беспроводной сети к проникновению // Системы управления, сложные системы: моделирование, устойчивость, стабилизация, интеллектуальные технологии : материалы VII Международной научно-практической конференции, Елец, 22–23 апреля 2021 года. Елец: Елецкий государственный университет им. И. А. Бунина, 2021. С. 294–296.

4. Kyei, M., & Asante, M. (2020). Penetration Testing of IEEE 802.11 Encryption Protocols using Kali Linux Hacking Tools // International Journal of Computer Applications. 176. pp. 26–33.

5. Kadam S. P., Mahajan B., Patanwala M., Sanas P. and Vidyarthi S. Automated Wi-Fi penetration testing // 2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), 2016. pp. 1092–1096. doi: 10.1109/ICEEOT.2016.7754855.

6. Бабков И. Н. Анализ эффективности SIEM-системы в организации // Актуальные проблемы инфотелекоммуникаций в науке и образовании. X Юбилейная Международная научно-техническая и научно-методическая конференция : сборник научных статей в 4-х т. СПб.: СПбГУТ, 2021. С. 72–77.

7. Карельский П. В., Зуев И. П., Ковцур М. М., Миняев А. А. Разработка методики тестирования IPS модуля // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2021. № 1. С. 25-31. DOI 10.46418/2079-8199_2021_1_4

УДК 004.451
ГРНТИ 81.93.29

АНАЛИЗ ХАРАКТЕРИСТИК И ВОЗМОЖНОСТЕЙ ВИРТУАЛЬНОЙ СЕТИ НА ОСНОВЕ ПРОСТРАНСТВ ИМЁН NETWORK NAMESPACE В ОПЕРАЦИОННОЙ СИСТЕМЕ GNU/LINUX

С. Г. Вьюгов, С. В. Козлов

Академия Федеральной службы охраны Российской Федерации

Одним из ключевых элементов операционной системы GNU/Linux является изоляция процессов. Внутренний механизм пространств имён, реализованный в данной операционной системе, позволяет изолировать процессы на уровне ядра. Дерево процесса Network, имеет собственный набор таблиц маршрутизации. Появляется возможность туннелировать трафик отдельных приложений и создавать модели виртуальных сетей с заданными качественными характеристиками канала связи.

пространство имен, физический стек, виртуальный стек, характеристики канала связи.

В наше время сфера сетевых технологий является наиболее перспективным направлением, так как возрастает необходимость моделирования распределенных сетей с последующей возможностью анализа характеристик каналов связи при различных уровнях нагрузки сетевого трафика. С точки зрения информационной безопасности сетевых технологий, возникает потребность туннелирования трафика для отдельных приложений операционной системы.

В операционной системе GNU/Linux в версии ядра 2.4.19 была усовершенствована изоляция процессов. Таким образом на данный момент доступно шесть пространств имён:

1. Файловая система (Mount);
2. UTS;
3. ID процессов (PID);
4. Сети (Network);
5. Межпроцессное взаимодействие (IPC);
6. Пользовательские ID (User).

В рамках моделирования виртуальной сети используется пространство имён Network. Сетевое пространство имён ограничивает видимость процесса внутри сети. Оно позволяет создавать собственные интерфейсы,

наборы IP-адресов и портов, таблицы маршрутизации и правила файрволла [1].

В рамках оценки характеристик и возможностей виртуальной сети на основе технологии сетевого пространства имён была реализована модель сети, представленная на рис. 1.

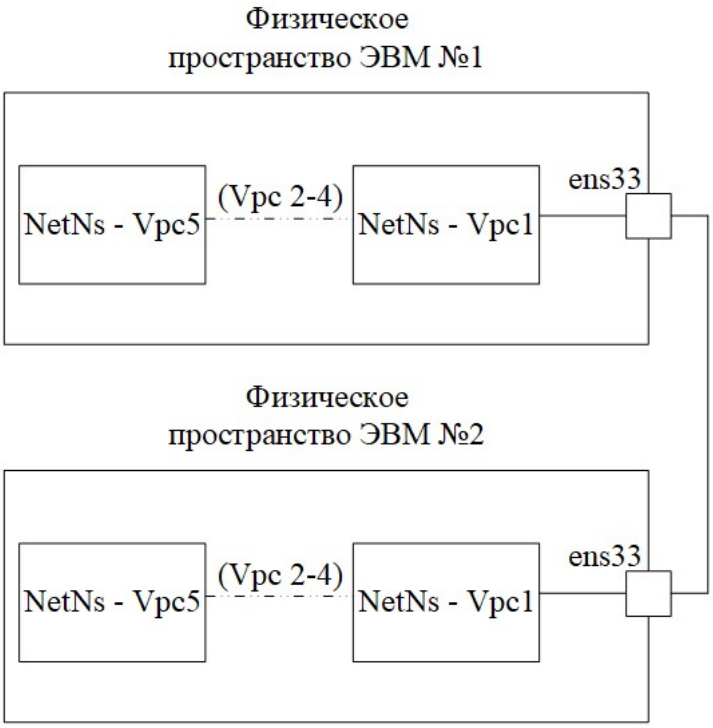


Рис. 1. Модель виртуальной сети
в операционной системе GNU/Linux

Задача воссоздания реального процесса работы пользователей в сети решилась на основе имитационного моделирования. Для формирования потока данных необходимо использовать два генератора случайных чисел (ГСЧ). Один ГСЧ используется для задания интервалов между пакетами, второй генератор – для определения размера пакетов. В соответствии с принятыми в теории телетрафика подходами [2], для каждого моделируемого потока данных создаются независимые ГСЧ, обеспечивающие формирование последовательностей случайных чисел, некоррелированных между собой и распределенных по экспоненциальному закону.

Формирование экспоненциально – распределенных последовательностей осуществляется на основе преобразования исходной линейно – распределенной случайной последовательности [3].

Экспоненциальное распределение задано выражением:

$$F(x) = 1 - e^{\frac{-x}{\mu}}, x \le 0. \quad (1)$$

А случайная величина (СВ) определяется как:

$$X = -\mu \ln U, 0 < U \le 1 \quad (2)$$

и имеет экспоненциальное распределение со средним μ, если U – равномерно – распределенная СВ на интервале [0,1].

Для того чтобы определить СВ при $U = 0$, берется достаточно малое значение, для которого вычисляется логарифм с заданной точностью.

Для генерации экспоненциально – распределенных СЧ может быть использован итерационный алгоритм, основанный на генерации битовых последовательностей, а для генерации равномерно – распределенной СВ U на интервале [0,1] используется линейный конгруэнтный метод или метод вихря Мерсена [3].

За основу возьмем линейно конгруэнтный метод. По данному методу последовательности строятся в соответствии с выражением

$$X_{k+1} = (aX_k + c) \bmod m, \qquad (3)$$

где a, c, m – случайные целые числа.

Формируемая последовательность зависит от начального значения X_0 – «посева». Для генерации двух последовательностей СЧ при моделировании межпакетного интервала и размера пакетов необходимо задавать разные значения X_0. Также для формирования разных последовательностей при каждом запуске, необходимо определить источник энтропии для начального заполнения X_0. В качестве источника энтропии используется комбинация значений MAC – адреса сетевой карты, системного таймера, номеров процессора и диска компьютера.

Используя свойства рекуррентной последовательности (3) могут быть подобраны коэффициенты a, c, m таким образом, чтобы период последовательности был максимален [3]. Эта комбинация, следующая: $a = 48\,271$, $c = 0$, $m = 231\text{-}1$.

Поскольку линейно конгруэнтный метод генерирует целочисленную последовательность на интервале [0, 231-2], то ее необходимо привести к вещественной последовательности случайных величин U на интервале [0, 1]. Такое преобразование возможно с точностью 2^{-31}.

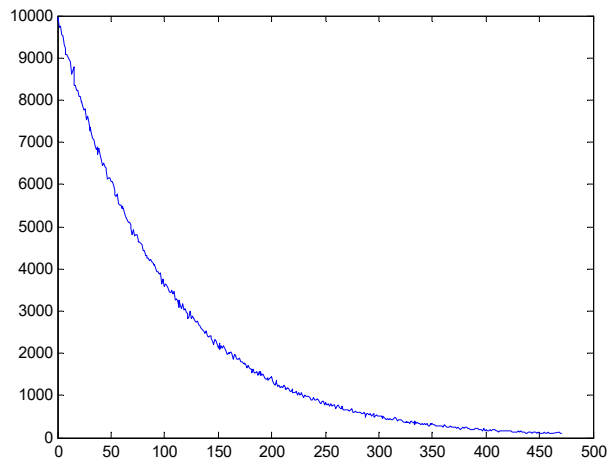


Рис. 2. Эмпирическое распределение частот случайных чисел

Для экспериментальной оценки качества полученного распределения случайных чисел разработана программа на языке программирования C++, в которой используется линейный конгруэнтный генератор из стандартной библиотеки с указанными выше коэффициентами минимального стандарта.

На рис. 2 (см. выше) представлен график эмпирического распределения частот случайных чисел.

Из графика видно, что эмпирическое распределение соответствует экспоненциальному закону. Полученный результат позволяет использовать разработанные ГСЧ для формирования трафика.

В результате проведения анализа канала связи были получены результаты, представленные в таблице.

Таблица. Результаты тестирования виртуальной сети

Интервал времени	Количество переданных данных	Средняя скорость передачи данных	Количество повторных отправлений	Тип источника
0.00 – 10.00	1.10 GBytes	115111 KBytes/s	250	Отправитель
0.00 – 10.00	1.10 GBytes	114828 Kbytes/s	-	Приемник

Остальные тесты проводились при изменении количество виртуальных стеков в модели виртуальной сети. Количество переданных данных и средняя скорость передачи данных на протяжении всего тестирования оставались неизменными. На рисунке 3 представлен график зависимости количества повторных запросов от количества виртуальных узлов между двумя оконечными пользователями сети.

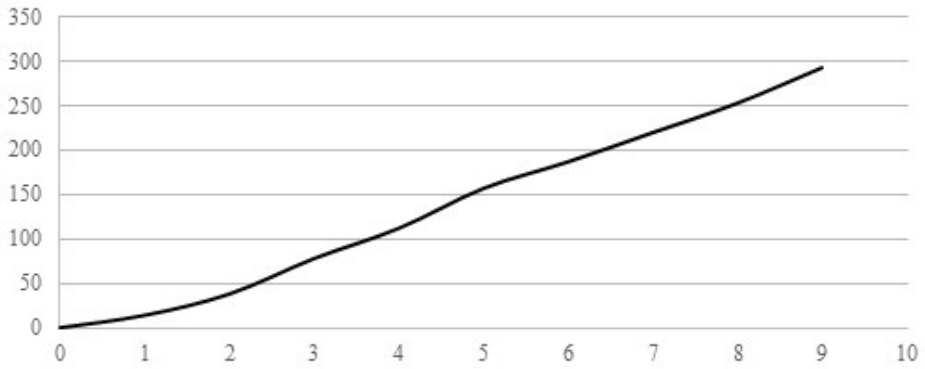


Рис. 3. График зависимости количества повторных запросов от количества виртуальных стеков между оконечными абонентами

Высокая скорость передачи данных, объясняется тем, что технология пространств имён работает на уровне ядра. Недостатком на данный момент является зависимость количества повторных запросов при увеличении числа транзитных виртуальных узлов. Таким образом технология сетевого пространства имен очень перспективна и требует дальнейшего изучения её возможностей.

Список используемых источников

1. Козлов С. В., Вьюгов С. Г., Щукин А. В. Моделирование сетей передачи данных на основе пространств имен в операционное систему GNU/Linux // Информационное технологии моделирования и управления 2021. Т. 126, № 4. С. 279–286.
2. Корнышев Ю. Н., Пшеничников А. П., Харкевич А. Д. Теория телетрафика. М. : Радио и связь, 1996. 272 с.
3. Кнут Д. Э. Искусство программирования: Получисленные алгоритмы : пер. с англ. 3-е изд. Москва : Издательский дом «Вильямс», 2001. 832 с.

УДК 004.056
ГРНТИ 49.33.35

МОДЕЛИ ОБРАБОТКИ СОБЫТИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ИНТЕЛЛЕКТУАЛЬНЫХ СИСТЕМАХ МОНИТОРИНГА И ОЦЕНКИ ЗАЩИЩЁННОСТИ КРИТИЧЕСКИ ВАЖНЫХ ИНФРАСТРУКТУР

Д. А. Гайфулина, И. В. Котенко

Санкт-Петербургский Федеральный исследовательский центр Российской академии наук

К критически важным инфраструктурам можно отнести совокупность автоматизированных систем управления процессами критически важных объектов, функционирующих в сферах здравоохранения, науки, транспорта, связи, энергетики, финансов, обороны и промышленности. Как правило, такие инфраструктуры требуют непрерывного контроля и анализа событий безопасности с целью предсказания вероятности возможного отказа, снижения уровня надежности, а также атакующих действий. В данном исследовании проводится анализ и разработка моделей обработки событий информационной безопасности в интеллектуальных системах мониторинга и оценки защищённости критически важных инфраструктур. В качестве моделей событий предлагается использовать модели представления знаний о событиях безопасности следующих видов: правила, логическое представление, семантические сети и фреймы. Модели обработки событий безопасности определяются в соответствии с представленными моделями событий, а также в соответствии с решаемой задачей: классификацией, прогнозированием или восстановлением зависимостей событий.

события безопасности, обработка событий безопасности, управление безопасностью.

В настоящее все большую актуальность и практическую важность приобретают вопросы обеспечения безопасности критически важных инфраструктур (КВИ), которые функционируют в таких сферах как промышленность, здравоохранение, государственное управление, энергетика и других.

Подобные инфраструктуры требуют непрерывного контроля и анализа состояния с целью предсказания вероятности возможного отказа, а также угроз кибербезопасности [1, 2]. Наиболее перспективными методами мониторинга и оценки защищенности объектов КВИ являются различные методы и подходы, основанные на моделях искусственного интеллекта. Подобные методы позволяют отслеживать большое количество системных событий и определять те их них, которые могут представлять потенциальную угрозу или указывать на атаку [3, 4]. В таком контексте часто речь идет о событиях безопасности, примером которых могут быть сообщения об обнаружении необычной активности.

Главной задачей данного исследования является разработка и анализ моделей обработки событий информационной безопасности в интеллектуальных системах мониторинга и оценки защищённости критически важных инфраструктур. Модели обработки событий безопасности предлагается определить в соответствии с моделями последовательности событий, а также в соответствии с решаемой задачей обработки. Ранее авторами был проведен обзор существующих исследований в области обработки событий безопасности и на его основе составлена классификация используемых методов [5]. Данные обзор и классификация лежат в основе предлагаемых моделей.

В общем значении события в объектах КВИ представляют собой информацию об изменении состояния с любым физическим, логическим или иным дискриминирующим условием. Обозначим как E набор регистрируемых событий безопасности e, например в системных журналах или сетевых пакетах. Информация об изменении состояния, как правило, включает в себя временную метку t, определяющую порядок возникновения событий во временном ряду $T = \{t_1, \ldots, t_m\}$, где m – длина временного ряда. Таким образом, последовательные события часто упорядочены по времени: $E(t) = \{e(t_k) \mid t_k \leq t_{k+1}\}$.

Последовательность событий обозначим как пару $eS = (E, R)$, где E – набор упорядоченных событий, а R – множество отношений между ними. Каждый элемент множества R описывает некоторые условия отношения пары событий e_1 и e_2 как $r(e_1, e_2)$. Мы предлагаем классификацию моделей последовательности событий на основе методов представления знаний в интеллектуальных системах: правила, логическое представление, семантические сети и фреймы [3]. Описание предложенных моделей представлено в таблице.

Часто для представления соответствия событий безопасности говорят об их корреляции [6]. Корреляция событий представляет собой создание контекста между независимыми событиями и собранной ранее информацией в реальном времени. Данный процесс можно представить в виде отоб-

ражения *Corr*: $e_1 \rightarrow e_2$, где символ (→) обозначает функциональную зависимость между событиями e_1 и e_2. При этом событие e_2. называется коррелирующим для события e_1, если $e_2 = Corr(e_1)$. При этом пара событий может принадлежать как одной последовательности событий (e_1, $e_2 \in E$), так и к разным ($e_1 \in E_1$, $e_2 \in E_2$). Сопоставление событий разных последовательностей eS_1 и eS_2 аналогично позволяет говорить об их корреляции как об отображении *Corr*: $eS_1 \rightarrow eS_2$.

Мы выделяем три основных категории методов корреляции событий.

1. Методы корреляции на основе подобия ($Corr_{SB}$) основаны на идее, что схожие события могут иметь одну и ту же основную причину или один и тот же тип, а найденные связи зависят от присущего сходства между атрибутами каждого события. Пусть q^e – множество свойств (атрибутов) события e. Тогда можно говорить о пары подобии событий ($e_1 \sim e_2$) на основе попарного подобия их свойств ($q^{e_1} \sim q^{e_2}$) как:

$$(q^{e_1} \sim q^{e_2}) \wedge (e_1 \in E) \Rightarrow (e_1 \sim e_2) \Rightarrow (e_2 = Corr_{SB}(e_1)) \wedge (e_2 \in E).$$

ТАБЛИЦА. Модели последовательности событий безопасности

Модель представления знаний	Краткое описание	Модель последовательности событий
Правила	Обработка событий на основе правил использует знания о взаимосвязи событий в виде условных предложений.	$eS = (E, R)$, E – набор упорядоченных событий, R – набор условий для сравнения и агрегирования событий безопасности.
Логическое представление	Обработка событий на основе логики использует некоторый язык с определенными синтаксисом и семантикой для установления связи между вводом и выводом.	$eS = (e_0, E_i, E_f, \Sigma, \delta)$, $E = (e_0, E_i, E_f)$ – множество событий, e_0 – начальное событие, Ei – множество промежуточных событий, E_f – множество конечных событий, $R = (\Sigma, \delta)$ - множество отношений, Σ - входной алфавит, множество непустых символов, $\delta: E \times \Sigma \rightarrow E$ - функция перехода состояний.
Семантические сети	Обработка событий на основе семантических сетей использует знания в форме графических сетей.	$eS = (E, R, w)$, E – набор событий в виде вершин графа, $R \subset E \times E$ – множество ребер, $w: E \rightarrow \mathbb{R}$ – функция, отображающая ребра в их веса.

Модель представления знаний	Краткое описание	Модель последовательности событий
Фреймы	Обработка событий на основе фреймов использует структуру данных, которая состоит из набора характеристик события и его значений.	$eS = (E, Y, f)$, $E = (E, Y)$ – множество событий и соответствующих им типов (классов), E – множество событий, Y – множество типов событий, f – функция отображения $Y = f(E)$.

2. Причинно-следственные методы корреляции ($Corr_{CB}$) ориентированы на поиск предпосылок и последствий в последовательности событий, когда предыдущие шаги определяют последующие. Пусть $p^e = \{p \mid (p, e) \in E\}$ – множество предпосылок события e, а $c^e = \{c \mid (e, c) \in E\}$ – множество последствий. Тогда корреляция пары событий определяется сопоставлением последствий более раннего события $e(t_k)$ с последствиями последующего события $e(t_d)$ для временных отметок $(t_k, t_d) \in T$, где $t_k < t_d$. При этом предполагается, что предпосылки события $e(t_d)$ являются подмножеством последствий события $e(t_k)$: $p^{e(t_d)} \subset c^{e(t_k)}$. Тогда причинно-следственная корреляция определяется как:

$$(p^{e(t_d)} \subset c^{e(t_k)}) \wedge ((e(t_d), e(t_k)) \in E) \Rightarrow e(t_d) = Corr_{CB}(e(t_k)).$$

3. Интеллектуальный анализ данных ($Corr_{DM}$), представляющий собой процесс обнаружения существенных закономерностей eS_p в последовательности событий безопасности:

$$eS_p = Corr_{DM}(eS),\ eS_p \subset eS.$$

В дополнении можно выделить гибридные (смешанные) методы корреляции событий, которые позволяют объединять перечисленные категории методов. Применение обработки событий безопасности в интеллектуальных системах мониторинга и оценки защищенности, в свою очередь, также можно разделить на три основных направления.

1. Кластеризация событий для уменьшения объема обрабатываемой информации и классификация событий безопасности для группировки событий. Обработка событий при этом заключается в построении последовательностей eS на основе анализа внутренней корреляции событий как:

$$(e_2 = Corr(e_1)) \wedge (e_1 \in eS) \Rightarrow e_2 \in eS.$$

2. Обнаружение вторжений, которое имеет дело с многошаговыми и целенаправленными атаками, или обнаружение аномалий. При условии

наличия базы знаний о всех состояниях объекта КВИ, задачу оценивания и прогнозирования состояния можно свести к задаче классификации [7]. Так последовательность определенных событий eS_a можно рассматривать как сценарий атаки, где каждое событие является шагом злоумышленника. Путь атакующего при этом можно описать как $eS_a = \{a_0 \ldots a_n \mid a \in E\}$, где a_0 – начальное событие атаки, a_n – цель атаки, n – длина пути.

Обозначим текущее состояние объекта КВИ, с точки зрения кибербезопасности, как последовательность текущих событий безопасности eS_c. Сопоставление текущей последовательности событий с известной последовательностью атакующих действий, как $Corr$: $eS_c \rightarrow eS_a$, используется для обнаружения многошаговых атак [8]. При условии, наличия априорной базы знаний только о некоторых штатных состояниях объекта КВИ можно говорить о задаче детектирования аномалий. При этом известна последовательность событий при нормальной работе eS_n, а отображение вычисляется как $Corr$: $eS_c \rightarrow eS_n$.

3. Предсказание вторжений на основе входящих событий, позволяющее заблаговременно обнаруживать цели злоумышленников. Задачу прогнозирования состояния объектов КВИ можно представить в виде задачи идентификации класса состояния объекта в следующий момент времени. При этом осуществляется как предсказание последующего за событием $e(t_k)$ события $e(t_{k+1}) = Corr_e(e(t_k))$, так и определения класса подобной последовательности: $Corr_s(eS_c) = \{eS_a, eS_n\}$.

Подводя итоги, общая модель обработки событий безопасности включает в себя пару:

$$B = (eS, CR),\ eS = (E, R),\ CR = \{Corr_i\},$$

где eS – модель последовательности событий безопасности, CR – множество методов корреляции событий безопасности, применимых к eS.

В своей основе модели обработки событий позволяют описать подходы к решению задачи оценки защищенности и прогнозирования состояния объектов КВИ на основе интеллектуальной обработки событий. Подобные подходы имеют общую цель: обнаружение и прогнозирование нарушений безопасности, которые имеют пошаговый характер, такие как многошаговые или целевые атаки или причинно-следственные нарушения стабильности системы. Оценка и прогнозирование состояния безопасности сложных объектов должны всесторонне учитывать аспекты работоспособности алгоритмов анализа данных. В качестве перспективного подхода можно использовать гибридные методы, позволяющие совмещать как различное представление данных, так и различные методы корреляции.

Работа выполнена при частичной финансовой поддержке РНФ (проект № 21-71-20078).

Список используемых источников

1. Законодательно-правовое и организационно-техническое обеспечение информационной безопасности автоматизированных систем и информационно-вычислительных сетей / И. В. Котенко, М. М. Котухов, А. С. Марков и др.; под редакцией И. В. Котенко. Санкт-Петербург, 2000. 190 с.
2. Kotenko I., Stepashkin M. Network Security Evaluation based on Simulation of Malefactor's Behavior // Proceedings. International Conference on Security and Cryptography, SECRYPT 2006. Polytechnic Institute of Setubal. Setubal, 2006. pp. 339–344.
3. Охтилев М. Ю. Системы искусственного интеллекта и их применение в автоматизированных системах мониторинга состояния сложных организационно-технических объектов. СПб.: ГУАП. 2018. 261 с.
4. Котенко И. В., Полубелова О. В., Саенко И. Б., Чечулин А. А. Применение онтологий и логического вывода для управления информацией и событиями безопасности // Системы высокой доступности. 2012. Т.8, № 2. С. 100–108.
5. Гайфулина Д. А., Котенко И. В. Анализ критериев классификации подходов к корреляции событий безопасности // Актуальные проблемы инфотелекоммуникаций в науке и образовании. X Юбилейная Международной научно-технической и научно-методической конференции : сб. науч. ст. в 4 т. СПб.: СПбГУТ, 2021. С. 206–210.
6. Yu Beng, L., Ramadass, S., Manickam, S., Soo Fun, T. A survey of intrusion alert correlation and its design considerations // IETE Technical Review. 2014. Vol. 31. N. 3. pp. 233–240.
7. Kovačević I., Groš S., Slovenec K. Systematic Review and Quantitative Comparison of Cyberattack Scenario Detection and Projection // Electronics. 2020. Vol. 9. N 10. P. 1722.
8. Kotenko I., Fedorchenko A., Doynikova E. Data Analytics for Security Management of Complex Heterogeneous Systems: Event Correlation and Security // Advances in Cyber Security Analytics and Decision Systems. EAI/Springer Innovations in Communication and Computing. Springer, Cham. 2020. pp. 79–116.

УДК 004.056
ГРНТИ 81.93.29

ОЦЕНКА ТОНАЛЬНОСТИ ТЕКСТОВЫХ ПУБЛИКАЦИЙ ДЛЯ ВЫЯВЛЕНИЯ ДЕСТРУКТИВНЫХ ВОЗДЕЙСТВИЙ В СОЦИАЛЬНЫХ СЕТЯХ

Д. А. Гайфулина[1], И. В. Котенко[1,2], Е. В. Федорченко[1,2]

[1]Санкт-Петербургский Федеральный исследовательский центр Российской академии наук

[2]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Информация, предоставляемая пользователями на страницах сообществ в социальных сетях, может оказывать деструктивное воздействие на других пользователей, особенно представителей социально-демографической группы «молодежь». Одним из признаков, используемых для выявления деструктивных воздействий в социальной сети

может быть тональность текстовых публикаций. В исследовании проанализированы существующие размеченные по тональности наборы русскоязычных постов, выбран набор данных для обучения и протестирован ряд классификаторов. В результате был выбран классификатор FastText, который использовался для классификации постов отобранных сообществ на положительные, отрицательные, нейтральные, речь и неопределенные. Результаты были проверены экспертами. На основе тональности постов предложена дополнительная метрика оценки тональности для выявления деструктивных сообществ в социальных сетях.

деструктивное воздействие, социальная сеть, тональность, классификация, FastText, метрика оценки.

В настоящее время информационное пространство является популярной средой коммуникации. Потребляемая информация может влиять на чувства и в перспективе на личностные качества людей, в том числе деструктивно. Особенно это относится к молодому поколению. Чтобы подтвердить данное утверждение авторы ранее предложили подход к выявлению сообществ социальной сети, которые могут оказывать потенциально деструктивное (разрушающее) воздействие [1]. Для анализа авторы выбрали популярную социальную сеть ВКонтакте (ВК) [2]. Для разметки сообществ по потенциальному оказанию деструктивных воздействий использовались шкалы психологического теста [3], на текущий момент исследование было ограничено анализом шкалы «деструктивная тревожность». В качестве входных данных для классификации использовались текстовые публикации 244 сообществ. Эксперименты проводились с использованием текстовых классификаторов. Поскольку полученные результаты – точность классификации 55,72 % по трем классам (низкая, средняя и высокая деструктивная тревожность) [1] – не являются удовлетворительным, в данной работе исследуется тональность текстовых публикаций с целью дальнейшего использования для повышения точности классификации и как следствие – точности выявления потенциально деструктивных информационных воздействий. Тональность текста отражает эмоциональное отношение автора к какому-либо объекту, выраженному в тексте. Основной целью анализа тональности является поиск мнений в тексте и выявление их свойств. При этом текст классифицируют на три распространенные категории: позитивный, негативный и нейтральный.

Существует ряд популярных наборов данных, содержащий русскоязычные тексты из социальных сетей – RuTweetCorp [4], RuSentiment [5], и Russian Language Toxic Comments (RLTC) [6]. RuTweetCorp содержит более 200 000 публикаций социальной сети Твиттер (Twitter), которые автоматически размечены на две категории тональности: негативную и позитивную. RuSentiment представляет собой набор около 27 000 текстовых постов из социальной сети ВКонтакте, вручную отнесенных к одной из 5 категорий тональности. Помимо классических (позитивная, негативная и нейтральная

тональность) авторы набора данных добавили категорию «речь» (speech) и «неопределено» (skip). Под речью понимаются шаблонные приветствия, поздравления и благодарности, для которых сложно определить эмоциональное отношение автора. К неопределенной категории относятся неявные случаи, зашумленные посты и такой неавторский контент как цитаты, стихотворения и тексты песен. RLTC является набором данных 14 000 комментариев с сайтов 2ch.hk и pikabu.ru, отмеченных как негативные или позитивные с точки зрения тональности.

В качестве входных данных для проведения эксперимента выступают публикации сообществ ВК. Для определения тональности постов предлагается использовать классификатор, предобученный на наборе данных RuSentiment, который получен из аналогичного источника. Ряд таких классификаторов представлен в библиотеках машинного обучения для обработки текстов на естественном языке. Для сравнения приводятся две популярные библиотеки: DeepPavlov [7] и Dostoevsky [5]. Содержащиеся в них модели основаны на глубоких нейронных сетях (*Deep Neural Networks*, DNN), таких как сверточные нейронные сети (*Convolutional Neural Network*, CNN) или двунаправленные генеративно-состязательные сети (*Bidirectional Gated Recurrent Units*, BiGRU). Важной частью также являются методы встраивания текстов (*Word Embedding*), среди которых представлены BERT, FastText и ELMo [8]. Результаты сравнения моделей анализа тональности текста из приведенных библиотек представлены в таблице. Сравнение производится по двум характеристикам: точность определения категории текста и время обработки заданной выборки. Для каждого классификатора входными данными являлась выборка из 4 000 строк набора данных RuSentiment. Полученные результаты позволяют выбрать модель из библиотеки Dostoevsky в качестве классификатора тональности публикаций, так как она отличается наибольшим быстродействием при достаточно высокой точности.

ТАБЛИЦА. Сравнительная характеристика моделей анализа тональности текста

Библиотека	Модель	Точность	Время (сек)
Dostoevsky	FastText + DNN	0.847	0.807
DeepPavlov	BERT	0.842	568.18
	Conversational RuBERT	0.891	605.38
	FastText + CNN	0.92	41.65
	ELMo + CNN	0.839	1049.35
	FastText + BiGRU	0.793	31.96

В качестве одного из признаков определения потенциально деструктивных воздействий сообществ в социальных сетях на основе машинного

обучения предлагается метрика тональности текста публикаций сообщества. Публикация в социальной сети (*post*) представляет собой пару из оригинального контента владельца страницы (*post*) и цитируемого контента другого владельца (*repost*): *post* = (*post, repost*). Обозначим тональность текстовой публикации как *S*(*post*), значение которой лежит в ограниченном списке категорий или некотором интервале оценки. В данном исследовании используются следующие категории тональности: позитивная (+1), негативная (−1) и нейтральная (0), так что $S(post) \in \{-1, 0, +1\}$. Владелец страницы (пользователь или сообщество) U публикует серию постов $P^U = \{post_1, post_2, ..., post_n\}$, где n – количество постов. Для данного набора соответствующее множество оценок тональности текста модет быть обозначено как $S(P^U) = \{S(post_1), S(post_2), ..., S(post_n)\}$, где $S(post_k) \in \{-1, 0, +1\}$, $k \in [1, n]$.

Интегральная метрика тональности постов SP^U определяется как: $SP^U = \frac{1}{n}\sum_{k=1}^{n} S(post_k)$.

$SP^U \in [-1, +1]$, где $SP^U = -1$ характеризует абсолютную негативную тональность, $SP^U = +1$ – абсолютно позитивную тональность. Значения SP^U, близкие к 0, говорят о нейтральной тональности текста постов. На текущий момент учитывается текст публикаций, которые содержат только оригинальную публикацию или только цитируемый контент, поскольку вопрос их совместного оценивания требует дополнительного изучения.

В качестве входных данных для эксперимента использовалось 162,607 текстовых публикаций 244 сообществ ВК. Выбранная модель Dostoevsky обучалась на наборе данных RuSentiment для классификации постов на пять классов: негативные, позитивные, нейтральные, речь и неопределено. По результатам большинство постов (130 250) были отнесены к классу «нейтральные». Также были проанализированы отношения между популярностью текстовых публикаций (отношение количества просмотров к количеству отметок «мне нравится») и их тональностью. Отметим, что публикации, отнесенные к классам «негативные» и «позитивные», оказались популярнее нейтральных постов. Т. о. можно заключить, что тональность публикации влияет на ее восприятие пользователями.

Для анализа предложенного показателя тональности сообществ было выбрано 200 публикаций из 212 сообществ (из исходного набора данных были исключены сообщества с небольшим количеством публикаций и публикации, отнесенные к классу «неопределено»). Отметим, что полученное распределение предложенного показателя тональности оказалось близким к нормальному. На основе полученного распределения предлагается вести следующие качественные значения для интегрального показателя тональности сообщества: положительная тональность, если $SP > 0.1$, отрицательная тональность, если $SP < -0.1$, и нейтральная тональность, если $-0.1 \leq SP \leq 0.1$. Отметим, что среди выбранных 212 сообществ большинство получили

нейтральную интегральную оценку тональности. При этом количество сообществ с положительной интегральной оценкой больше, чем с отрицательной.

В дальнейших исследованиях предполагается использовать предложенный интегральный показатель тональности как дополнительный признак для обучения классификатора сообществ с точки зрения потенциальных деструктивных воздействий.

Работа выполнена при финансовой поддержке РФФИ (проект 18-29-22034 мк).

Список используемых источников

1. Браницкий А. А., Котенко И. В., Федорченко Е. В. Методика классификации сообществ в социальных сетях с использованием нейронных сетей // Актуальные проблемы инфотелекоммуникаций в науке и образовании. X Юбилейная Международной научно-технической и научно-методической конференции : сб. науч. ст. в 4 т. СПб.: СПбГУТ, 2021. С. 100–103.

2. Социальная сеть vkontakte. URL: https://vk.com (дата обращения: 30.03.2022).

3. Кабанов М. М., Незнанов Н. Г. Очерки динамической психиатрии: Транскультуральное исследование. СПб.: Институт им. В. М. Бехтерева, 2003. 438 с.

4. Рубцова Ю. Автоматическое построение и анализ корпуса коротких текстов (постов микроблогов) для задачи разработки и тренировки тонового классификатора // Инженерия знаний и технологии семантического веба. 2012. Т. 1. С. 109–116.

5. Rogers A., RomanovA., Rumshisky A., Volkova S., Gronas M., Gribov A. RuSentiment: An enriched sentiment analysis dataset for social media in Russian // Proc. of the 27th international conference on computational linguistics. 2018. pp. 755-763.

6. Belchikov A. Russian language toxic comments. URL: https://www.kaggle.com/blackmoon/russianlanguage-toxic-comments (дата обращения: 15.03.22).

7. Burtsev M. S. Seliverstov A. V., Airapetyan R., Arkhipov M., Baymurzina D., Bushkov N., Zaynutdinov M. DeepPavlov: Open-Source Library for Dialogue Systems // ACL (4). 2018. pp. 122–127.

8. Wang B. Wang A., Chen F., Wang Y., Kuo C. C. J. Evaluating word embedding models: Methods and experimental results // APSIPA transactions on signal and information processing. 2019. Vol. 8. pp. 1–14.

УДК 543.42
ГРНТИ 81.93.29

СПОСОБЫ ЗАЩИТЫ ИНФОРМАЦИИ И ПРЕДОТВРАЩЕНИЯ НЕСАНКЦИОНИРОВАННОГО СЪЕМА ИНФОРМАЦИИ С ПОМОЩЬЮ ИСПОЛЬЗОВАНИЯ СПЕЦИАЛЬНОЙ АППАРАТУРЫ

М. А. Гаманова, Д. С. Клюев, А. О. Фролов

Поволжский государственный университет телекоммуникаций и информатики

При обеспечении комплексной защиты объектов информатизации необходимо обеспечение предотвращения утечки и перехвата конфиденциальной информации, а также защиты информации ограниченного доступа. Анализаторы спектра имеют лучшие характеристики для поиска и обнаружения закладных устройств, в том числе они используются для защиты информации в многоканальной системе передачи. Рассматриваемые анализаторы спектра используют метод гармонического анализа функции y(t), основанный на использовании дискретных анализаторов частотного спектра сигнала.

анализатор спектра, защита информации.

К одним из основных угроз безопасности информации ограниченного доступа относят утечку и перехват информации по техническим каналам, поэтому особо важно обеспечивать комплексную защиту помещений, предназначенных для конфиденциальных мероприятий [1].

К распространенным техническим средствам, которые используются для несанкционированного съема информации, относят закладные устройства (далее – ЗУ). Под ЗУ понимается некий ретранслятор, на вход которого подаётся сигнал с информацией, а на выходе – преобразованный сигнал в соответствии с условиями и характеристиками среды распространения.

Поиск и обнаружение ЗУ осуществляется визуально, а также с использованием специальной аппаратуры, которая определяет эффективность поиска ЗУ. Используя специальные технические средства и аппаратуру, такую как: индикаторы (детекторы) электромагнитного поля, радио-частотометры, сканирующие приемники, интерсепторы, анализаторы спектра, программно-аппаратные комплексы радио контроля, нелинейные локаторы, ренгеновские и рентгено-телевизионные комплексы, анализаторы проводных линий и другие, проводятся специальные технические проверки объектов информатизации и выделенных помещений.

Лучшими возможностями по поиску радиозакладок обладают анализаторы спектра. Помимо того, что они перехватывают излучения ЗУ, они также могут анализировать их характеристики, что является полезным свойством, в случае использования для передачи информации сложных видов сигналов.

Анализаторы спектра могут визуализировать и анализировать спектр сигнала, который представляет собой набор синусоидальных волн в конкретный момент времени. Благодаря использованию этого прибора можно увидеть распределение энергии по частотам и получить амплитудно-частотную характеристику сигнала.

Анализаторы имеют в своем составе встроенные AM/FM детекторы для прослушивания и идентификации ЗУ. Основные, доступные радиозакладки работают в диапазоне 60–108 МГц, 110–170 МГц, 350–450 МГц, что означает, что данные частоты необходимо перекрывать рабочим диапазоном частот анализатора. С помощью анализатора спектра удается получить частотный портрет сигнала за счет того, что принятый сигнал как бы последовательно просматривается специальным узкополосным фильтром, в результате чего данные выводятся на экран устройства.

Чтобы определить расстояние до ЗУ, в паре с анализатором спектра используется прибор, который в соответствии с изменениями спектральной диаграммы определяет примерное местонахождение ЗУ. Совместное использование данных устройств позволяет получение детального анализа спектров обнаруженных радиосигналов, благодаря чему становится возможным определение нахождения источника сигнала в как в выделенном помещении, так и вне него. Анализатор должен иметь звуковой выход для стыковки с прибором, чтобы было удобнее определять расстояния до радиомикрофона.

К одним из методов обнаружения ЗУ относится сравнение спектров сигналов, зафиксированных до включения тестового акустического сигнала в защищаемом помещении и после его включения. Если сканирующий приемник обнаруживает некий радиосигнал, то в данном помещении требуется отключить все источники сигналов и шумов, в результате чего образуется режим относительной тишины. Ответственный сотрудник запоминает вид спектра сигнала на экране измерительного устройства. Затем происходит включение тестового акустического сигнала. Если источник радиосигнала находится в обследуемом помещении, то на спектрограмме должно наблюдаться расширение спектра. Если сотрудник, проводящий обследование, на слух или же визуально может установить причинно-следственную связь между включением тестового акустического сигнала и изменением (расширением) спектра, то это говорит о том, что ЗУ находится в помещении. Ещё одним методом обнаружения ЗУ является детальный анализ спектра обна-

руженного сигнала и последующее выявление в его составе побочных электромагнитных излучений. Данные побочные электромагнитные излучения могут создаваться передатчиком, который находится на незначительном расстоянии от точки приема. Если известны спектры типовых радиозакладок, то задача их обнаружения значительно упрощается.

В таблице представлено сравнение моделей анализаторов спектра разных производителей по их техническим характеристикам [2].

ТАБЛИЦА. Сравнительный анализ моделей анализаторов спектра

Характеристика	Модель		
	Anritsu MS2090A-0754	Anritsu MS2830A-045	Aaronia SPECTRAN V6-RSA2000X
Тип	Портативный	Лабораторный	Анализатор спектра реального времени
Частота	9 кГц – 54 ГГц	9 кГц – 43 ГГц	10 МГц – 6 ГГц, полоса 2×160 МГц, I/Q генератор
Разрешение (RBW)	1 Гц – 10 МГц	1 Гц – 10 МГц	0,062 Гц – 200 МГц
Амплитуда	От +30 дБм до −164 дБм	От +30 дБм до −153 дБм	От +23 дБм до −150 дБм
Шумы	−164 дБм	−164 дБм	−150 дБм
Полоса анализа реального времени	20 МГц, 50 МГц или 100 МГц	-	80 МГц, 120 МГц, 160 МГц или 245 МГц
Особенности	Демодуляция и анализ качества беспроводных стандартов связи: 5G и LTE.	Генерация, демодуляция и анализ беспроводных стандартов связи: LTE, GSM/EDGE, W-CDMA/HSPA+, TD-SCDMA, CDMA2000, EV-DO, HSDPA/HSUPA, Wi-MAX, WLAN (802.11), Bluetooth и другие	Непрерывная передача I/Q данных со скоростью до 784 МБ/с (через два USB 3).
Стоимость	От 600 тыс. руб.	От 1100 тыс. руб.	От 900 тыс. руб.

Помимо поиска и обнаружения электронных устройств перехвата информации анализаторы спектра также применяются для обеспечения защиты информации в многоканальной системе передачи (далее – МСП) и приема дискретных сообщений для идентификации каждого канала в соответствии с номером гармонического коэффициента Фурье и для защиты

передаваемой информации от ее несанкционированного разглашения в линии связи.

Существует несколько методов, на которых работают анализаторы частотного спектра для защиты информации. Один из таких методов – метод гармонического анализа функции $y(t)$, основанный на использовании дискретных анализаторов частотного спектра сигнала. С помощью этого приема становится возможным обеспечение достоверности результата защиты информации, которая передается по МСП, где каждому каналу передачи информации соответствует свой номер гармоники Фурье.

В данный методе используется аппроксимация анализируемой функции $y(t)$ с помощью тригонометрического полинома, который составлен из совокупности ступенек, квантованных по уровню и по времени (1).

$$y(t) = \frac{1}{2} A_0 + \sum_{j=1}^{j=n} (A_j \cos \frac{2\pi t}{T} j + B_j \sin \frac{2\pi t}{T} j), \text{ при } n < \frac{m}{2}, \quad (1)$$

где m – число ступенчатых значений $y(t_i) = y_i$ при условии, что квантование по времени протекает в соответствии с математическим выражением (2):

$$t_i = \frac{T}{m} i \text{ и } i = 0,1,2,...,m-1. \quad (2)$$

Каждому частотному каналу передачи информации соответствуют выделенные дискретным анализатором частотного спектра сигнала гармонические коэффициенты Фурье A_j и B_j. Формулы (3) и (4) определяют алгоритм вычисления коэффициентов Фурье, в данных формулах j является порядковым номером «дискретной» гармоники Фурье и условным номером канала связи МСП и приема информации.

$$A_j = \frac{2}{m} \sum_{i=0}^{i=m-1} y_i \cos \frac{2\pi i}{m} j. \quad (3)$$

$$B_j = \frac{2}{m} \sum_{i=0}^{i=m-1} y_i \sin \frac{2\pi i}{m} j. \quad (4)$$

A_j и B_j – косинусоидальный и синусоидальный гармонические коэффициенты тригонометрического полинома Фурье соответственно.

Защита информации в многоканальной системе связи с помощью известного дискретного анализатора частотного спектра осуществляется путем сохранения в тайне условного порядкового номера j «дискретной» гармоники Фурье и условного номера канала связи МСП и приема информации.

В частном случае, если $2n = m$, то даже при произвольном B_j (4) формулы (1) и (2) вместе с выражением (5)

$$A_n = A_{\frac{m}{2}} = \frac{1}{m} \sum_{i=0}^{i=m-1} y_i \cdot (-1)^i \quad (5)$$

дают полную тригонометрическую интерполяцию ступенчатых значений $y(t_i) = y_i$.

Недостатком способа защиты информации в МСП, основанного на дискретном анализаторе частотного спектра частотно-модулированного сигнала является то, что объем искажающей информации на передающей стороне достаточно мал, а именно: равен всего лишь числу сочетаний и перестановок порядкового номера *j* «дискретной» гармоники Фурье и условного номера канала связи. Вариации фазового сдвига гармоник Фурье не получится определить, так как наблюдается большая сложность вычисления сдвига фазы. В данном случае нет использования искажающего наложения случайных величин на передаваемый многочастотный сигнал МСП. Рассмотренный способ защиты информации с применением дискретного анализатора частотного спектра сигнала МСП способен обеспечить временную криптографическую стойкость, но для многих случаев на практике этого недостаточно.

В данной работе проведен сравнительный анализ финансово-экономических показателей и технических характеристик современных анализаторов, проведен анализ существующих методов работы анализаторов спектра. Необходимо разработать программно-аппаратные части экспериментального анализатора спектра, алгоритм работы которого будет основываться на дискретизации исследуемого сигнала, осуществляемой четным числом отрезков (шагов) с последующим выполнением гармонического анализа дискретных значений сигнала, при учете их значений в отдельности друг от друга на четных и нечетных номерах отрезков. С помощью данного алгоритма можно будет повысить криптографическую стойкость передачи информации, а также сократить время наблюдения анализируемой величины.

Список используемых источников

1. Ворона В. А., Костенко В. О. Способы и средства защиты информации от утечки по техническим каналам // Computational nanotechnology. 2016. С. 208–223.

2. Гаманова М. А., Демидов А. В., Клюев Д. С., Фролов А. О. Методы и средства поиска электронных устройств перехвата информации с использованием анализаторов спектра в защищаемом помещении // V Научный форум телекоммуникации: теория и технологии ТТТ-2021. «Физика и технические приложения волновых процессовФиТПВП-2021» : Материалы XIX Международной научно-технической конференции., Самара, 23–26 нояб. 2021 г. М., 2021. С. 133–134.

УДК 004.056
ГРНТИ 49.33.35

РАЗРАБОТКА МЕТОДА АНАЛИЗА ТРАФИКА БЕСПРОВОДНОЙ СЕТИ НА БАЗЕ WPA2 ENTERPRISE

Е. Ю. Герлинг, Е. А. Зебзеев, А. Ю. Киструга

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В настоящее время широко распространены технологии беспроводной передачи данных, в частности Wi-Fi. Одна из основных проблем заключается в обеспечении безопасной передачи, особенно в корпоративных сетях, где под угрозой находится конфиденциальная информация компании. Необходимый уровень защиты обеспечивает стандарт WPA2 Enterprise. Другим важнейшим аспектом обеспечения информационной безопасности является анализ трафика, позволяющий выявить аномальную активность и присутствие злоумышленников. В данной статье рассматривается метод анализа трафика беспроводной сети на базе WPA2 Enterprise. Использование данного стандарта защиты предполагает передачу трафика в зашифрованном виде, в связи с чем приводится подробный процесс его дешифрования.

WPA2 Enterprise, IEEE 802.1X, RADIUS, информационная безопасность, дешифрование трафика, анализ трафика, администрирование сети.

В настоящее время широко распространены технологии беспроводной передачи данных, в частности Wi-Fi. Многие компании делают свой выбор в пользу беспроводных сетей, которые предоставляют такие преимущества как мобильность и простота масштабируемости.

По данным аналитиков IDC, во втором квартале 2021 года мировой рынок оборудования для WLAN вырос на 4,6 % по сравнению с тем же периодом 2020 года [1]. Положительную динамику обеспечил именно корпоративный сегмент, где продажи увеличились на 22,4 % – до 1,7 млрд долларов.

В WLAN сетях генерируется и передается огромное количество данных. Одна из основных проблем заключается в обеспечении безопасной передачи данных, особенно в корпоративном сегменте, где под угрозой находится конфиденциальная информация компании. Необходимый уровень защиты обеспечивает стандарт WPA2 Enterprise, основой которого является аутентификация по стандарту IEEE 802.1X [2]. Использование данного стандарта предполагает наличие в сети структуры, представленной на рис. 1, которая состоит из трех компонентов: суппликант, аутентификатор и AAA сервер, в качестве которого может быть использован RADIUS-сервер [3].

Рис. 1. Структурная схема WPA2 Enterprise

В работе сетевого администратора могут возникать ситуации, в которых необходимо провести анализ беспроводного трафика, например, для выявления аномальной активности или присутствия в сети лиц, отправляющих вредоносные пакеты [4]. Данный случай был рассмотрен на примере экспериментального стенда, схема которого представлена на рис. 2. Перехват трафика между клиентом и аутентификатором осуществлялся на компьютере под управлением ОС Kali Linux, с помощью программы-анализатора трафика Wireshark. Для обеспечения возможности перехвата всех пакетов в беспроводной сети, Wi-Fi адаптер был переведен в режим monitor [5].

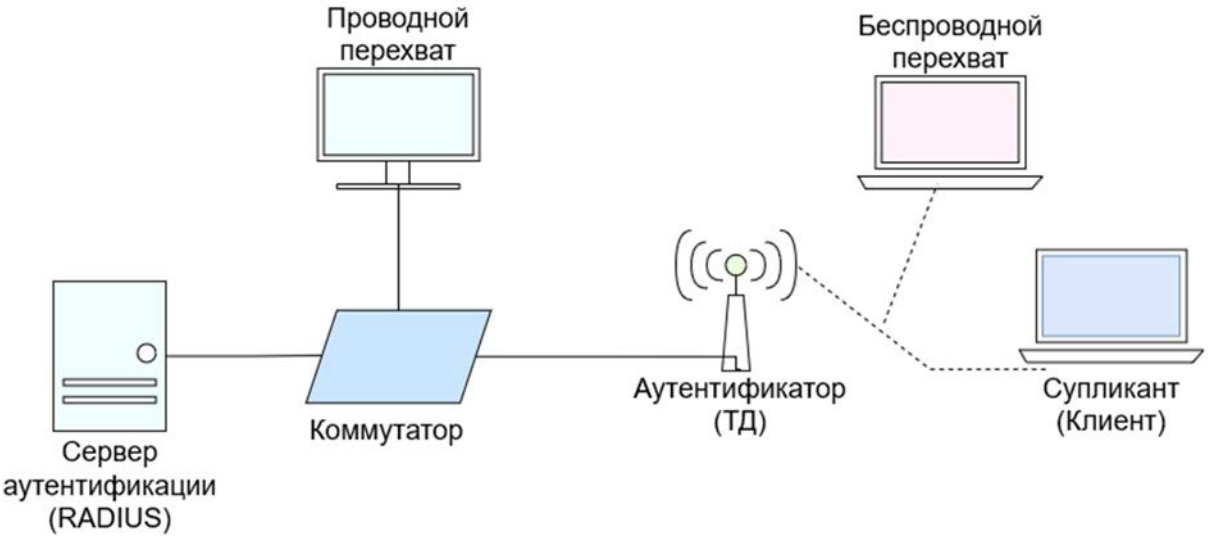


Рис. 2. Схема экспериментального стенда

На рис. 3 представлен перехваченный трафик. Провести его анализ невозможно в связи с тем, что в Wi-Fi сети данные не передаются в открытом виде [6].

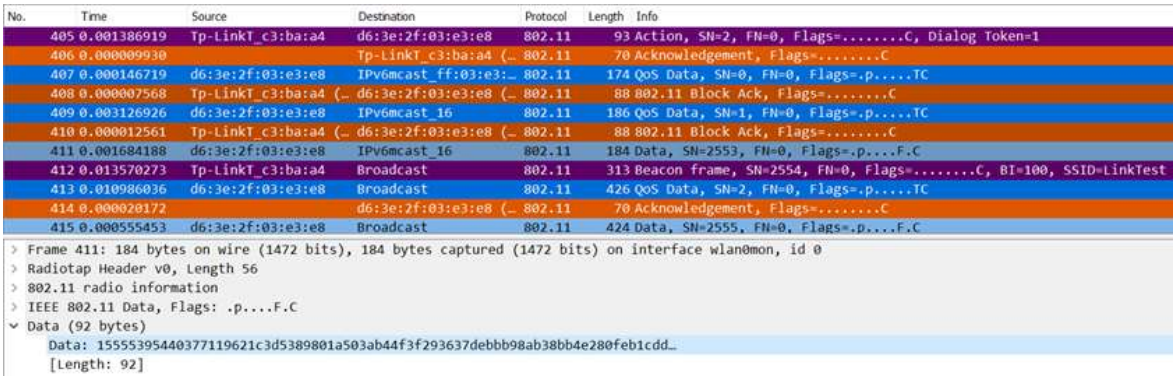


Рис. 3. Перехваченный трафик

Шифрование трафика WPA2 Enterprise делает подробный анализ невозможным. Именно поэтому в статье представлен метод, позволяющий дешифровать пакеты. Структуру метода, представленную на рис. 4, можно разделить на две части:

– Перехват трафика беспроводной сети;

– Перехват трафика проводной сети.

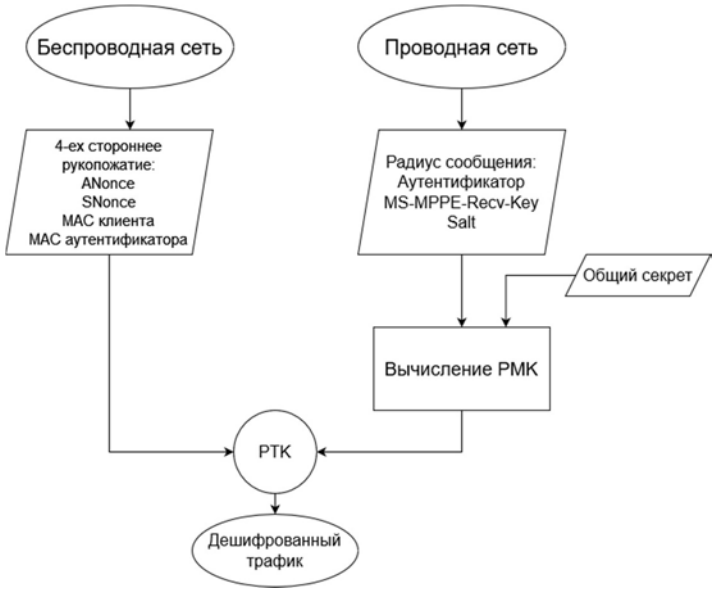


Рис. 4. Структура метода

В процессе аутентификации по стандарту IEEE 802.1X формируется PMK (*Pairwise Master Key*) – парный мастер ключ. Он генерируется в конце этапа взаимной аутентификации между клиентом и сервером аутентификации. После того как PMK сгенерирован, он участвует в вычислении парного передаточного ключа PTK с помощью псевдослучайной функции PRF-512. Затем из PTK выделяется 3 ключа: KCK (*Key Confirmation Key*) – Ключ подтверждения, KEK (*Key Encryption Key*) – Ключ шифрования ключа,

TK (*Temporal Key*) – Временный ключ. Именно TK используется для шифрования unicast трафика, следовательно, для дешифрования необходимо получить PTK [3].

Процесс вычисления PTK происходит в момент 4-х стороннего рукопожатия. Эта операция предназначена для того, чтобы в рамках стандарта WPA2 стороны убедились в том, что им известен одинаковый PMK ключ, выработали PTK, пришли к соглашению о выборе набора алгоритмов шифрования. Стоит понимать, что этот ключ создается заново для каждого нового соединения клиента с точкой доступа, соответственно и трафик для каждого соединения зашифрован разными PTK.

Дешифрование трафика можно начать с перехвата 4-х стороннего рукопожатия, который необходимо провести в момент подключения клиента к сети. В первом сообщении полученного рукопожатия есть псевдослучайное число ANonce, во втором сообщении содержится сгенерированное число SNonce, кроме того, известны MAC адреса клиента и аутентификатора.

Как было сказано ранее, для вычисления PTK также необходим PMK ключ. Алгоритм его формирования описан в документе RFC 2548 [7]. Именно поэтому, в отличие от WPA2-PSK (WPA2 Personal), в WPA2 Enterprise для выполнения дешифрования необходимо выполнить перехват RADIUS-сессии между аутентификатором и сервером аутентификации. Это позволит получить необходимые для вычисления PMK ключа значения:

1. Authenticator из последнего Access-Request запроса (далее R);
2. Атрибут MS-MPPE-Recv-Key из Access-Accept сообщения (далее M);
3. Поле Salt – первые два октета атрибута MS-MPPE-Recv-Key (далее A).

Кроме перехваченных значений, в вычислении используется заведомо известный сетевому администратору Shared key (общий секрет), который устанавливается на RADIUS сервере и аутентификаторе (далее S).

Формирование PMK происходит по представленному на рис. 5 алгоритму:

C = Длина(M) + M + Отступ
$C = c(1) + c(2) + \ldots + c(i)$

$b(1) = MD5(S + R + A)$	$p(1) = c(1)\ xor\ b(1)$	$P = p(1)$
$b(2) = MD5(S + c(1))$	$p(2) = c(2)\ xor\ b(2)$	$P = P + p(2)$
. . .		
$b(i) = MD5(S + c(i-1))$	$p(i) = c(i)\ xor\ b(i)$	$P = P + p(i)$

Результат: $P = p(1) + p(2) + \ldots + p(i)$

Рис. 5. Алгоритм формирования PMK

1. Создается строка (далее С) путем сложения (конкатенации) длины(М), М, отступа. Отступ необходим для того, чтобы общая длина стала кратным 16;

2. С разбивается на 16 октетов *c(1)*, *c(2)*, …, *c(i)*;

3. Создаются временные блоки *b(i)* равные *MD5* хешу от суммы *S*, *R*, *A* и равные *MD5* хешу от суммы *S*, *p(i-1)* при *i >1*;

4. Побитовым сложением *c(i)* и *b(i)* создаются блоки *p(i)*;

5. Блоки *p(i)* складываются, образуя тем самым PMK ключ.

При наличии перехваченного 4-х стороннего рукопожатия и вычисленного PMK ключа, можно рассчитать PTK ключ с помощью Wireshark. Для этого необходимо зайти в настройки протокола IEEE 802.11, включить дешифрование и указать полученный PMK в качестве ключа WPA-PSK, после чего программа рассчитает PTK и трафик будет расшифрован. Пример дешифрованного трафика представлен на рис. 6.

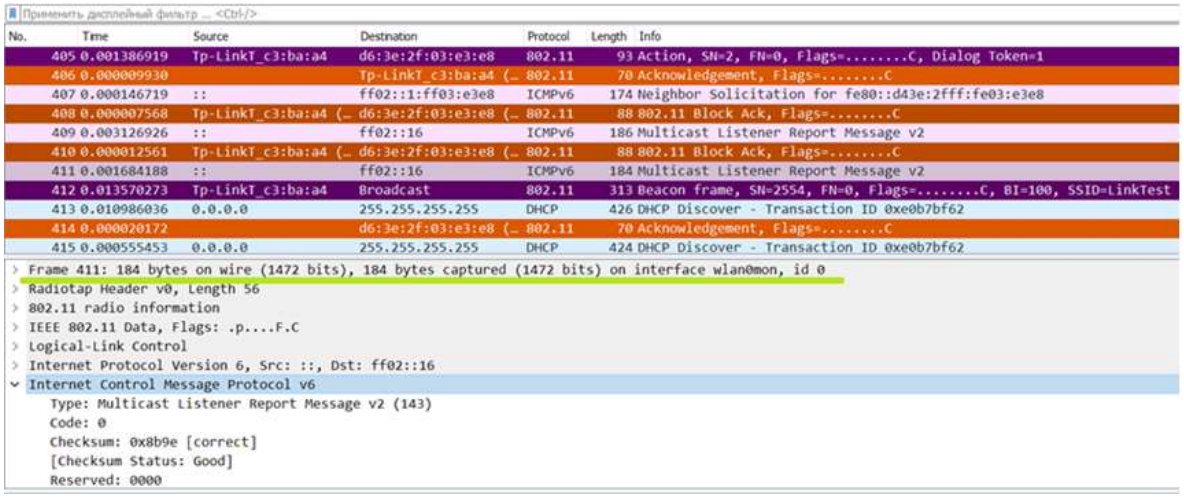


Рис. 6. Дешифрованный трафик

Полученный дешифрованный трафик позволяет определить, к какому протоколу относится пакет, рассмотреть его структуру и, следовательно, провести полный дальнейший анализ.

Таким образом, в статье представлен метод анализа трафика беспроводной сети на базе WPA2 Enterprise и приведен подробный процесс его дешифрования.

Список используемых источников

1. Worldwide Enterprise WLAN Market Continued Strong Growth in Second Quarter 2021, According to IDC. URL: https://www.idc.com/getdoc.jsp?containerId=prUS48217321&utm_medium=rss_feed&utm_source=alert&utm_campaign=rss_syndication (дата обращения 15.02.2022).

2. Докшин А. Д., Ковцур М. М., Прудников С. В., Таргонская А. И. Исследование подходов для аутентификации пользователей беспроводной сети с применением различных LDAP решений // Наукоемкие технологии в космических исследованиях Земли. 2021. Т. 13. № 3. С. 28–35.

3. Ковалев Д., Ковцур М. Механизмы аутентификации и управления ключами стандарта IEEE 802.11-2012 // Первая миля. 2014. № 3 (42). С. 72–77.

4. Kovtsur M., Kistruga A., Mikhailova A., Potemkin P., Volkogonov V. Research of wireless network traffic analysis using Big Data processing technology // The 13th international congress on ultra modern telecommunications and control systems. 2021. С. 115–121.

5. Ковцур М. М., Коновалова В. В., Мисливский Б. С., Михайлова А. В., Акилов М. В. Разработка методики удаленного мониторинга трафика в корпоративных сетях // Заметки ученого. 2021. № 6-1. С. 27–31.

6. Ковцур М. М., Герлинг Е. Ю., Коновалова В. В., Кистуга А. Ю. Исследование способов удаленного перехвата трафика в корпоративных сетях // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2021. № 4. С. 68–75.

7. RFC 2548, Microsoft Vendor-specific RADIUS Attributes, 1999.

УДК 004.057.5
ГРНТИ 20.53.23

ИССЛЕДОВАНИЕ ПРОИЗВОДИТЕЛЬНОСТИ ВЕБ-СЕРВЕРОВ ДЛЯ МАЛОМОЩНЫХ УСТРОЙСТВ НА БАЗЕ RASPBERRY OS

Е. Ю. Герлинг, И. А. Ковалев, А. Э. Фёдорова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Пандемия внесла свои коррективы в сложившуюся экономическую ситуацию в стране и мире, вследствие чего возросла популярность микроконтроллеров, спрос на которые растет с каждым днем. Растет спрос на решения для умного дома, систем безопасности и различных аппаратных устройств. Особенную популярность новые системы получают в условиях тренда импортозамещения. Достаточно часто возникает необходимость реализации пользовательского интерфейса, а соответственно и установки специализированного программного обеспечения для решения поставленных задач. В статье обозреваются известные методы развертывания и обслуживания веб-серверов на базе маломощных устройств, приводятся примеры существующих лучших практик в данной области, а также проводится анализ потенциальных возможностей выбора оптимального веб-сервера для развертывания инфраструктуры на базе маломощных устройств, таких как Raspberry.

веб-интерфейс, Raspberry , безопасность сетей.

Использование веб-приложений уже долгое время входит в повседневную жизнь многих людей. И с каждым годом такие приложения набирают всё большую популярность, так как для взаимодействия с ними пользователю необходимо использовать лишь браузер, который установлен по-умолчанию в большинство операционных систем. Это упрощает доступ к необходимым ресурсам, обеспечивает удобство взаимодействия через мобильное устройство, персональный компьютер или ноутбук.

В современном мире множество маршрутизаторов, коммутаторов, модемов и других маломощных сетевых устройств поддерживает управление и настройку через веб-интерфейс.

Устройства, обладающие ограниченными ресурсами, имеют ряд особенностей. Далее на примере одноплатного компьютера Raspberry приводятся отличительные характеристики таких устройств [1]. К ним относятся:

– ограничение в энергопотреблении;

– небольшой запас постоянной памяти;

– отсутствие возможности увеличить оперативную память;

– медленная производительность центрального процессора.

При разработке веб-интерфейса для маломощных систем требуется учитывать изложенные выше особенности, а также их влияние на работу необходимых сервисов.

Для демонстрации структуры решения используется виртуальная машина с операционной системой Ubuntu Server, обладающая 1 CPU и объёмом оперативной памяти равным 1 GB. Данные параметры идентичны характеристикам одноплатного компьютера Raspberry Pi 3 Model B.

В качестве веб-сервера выбран Apache HTTP-сервер, хотя существует великое множество других альтернативных решений, например, nginx, HAproxy и другие. Он представляет собой открытое программное решение, а также распространяется абсолютно бесплатно. Среди других преимуществ можно выделить тот факт, что его лицензия позволяет конечному пользователю редактировать исходный код, чтобы адаптировать Apache под собственные нужды. Следует отметить, что 2019 году web-сервер Apache вошёл в тройку лидеров рейтинга самых популярных веб-серверов в рунете [2].

В отличие от веб-сервера Internet Information Services, который работает только с Windows и поставляется в комплекте с этой операционной системой, и веб-сервера Nginx, который в свою очередь осуществляет лишь некоторую поддержку Windows, Apache является кроссплатформенным решением и

Рисунок. Структура веб-интерфейса

поддерживается на Windows, Linux, Unix и Mac OS в полной мере.

На рис. приведена структура вышеизложенного решения.

Для обеспечения безопасности полученного решения необходимо определить типы атак на веб-приложения [3]. К ним относятся:

– атаки на веб-сервер;

– атаки на базу данных;

– атаки на операционную систему.

Чтобы повысить уровень защиты веб-сервера необходимо совершать регулярные обновления Apache, отключить ненужные модули данного сервера, скрыть версию Apache и имя используемый операционной системы сервера, а также отключить список каталогов [4]. Также рекомендуется выполнять стандартные требования защиты информационной безопасности, такие как:

– отключение неиспользуемых портов;

– изоляция приложений, работающих на сервере;

– ограничение прав доступа приложений, работающих на сервере;

– создание отдельного пользователя для работы веб-приложения;

– грамотные настройки firewall;

– использование современных технологий, такие как nftables и SELinux.

Защитить от пассивного прослушивания веб-сервер позволяют SSL-сертификаты. Сертификат SSL – это популярный тип цифрового сертификата, который привязывает информацию о владельце веб-сервера к ключу шифрования. Эти ключи используются в протоколе SSL/TLS для создания безопасной сессии между браузером и веб-сервером, на котором расположен SSL-сертификат. Центры сертификации выдают множество типов сертификатов. Сертификаты, выданные центрами сетификации, обеспечивают безопасность транзакций на веб-сайте, защиту от вредоносных программ и проверку подлинности документов и обменов электронной почтой. Существует возможность использования самоподписанных сертификатов, но она не гарантирует клиентам, что сервер является именно тем сервером, который им нужен. Преимуществом самоподписанных сертификатов является их бесплатность [5]. В современном мире самоподписанный сертификат сделать очень легко: достаточно использовать в своей LetsEncrypt и установить самоподписанный сертификат. Преимуществом данного современного подхода является не только свобода реализации, упрощенная поддержка последних решений в области информационной безопасности и бесплатное использование, но и возможность полноценно автоматизировать выдачу сертификатов в своей системе для поддержания принципов DevSecOps и автоматического внедрения лучших практик информационной безопасности в соответствии с самыми современными методологиями такими как DevOps.

В общем и целом, в рамках лирического отступления к очень связанной с веб-серверами темой DevOps методологии, будет важным отметить несколько моментов. Методология DevOps и DevSecOps были созданы для предотвращения всевозможных препятствий между двумя сторонами разработки и администрирования. Команды разработки и администраторов работают вместе друг с другом и роли этих участников объединяются в методологии DevOps [6].

Производительность веб-сервера можно продемонстрировать с помощью специального программного обеспечения, такого как top, htop, bashtop и тому подобные программные продукты, реализующие функциональность диспетчера задач. Такие решения могут отображать нагрузку на центральный процессор, расход оперативной памяти, визуализировать полученные значения для удобного отображения соответствующих параметров по графическим инструментам с конкретными датами, для точного наблюдения потребления ресурсов в разные моменты активности функционирования веб-серверов. Также имеется возможность наблюдать простой центрального процессора, процент потребления памяти, «украденного» гипервизором, загрузку каждого ядра центрального процессора, его температуру, температуру графического чипа и так далее.

В общем и целом, существует возможность просматривать каждый возможный параметр всех минимальных схемотехнических единиц устройства аппаратного обеспечения. По статистическим данным веб-сервера потребляют крайне малый процент мощности, относительно потребляемых ресурсов приложения, которое обслуживает конкретный сервер. Другими словами, имеет смысл прежде всего смотреть на потребление ресурсов приложением, обслуживаемым сервером, а затем на потребление ресурсов самого сервера, которое будет крайне невелико по сравнению с потреблением обслуживаемого приложения.

Подводя итог вышеизложенному, следует отметить, что разработка и сопровождение веб-приложения для системы, развёрнутой на маломощном устройстве, является трудоёмким процессом и требует учитывать различные особенности работы веб-серверов при ограниченных ресурсах и дополнительно анализировать решения, выбранные для реализации данного сервиса.

Список используемых источников

1. Габуев А. Г., Красов А. В., Ощенков Ф. Д., Тарасов Н. М. Анализ защищённости современных средств передачи информации посредством портативной лаборатории на основе микрокомпьютера Raspberry Pi // Актуальные проблемы инфотелекоммуникаций в науке и образовании. IX Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2020. С. 295–298.

2. Ковцур М. М., Горлов С. Е., Таргонская А. И., Ушаков И. А. Модуль аутентификации пользователей для веб-приложения. Свидетельство о регистрации программы для ЭВМ 2021619744, 16.06.2021. Заявка № 2021618748 от 03.06.2021.

3. Ахрамеева К. А., Ковцур М. М., Михайлова А. В. Обеспечение информационной безопасности баз данных web-приложений // Актуальные проблемы инфотелекоммуникаций в науке и образовании. IX Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2020. С. 107–110.

4. Ковцур М. М., Луеке П. Э. Разработка системы учёта посещаемости студентов масштаба вуза // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VIII Международной научно-технической и научно-методической конференция : сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2019. С. 532–537.

5. Герлинг Е. Ю., Ковцур М. М., Фёдорова А. Э. Разработка веб-интерфейса для системы мониторинга беспроводных сетей семейства IEEE 802.11 // Актуальные проблемы инфотелекоммуникаций в науке и образовании. X Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2021. С. 224–228.

6. Ковцур М. М., Казаков Н. И., Коновалова В. В. Исследование подходов интеграции мессенджеров с корпоративными информационными системами // Методы и технические средства обеспечения безопасности информации. 2020. № 29. С. 64–66.

7. Герлинг Е. Ю., Горлов С. Е., Кириллов Д. И. Обеспечение информационной безопасности при разработке web-приложений // Актуальные проблемы инфотелекоммуникаций в науке и образовании. IX Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2020. С. 326-330.

Статья представлена заведующим кафедрой ЗСС СПбГУТ, кандидатом технических наук, доцентом А. В. Красовым.

УДК 621.39, 530.182
ГРНТИ 49.44.31

ПОДДЕРЖАНИЕ КВАЗИСОЛИТОННОГО РЕЖИМА В ВОСС С ИСПОЛЬЗОВАНИЕМ УСИЛИТЕЛЕЙ РАМАНА

С. Ф. Глаголев, С. Э. Доценко

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В работе рассмотрен метод поддержания квазисолитонного режима в многопролетных волоконно-оптических системах связи с использованием одномодовых оптических волокон с потерями и усилителей Рамана со встречной и двунаправленной накачкой. Проведены теоретические расчеты и моделирование в программе OptiSystem процессов распространения квазисолитонных импульсов на отдельных усилительных

участках (пролетах) и в системе связи в целом. Сопоставлены результаты теоретических расчетов с результатами моделирования и показаны преимущества двунаправленной накачки.

солитон, квазисолитонный режим, оптический усилитель Рамана, одномодовое оптическое волокно, хроматическая дисперсия, фазовая самомодуляция.

Данная статья продолжает работы [1, 2], посвящённые применению оптических усилителей (ОУ) EDFA и ВКР для поддержания квазисолитонного режима распространения сигналов в магистральных волоконно-оптических системах связи (ВОСС).

Моделирование ВОСС с ОУ Рамана и встречной накачкой

Рассмотрим упрощенную схему одноканальной ВОСС (рис. 1), состоящую из двух оконечных пунктов (ОП), содержащих передающий ТХ и приемный RX транспондеры ТР, и нескольких усилительных участков (УУ) с ОУ Рамана. Для поддержания квазисолитонного режима на УУ в одномодовом оптическом волокне (ОМ ОВ), на его выход через направленный ответвитесь (НО) подается непрерывное излучение от источника встречной накачки (ИН) с частотой превышающей на 13 ТГц несущую частоты сигнала [3]. Излучение накачки отдает свою энергию усиливаемому сигналу.

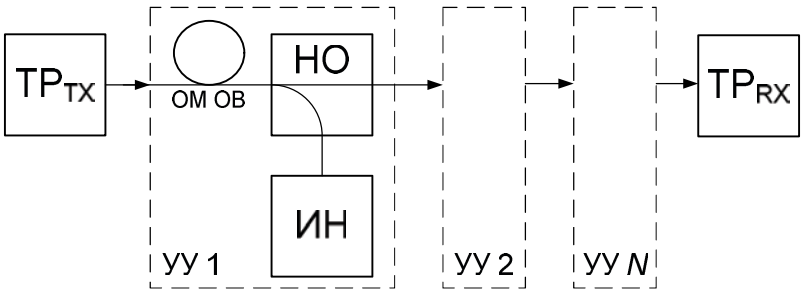


Рис. 1. Схема ВОСС с ОУ Рамана и встречной накачкой

Приведем параметры необходимые для расчета и моделирования ВОСС: скорость передачи B = 10 Гбит/с, длина волны λ = 1 550 нм, длительность секансного импульса на уровне половины амплитуды t_u = 0.2 бит, длина УУ L_A = 40–140 км. Применялось ОМ ОВ типа DSF с параметрами: коэффициент затухания α = 0.22 дБ/км на длине волны λ = 1 550 нм, коэффициент хроматической дисперсии (ХД) D_x = 1 пс/(км·нм), дисперсия групповых скоростей (ДГС) $\beta_2 = -1.275$ пс/нм^2, крутизна дисперсионной характеристики S_x = 0.085 пс/нм^2/км, эффективная площадь модового поля A_{ef} = 41 мкм^2, нелинейный показатель преломления $n_2 = 26 \cdot 10^{-21}$ м^2/Вт, коэффициент нелинейности γ = 2.571 1/(Вт·км). Длина волны накачки ОУ Рамана λ_p = 1 450 нм, мощность накачки P_p = 18–22 дБм, подбиралась экспериментально.

Проведем расчеты полуширины секансного импульса $T_0 = t_u/1.763 = 11.34$ пс. Мощность, необходимая для поддержания солитонного режима в ОВ без потерь $P_{ФmT} = -\beta_2/(\gamma \cdot T_0^2) = 3.9$ мВт. Дисперсионная длина $L_D = T_0^2/(-\beta_2) = 100.8$ км [3].

Моделирование процессов распространения секансных импульсов по ОМ ОВ без потерь показало, что для реализации солитонного режима пиковая мощность должна быть увеличена с 3.9 до 4.7 мВт.

Рассмотрим один УУ длиной L_A многопролетной ВОСС со встречной накачкой. Будем учитывать коэффициент затухания α и усилительную способность $g(z)$ реального ОМ ОВ. Для изменения пиковой мощности сигнала $P_m(z)$ на малом участке dz ОМ ОВ можно записать дифференциальное уравнение (ДУ) [3, 4]

$$\frac{dP_m(z)}{dz} = [g(z) - \alpha] \cdot P_m(z). \quad (1)$$

Отметим, что величина $g(z)$ зависит от z и определяется уровнем накачки в этой точке. В конце УУ при $z = L_A$ уровень накачки и $g(L_A)$ максимальны. При $g(z) < \alpha$, пиковая мощность уменьшается, а при $g(z) > \alpha$ возрастает.

Хотя в каждой точке ОМ ОВ невозможно компенсировать потери, но можно скомпенсировать общее затухание на УУ длиной L_A при условии

$$\int_0^{L_A} g(z) \cdot dz = \alpha \cdot L_A. \quad (2)$$

Пренебрегая истощением накачки, запишем упрощенное выражение для изменений $g(z)$ на УУ

$$g(z) = g_0 \cdot \exp\left[-\alpha_p \cdot (L_A - z)\right], \quad (3)$$

где α_p – коэффициент затухания ОМ ОВ для накачки, $g_0 = g(L_A)$ – максимальная усилительная способность ОУ ВКР.

Запишем уравнение (4) для изменений пиковой мощности сигнала в пределах УУ, решив уравнение (1) с учетом (3) для такой мощности накачки, которая обеспечивает требуемое значение g_0 и при которой пиковая мощность на выходе УУ соответствует входной $P_{0m} = P_m(L_A)$ [3]

$$P_m(z) = P_{0m} \cdot \exp\left\{\alpha \cdot \left[L_A \cdot \left[\frac{\exp(\alpha_p \cdot z) - 1}{\exp(\alpha_p \cdot L_A) - 1}\right] - z\right]\right\} = P_{0m} \cdot p(z). \quad (4)$$

Пиковая мощность входных импульсов P_{0m} должна быть больше мощности фундаментального солитона $P_{mФ}$ в ОМ ОВ без потерь [1–3]

$$P_{0m} = P_{m\Phi}/p_0, \quad p_0 = (1/L_A) \cdot \int_0^{L_A} p(z) \cdot dz, \qquad (5)$$

где p_0 – среднее значение нормализованной пиковой мощности излучения на УУ.

Рассчитанные по (5) значения p_0 и P_{0m}, приведены в табл. 1.

ТАБЛИЦА 1. Результаты расчетов p_0 и P_{0m} для различных L_A

L_A, км	40	60	80	100	120
p_0	0.736	0.542	0.391	0.290	0.226
P_{0m}, мВт	6.384	8.674	12.01	16.187	20.817

При моделировании длина УУ варьировалась от 40 до 120 км, а их количество от 2 до 16. Общая длина линии достигала 1 920 км. Результаты моделирования приведены ниже.

ВОСС с ОУ Рамана и двунаправленной накачкой

На рис. 2 показана упрощенная схема многопролетной ВОСС, использующая ОУ Рамана с двунаправленной накачкой. Обозначения на схеме аналогичны рис. 1, а исходные данные те же, что в предыдущем разделе.

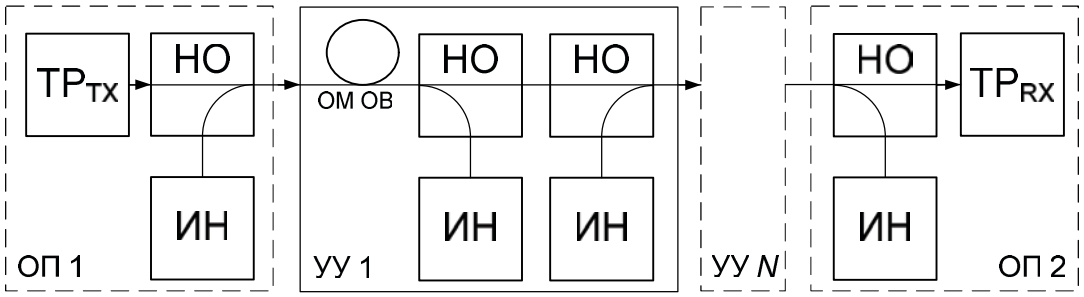


Рис. 2. Схема ВОСС с ОУ Рамана и двунаправленной накачкой

Выражения (1) и (2) справедливы и для УУ при двунаправленной накачке. Для изменений $g(z)$ на УУ вместо (3) можно записать упрощенное выражение

$$g(\mathrm{z}) = g_1 \cdot \exp(-\alpha_p z) + g_2 \exp[-\alpha_p (L_A - z)],$$

где g_1 и g_2 связаны с мощностями попутной и встречной накачек.

Считая, что мощности встречной и попутной накачки равны g_0, запишем уравнение (6) зависимости мощности секансных ОИ на УУ для двунаправленной накачки [3, 4]

$$P_m(z) = P_{0m} \cdot \exp\left\{\alpha L_A \left(\frac{sh[\alpha_p(z-L_A/2)]+sh(\alpha_p L_A/2)}{2 \cdot sh(\alpha_p L_A/2)}\right) - \alpha z\right\} = P_{0m} \cdot p(\mathrm{z}). \quad (6)$$

Определим p_0 и P_{0m} по выражениям (5) и поместим в табл. 2.

ТАБЛИЦА 2. Результаты расчетов p_0 и P_{0m} для разных L_A

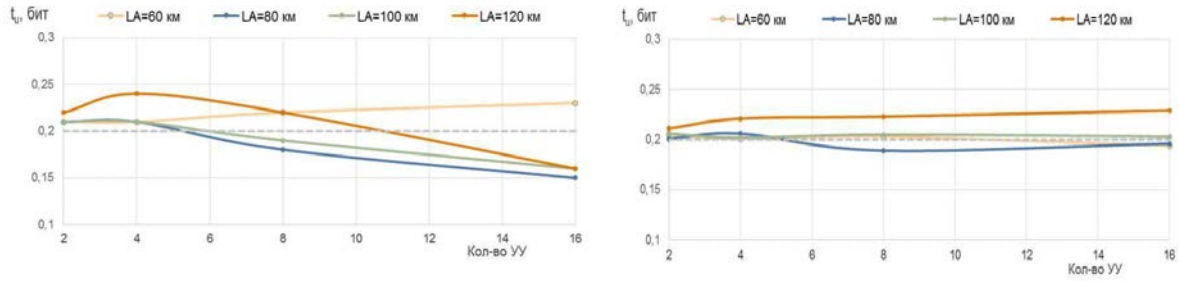
L_A, км	40	60	80	100	120	140
p_0	1.001	1.009	1.037	1.106	1.239	1.463
P_{0m}, мВт	4.7	4.66	4.53	4.25	3.79	3.21

Из табл. 2 видно, что с увеличением L_A требуемая пиковая мощность становится даже меньше мощности $P_{m\Phi}$, необходимой для формирования фундаментального солитона.

При моделировании длина УУ варьировалась от 40 до 140 км, а их количество от 2 до 16. Общая длина линии достигала 2 240 км.

Результаты моделирования

На рис. 3, представлены изменения длительности выходного импульса в зависимости от количества УУ различной длины.



а б

Рис. 3. Изменение длительности выходного импульса для встречной (а) и двунаправленной (б) накачки

Из рис. 3 видно, что квазисолитонный режим позволяет сохранить на больших расстояниях диапазон изменения длительности импульсов в пределах от 0.25 до 0.15 бита при встречной накачке и от 0.23 до 0.18 бит при двунаправленной накачке.

На рис. 4 представлены изменения пиковой мощности выходного импульса в зависимости от количества УУ различной длины. Видно, что при встречной накачке требуемые значения входной пиковой мощности очень сильно зависят от длины УУ. Выходная пиковая мощность также сильно зависит от количества УУ и их протяженности. При двунаправленной накачке требуемая входная мощность мало зависит от длины УУ, а выходная мощность мало изменяется при увеличении количества участков.

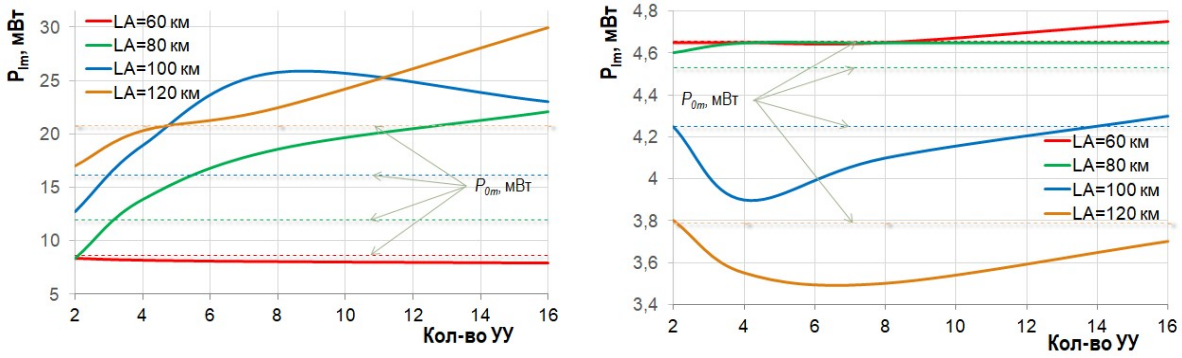


Рис. 4. Изменение пиковой мощности выходного импульса для встречной (а) и двунаправленной (б) накачки

Выводы

•В статье продемонстрирована возможность поддержания квазисолитонного режима ВОСС с ОУ Рамана со встречной и двунаправленной накачками. Показаны значительные преимущества использования двунаправленной накачки по сравнению со встречной, позволяющие значительно увеличить длину УУ и общую протяженность ВОСС между регенераторами (транспондерами).

•Обнаружено расхождение в определении мощности требуемой для формирования фундаментального солитона в ОМ ОВ без потерь по теоретическому выражению и результату моделирования. Для объяснения этого требуются дополнительные исследования.

Список используемых источников

1. Глаголев С. Ф., Горсков В. С., Доценко С. Э. Использование оптических усилителей EDFA для поддержания квазисолитонного режима распространения сигналов по одномодовым волокнам со смещенной дисперсией // Актуальные проблемы инфотелекоммуникаций в науке и образовании. X Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2021. Т. 1. С. 228–234.

2. Глаголев С. Ф., Горсков В. С., Доценко С. Э. Использование ВКР усилителей для поддержания квазисолитонного режима в одномодовых волокнах со смещенной дисперсией // Актуальные проблемы инфотелекоммуникаций в науке и образовании. X Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2021.. Т. 1. С. 234–239.

3. Андреева Е. И., Былина М. С., Глаголев С. Ф., Доценко С. Э., Чаймарданов П. А. Свойства временных оптических солитонов в оптических волокнах и возможность их использования в телекоммуникациях. Части 1-4 // Труды учебных заведений связи. 2018–2019. Т. 4, № 1-3. Т. 5, № 1.

4. Агравал Г. Нелинейная волоконная оптика. М.: Мир, 1996. 323 с.

5. Кившарь Ю. С., Агравал Г. П. Оптические солитоны. От волоконных световодов до фотонных кристаллов. М.: ФИЗМАТЛИТ, 2005. 648 с.

УДК 681.7.068, 535.32
ГРНТИ 49.44.31

ИССЛЕДОВАНИЕ ВЛИЯНИЯ ХРОМАТИЧЕСКОЙ ДИСПЕРСИИ В ОДНОМОДОВЫХ ОПТИЧЕСКИХ ВОЛОКНАХ НА ИМПУЛЬСЫ РАЗЛИЧНОЙ ФОРМЫ

С. Ф. Глаголев, С. Э. Доценко, Г. Ю. Соколов, Е. А. Юдина

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Данная работа посвящена проверке и уточнению известных инженерных формул для расчета длительности и пиковой мощности нечирпированных оптических импульсов с формой гаусса и гиперболического секанса, прошедших значительное расстояние по одномодовому оптическому волокну с известными коэффициентами хроматической дисперсии и затухания. Работа ограничена рассмотрением процессов только в волоконно-оптических системах связи с бинарной амплитудной модуляцией и кодированием с возвратом к нулю. Нелинейные явления и поляризационно-модовая дисперсия в ОВ в этой работе не учитываются.

одномодовое оптическое волокно, коэффициент хроматической дисперсии, гауссовский импульс, импульс с формой гиперболического секанса.

Хроматическая дисперсия в одномодовых ОВ

Хроматическая дисперсия (ХД) в одномодоых оптических волокнах (ОВ) – это хорошо исследованное явление, при котором разные спектральные компоненты импульса длительностью t_u на уровне половине амплитуды распространяются с разными групповыми скоростями [1–3]. Полную ХД в ОВ принято разделять на две составляющие: материальную и волноводную, а коэффициент ХД D_x, состоящим из суммы двух соответствующих слагаемых D_m и D_v.

Материальная составляющая ХД D_m обусловлена зависимостью от длины волны λ групповых показателей преломления $n_g(\lambda)$ материалов, из которых изготавливаются телекоммуникационные ОВ (обычно это SiO_2 с учетом легирующих добавок). Зависимость $D_m(\lambda)$ мало зависит от типа ОВ и профиля показателя преломления (ППП). Зависимость волноводной составляющей ХД обусловлена конструкцией волновода, т. е. ППП. Она может изменяться в широких пределах.

ХД проявляется в расширении коротких оптических импульсов, уменьшении пиковой мощности и возникновении паразитной частотной внутриимпульсной модуляции (чирпинга) при прохождении импульсов по ОВ на расстояние z. Чем короче импульс, тем больше ширина его спектра $\Delta\lambda$ и тем больше расширение импульса. Для теоретического расчета длительности

спектрально ограниченных гауссовских импульсов t_{uz} на уровне половины амплитуды для расстояния z обычно используется выражение [2]

$$t_{uz} = t_{u0} \cdot \sqrt{1 + \left(\left|D_x\right| \cdot \Delta\lambda \cdot z / t_{u0}\right)^2}\,, \qquad (1)$$

где t_{u0} – длительность импульса на входе в ОВ.

В этом выражении не учитывается начальный чирпинг C_0, входящих в ОВ импульсов, и не вполне понятна величина $\Delta\lambda$, т. е. ширина спектра импульсов.

Параметры гауссовских и секансных оптических импульсов

Запишем выражения для зависимости мощности от времени (рис. 1а) для импульсов гауссовской формы

$$P_0(t) = P_{m0} \cdot exp\left(-t^2 / T_0^2\right),$$

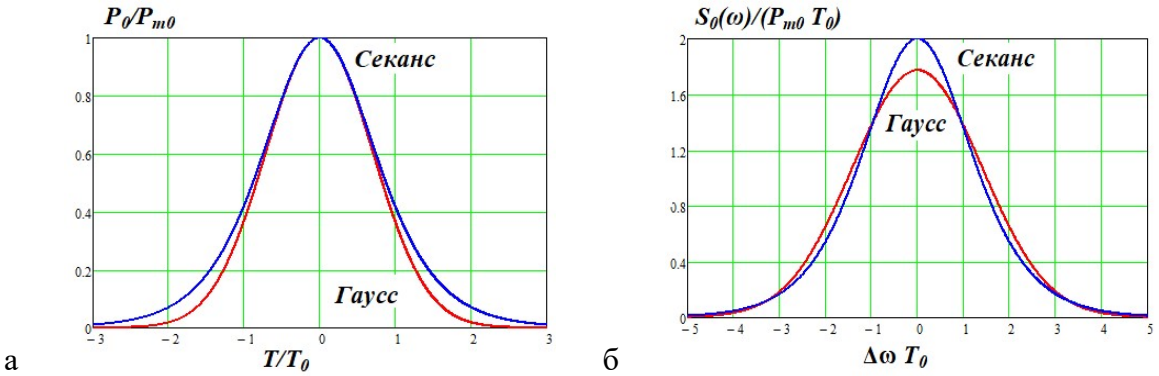
и для импульсов, имеющих форму гиперболического секанса

$$P_0(t) = P_{m0} \cdot \left[sech\left(t / T_0\right)\right]^2,$$

где P_{m0}, T_0 – пиковая мощность и каноническая полуширина импульсов.

Если импульсы формируется из монохроматического излучения с частотой ω_0 их называют спектрально ограниченными. Например, для гауссовского спектрально ограниченного импульса справедливо $\Delta\omega_0 = 1/T_0$.

На рис. 1а приведена форма нормализованных гауссовского и секансного импульсов с полушириной T_0. Было выполнено прямое преобразование Фурье для этих импульсов и построены графики их нормализованных спектров (рис. 1б).



а б

Рис. 1. Нормализованные формы (а) и спектры (б) гауссовского и секансного импульсов

В табл. приведены результаты расчетов нормализованных спектральных параметров гауссовского и секансного импульсов.

ТАБЛИЦА. Нормализованные параметры гауссовского и секансного импульсов

Форма импульса	Ширина импул. на уровне 0.5	Ширина спектра на уровне 0.5	Ширина эквивалентного спектра прямоугольной формы	Максим. нормализованная спектральная плотность
Гаусс	1.66 T_0	3.32 $\Delta\omega$ T_0	3.545 $\Delta\omega$ T_0	$\pi^{0.5} = 1{,}772$
Секанс	1.76 T_0	2.78 $\Delta\omega$ T_0	3.141 $\Delta\omega$ T_0	2

Видно, что гауссовский и секансный импульсы мало отличаются по форме и по спектру.

Для инженерных расчетов зависимости мощности гауссовских спектрально ограниченных импульсов, распространяющихся по одномодовым ОВ, от длины z и внутриимпульсного времени T с учетом коэффициентов затухания α и ХД D_x можно использовать выражение [2]

$$P_z(T) = P_{m0} \cdot \exp\left(-\frac{T^2}{T_0^2 \cdot \left[1+\left(z/L_D\right)^2\right]}\right) \cdot \frac{1}{\sqrt{1+\left(z/L_D\right)^2}} \cdot \exp\left(-\alpha \cdot z\right), \qquad (2)$$

где $P_{m0}=I_{m0}\,A_{ef}$ – пиковая мощность гауссовского импульса на входе в ОВ, I_{m0} – пиковая интенсивность входного излучения на оси ОВ, $A_{ef} = \pi \cdot r_{pm}^2$ – эффективная площадь модового поля, r_{pm} – радиус модового поля ОВ, $T = t\text{-}z/V_g$ – внутриимпульсное время, отсчитываемое от положения вершины импульса на оси времени, V_g – групповая скорость распространения гауссовских импульсов, $L_D = T_0^2/|\beta_2|$ – дисперсионная длина ОВ.

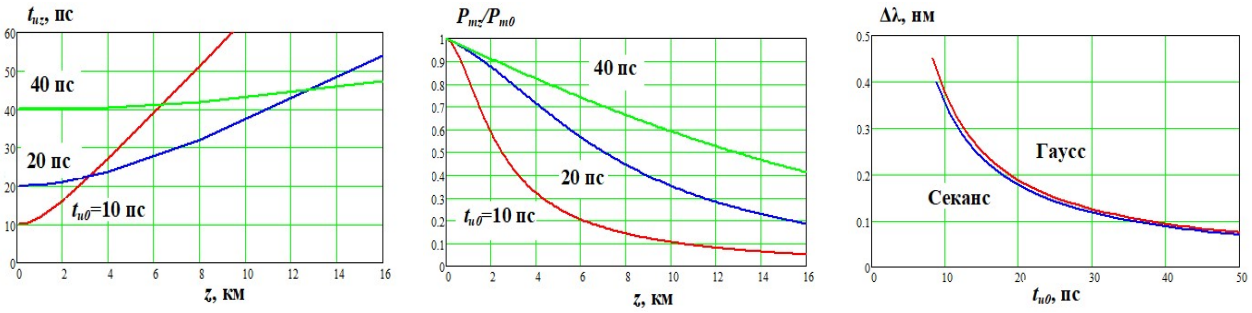
Из (2) видно, что гауссовский импульс при распространении по ОВ сохраняет гауссовскую форму, но расширяется и уменьшается по амплитуде с увеличением расстояния z. Причем уменьшение амплитуды связано не только с коэффициентом затухания α, но и с параметром ХД L_D.

В нашей работе мы использовали формулы (1) и (2) для расчетов не только для гауссовских, но и для спектрально ограниченных секансных импульсов. Корректность такого подхода проверялась экспериментально.

Отметим, что в выражение (1) входит ширина спектра импульса $\Delta\lambda$, которую можно определить по-разному (см. табл.), но тогда результаты расчета будут неоднозначными. Критерием правильности выбора $\Delta\lambda$ должен быть эксперимент.

Были проведены теоретические расчеты для гауссовских и секансных импульсов по выражениям (1) и (2), а также по выражениям из табл. Результаты приведены на рис. 2 для гауссовских импульсов. На этом же

рисунке приведены результаты расчетов зависимости ширины спектра для гауссовских и секансных импульсов по выражениям из табл.



а б в

Рис. 2. Теоретические зависимости длительности (а), пиковой мощности (б) гауссовских импульсов от расстояния z и длительности входных импульсов и ширины спектра гауссовских и секансных импульсов (в) от длительности импульсов

Результаты экспериментальных исследований

Исследование влияния ХД на импульсы гауссовской и секансной формы с длиной волны λ_0 = 1 550 нм и пиковым уровнем мощности p_{m0} = 0 дБм, распространяющихся в одномодовом стандартном ОВ проводилось в схеме одноканальной ВОСС со скоростью B = 10 Гбит/с с бинарной амплитудной модуляцией (АМ) (рис. 3), созданной в программе OptiSystem [4].

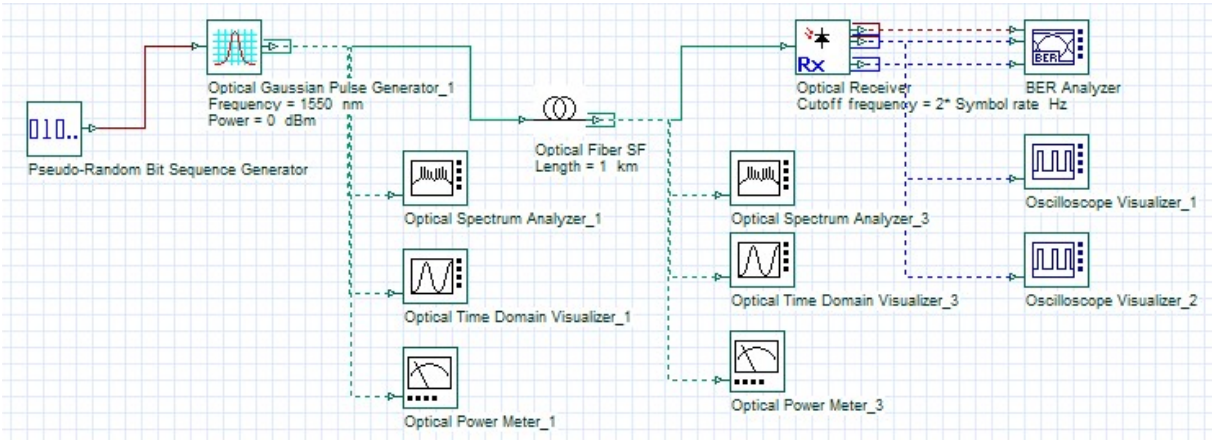


Рис. 3. Схема для исследования ХД в одномодовых ОВ

В процессе экспериментальных исследований проводились измерения выходной пиковой мощности P_{mz} и длительности импульса t_{uz} на уровне половины амплитуды на выходе ОВ для гауссовских и секансных импульсов. Исследования проводились для P_{m0} = 1 мВт, длительностей входных импульсов t_{u0} = 0.1, 0.2 и 0.4 бита, для расстояний от z = 1, 2, 4, 8 и 16 км.

Проводились расчеты относительных отклонений теоретических P_{mz} и t_{uz} и экспериментальных значений P_{mze} и t_{uze} по выражениям

$$\delta P_{mz} = \left(1 - \frac{P_{mze}}{P_{mz}}\right) \cdot 100\% \quad \text{и} \quad \delta t_{uz} = \left(1 - \frac{t_{uze}}{t_{uz}}\right) \cdot 100\%, \qquad (3)$$

а также средних и среднеквадратических значений погрешностей.

По результатам экспериментов определялась ширина спектра излучения $\Delta\lambda_e$ для каждой длины ОВ z и длительности входного импульса t_{u0} по следующему выражению, полученному из (1)

$$\Delta\lambda_e = \frac{t_{u0}}{|D_x| \cdot z} \cdot \sqrt{\left(\frac{t_{uz}}{t_{u0}}\right)^2 - 1}\,.$$

Объем статьи не позволяет привести результаты всех исследований и расчетов. Поэтому переходим к выводам.

Выводы

1. Анализ результатов расчетов и эксперимента показывает, что результаты теоретических расчетов для гауссовских импульсов хорошо совпадают с экспериментальными. Средние значения погрешностей, определенные по выражению (3), не превышают 1 % для определения пиковой мощности и 3 % для длительности импульса.

2. Для секансных импульсов теоретические результаты довольно сильно отличаются от экспериментальных. Видимо, это связано с тем, что для теоретических расчетов использовались формулы, полученные для гауссовских импульсов. Погрешности определения пиковой мощности и длительности импульса достигают 20 %, но для практики это обычно приемлемо.

3. Исследования ХД следует продолжить для других типов ОВ, форматов модуляции, форм импульсов с учетом начального чирпинга.

Список используемых источников

1. Листвин А. В., Листвин В. Н., Швырков Д. В. Оптические волокна для линий связи. М., ЛЕСАРарт, 2003. 106 с.

2. Оптические волокна для телекоммуникаций : учебное пособие / М. С. Былина, С. Ф. Глаголев ; СПбГУТ. СПб., 2019. 92 с.

3. Агравал Г. Нелинейная волоконная оптика: пер. с англ. М.: Мир, 1996. 323 с.

4. OptiSystem. User’s Reference. Optical Communication System Design Software Version 13.

УДК 001.18
ГРНТИ 49.01.11

ВЫЯВЛЕНИЕ КЛЮЧЕВЫХ ТЕХНОЛОГИЙ, ОБЕСПЕЧИВАЮЩИХ ЭВОЛЮЦИЮ МОБИЛЬНОЙ СВЯЗИ ОТ СЕТЕЙ 5G К СЕТЯМ 6G

В. Ю. Гойхман, В. В. Оленичев

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Выявлены шесть основных трендов развития технологий: иммерсивные коммуникации; распознавание, локализация и визуализация; автоматизация промышленности; умный город и умная жизнь; глобальное покрытие мобильной связи; машинное обучение и сетевой ИИ. Проведен анализ каждого направления. Представлены мнения различных крупных компаний и ассоциаций на тему развития ключевых технологий в сетях 6G. Приводятся основные варианты использования 6G, включая различные аспекты их влияния на повседневную жизнь и работу в будущем. Приведены сценарии развития по данным направлениям с точки зрения различных крупных компаний и ассоциаций, на основании которых делаются выводы относительно ключевых векторов развития технологий в сетях нового поколения.

5G, 6G, ML, AI, VR, XR сотовая сеть, инфокоммуникации, машинное обучение, искуственный интеллект, умный город.

Мировое сообщество постепенно входит в новый этап своего развития, этап четвертой промышленной революции (Индустрия 4.0), который будет характеризоваться цифровизацией экономики и всей социальной сферой жизнедеятельности людей, повсеместным проникновением информационно-коммуникационные технологий и искусственного интеллекта.

Технологической базой для осуществления цифровой трансформации общества являются мобильные сети связи пятого 5G и впоследствии шестого 6G поколений, которые дадут новый импульс к развитию ключевых отраслей экономики всего общества, в целом.

Задача статьи – выявление ключевых технологий сетей шестого поколения и определение проблемы, возникающие на пути их достижения. Понимание ожидающих нас проблем позволяет правильно распределить ресурсы, необходимые на их решение

Целью сетей 6G можно назвать стремление к коммуникации «всего со всем» с помощью повсеместной интеллектуализации. Эти сети станут связующим звеном между физическим и кибер-мирами. Именно возможности, предлагаемые технологическими инновациями, инфокоммуникационными технологиями, новыми материалами и т. д., обеспечат непрерывное развитие и совершенствование сетей связи шестого поколения.

Ключевыми технологиями, обеспечивающими эволюцию мобильной связи от сетей 5G к сетям связи 5G Advanced и далее к сетям 6G и эволюционирующими вместе с ними, являются следующие [2]:

1. Иммерсивные коммуникации;
2. Распознавание, локализация и визуализация;
3. Автоматизация промышленности;
4. Умный город и умная жизнь;
5. Глобальное покрытие мобильных связи;
6. Машинное обучение и сетевой ИИ.

1) Иммерсивные коммуникации

На данный момент это направление является наиболее перспективным во многих сферах деятельности. Поскольку эти технологии относительно новые и они ещё только на ранней стадии развития, многие компании ставят, как одну из целей, интеграцию иммерсивных технологий, используя их огромный потенциал. Huawei[1] приводит три вектора развития в данном направлении, а именно:

1. Облачная VR высокой степени достоверности
2. Тактильное и мультисенсорное общение
3. Дисплеи 3D без стекла и голографические дисплеи

По большей части, с данными направлениями солидарны многие ассоциации, выделив их так или иначе в своих статьях. FG-NET[2], к примеру, предполагают, что иммерсивные технологии шагнут куда дальше наших трёх органов чувств и как одной из своих задач ставят создание технологий “полного погружения”, которые будут воздействовать на все пять органов чувств, включая обоняние и вкус. В то время как “6G Flagship University of Oulu”[3] считают, что новые виды иммерсивныхх технологий изменят современное представление о жизни, представив нам совершенно новый спектр устройств, которые будут полезны не только отдельному человеку, но и миру в целом.

2) Распознавание, локализация и визуализация

Сканирование местности в реальном времени, картирование и виртуализация объектов окружающей среды – это те сценарии, которые рассматривают многие компании для сетей нового поколения. Huawei[1] считает, что более высокие диапазоны 6G позволят создавать решения для сканирования и визуализации, которые будут необходимым условием предоставления высококачественных услуг во многих областях. Один из вариантов использования сканирования и визуализации приводится в статьях FG-NET [2], Samsung [4] и Huawei [5], а именно цифровые двойники, которые помогут взаимодействовать с внешним миром из любой точки мира при помощи роботов или других автоматических устройств.

3) Автоматизация промышленности

Если говорить об индустрии 4.0, то данная «промышленная революция» планировалась именно в 5G и большая её часть будет происходить в ближайшее время, но с новыми технологиями нужно двигаться дальше, поэтому многие ассоциации начали задумываться об индустрии 4.0+, которая будет включать в себя доработку, а также усовершенствование уже имеющихся технологий. В основном многие компании говорят об автоматизации производства при помощи описанных выше технологий, а также ИИ, но у каждой из них своё видение их применения. К примеру, в статье «A Comprehensive Survey on 6G Networks» [6] приходят к мнению, что в системах 6G получится внедрить первые автономные системы и развить весь потенциал иммерсивных технологий в промышленном секторе.

4) Умный город и умная жизнь

Понятия «умный город» и «умная жизнь» имеют очень широкий спектр направленности, который расширяется с каждым годом, несмотря на то что это относительное новое направление в беспроводных сетях, и если раньше всё базировалось на уровне «умного дома», то с каждым разом технологии всё больше и больше расширялись и теперь перед сетями нового поколения ставятся задачи уже серьёзного муниципального масштаба. В статье «A Comprehensive Survey on 6G Networks» [6] сеть 6G будет объединять ИКТ и большое количество интеллектуальных физических устройств (например, устройство IoT) для оптимизации повседневных процессов, таких как транспортные системы, мониторинг трафика и операции, связанные с коммунальными услугами, и многие другие. Также значительное расширение трафика и доступность сети повсеместно тоже являются немаловажной задачей. Для достижения данных целей планируется использовать ИИ и машинное обучение, поскольку большинство задач будут требовать обработки Big Data, а также прогнозирования и анализа данных.

5) Глобальное покрытие мобильной связи

Данное направление затрагивается чуть ли не в каждой научной работе на тему 6G и это понятно, поскольку для выполнения множества задач, поставленных перед сетями нового поколения необходимо стабильное высокоскоростное подключение к беспроводным сетям, но это только одна из причин. Другая же заключается в наличии сред NLOS (*Non Line Of Sight* – среды вне зоны прямой видимости) и люди, находящиеся там, являются оторванными от информационного мира. И покрытие таких участков не только бы помогало людям оставаться на связи, но и способствовало развитию промышленности в таких регионах, а также быстрому реагированию в случае чрезвычайных ситуаций. Huawei [1, 5], а также NTT DOCOMO [7] в своих статьях приводят мнение, что использование спутников и псевдоспутников (HAPS) помогут решить эту проблему и создать конвергентную сеть связи,

которая обеспечивает бесперебойное покрытие на планете, удовлетворяя различным требованиям к услугам в любой точке мира.

6) Машинное обучение и сетевой ИИ

ИИ, конечно же, никто не обошёл стороной, поскольку такое развивающееся направление определённо принесёт пользу беспроводным сетям. Но нужно понимать, что ИИ не является решением всех проблем в реализации будущих сетей связи, а скорее его нужно воспринимать как помощника в развитии технологий и достижении поставленных результатов. К примеру, в NTT DOCOMO[7] считают, что использование ИИ в различных сферах жизнедеятельности позволит нам уменьшить риски в них, поскольку всё будет коммуницировать, как один большой механизм. Samsung [4] также считают, что ИИ очень сильно поможет в решении проблем с сетями будущих поколений взяв на себя решение немалого списка задач, начиная от снижения энергопотребления, заканчивая прогнозирования различных ситуаций для обеспечения оптимизации в нужный момент.

Выводы

Проведенный анализ позволил выявить ключевые направления развития мобильных сетей шестого поколения. Внедрение каждого из этих направлений сопряжено с решением ряда сложных технических задач, которые мы также попытались определить в этом обзоре. Некоторые из этих задач, такие как машинное обучением ИИ, активно прорабатываются в данный момент, другие требуют времени. 5G Advanced должен стать первым шагом к реализации этих направлений, а также позволит более реально взглянуть на те возможности, что могут быть достигнуты в технологиях 6G.

Список используемых источников

1. Вэнь Тонг, Пейин Чжу. Сети 6G. Путь от 5G к 6G глазами разработчиков. От подключенных людей и вещей к подключенному интеллекту / пер. с англ. В. С. Яценкова. М.: ДМК Пресс, 2022. 624 с. ISBN 978-5-97060-995-8

2. FG-NET. Network 2030 - A Blueprint of Technology, Applications and Market Drivers Towards the Year 2030 and Beyond / 2019 C. 19 URL: https://www.itu.int/en/ITU-T/focusgroups/net2030/Documents/White_Paper.pdf

3. Aazhang, Behnaam & Ahokangas, Petri & Alves, Hirley & Alouini, Mohamed-Slim & Beek, Jaap & Benn, Howard & Bennis, Mehdi & Belfiore, Jean & Strinati, Emilio & Chen, Fan & Chang, Kapseok & Clazzer, Federico & Dizit, Sudhir & Kwon, Dongseung & Giordiani, Marco & Haselmayr, Werner & Haapola, Jussi & Hardouin, Eric & Harjula, Erkki & Zhu, Peiying. Key drivers and research challenges for 6G ubiquitous wireless intelligence / 2019. C. 33. ISBN 978-952-62-2354-4.

4. Samsung. 6G The Next Hyper-Connected Experience for All / 2020. C. 42. URL: https://cdn.codeground.org/nsr/downloads/researchareas/20201201_6G_Vision_web.pdf

5. Huawei. 5G-Advanced Technology Evolution from a NetworkPerspective (2021) —Towards a New Era of Intelligent Connect X / 2021. C. 14. URL: https://www-file.huawei.com/-/media/CORP2020/pdf/event/1/5G_Advanced_Technology_Evolution_from_a_Network_Perspective_2021_en.pdf

6. Amin Shahraki, Member, IEEE, Mahmoud Abbasi, Member, IEEE, Md. Jalil Piran, Senior Member, IEEE and Amir Taherkordi. A Comprehensive Survey on 6G Networks: Applications, Core

Services, Enabling Technologies, and Future Challenges / IEEE TRANSACTIONS ON NETWORK AND SERVICE MANAGEMENT, VOL. XX, NO. XX, XX 2021 – 2021. С. 21

7. NTT DOCOMO. 5G Evolution and 6G / 2020. С. 17. URL: https://www.docomo.ne.jp/binary/pdf/corporate/technology/rd/docomo5g/20200122_01/DOCOMO_6G_White_PaperEN_20200124.pdf

УДК 004.921
ГРНТИ 28.17.33

РЕАЛИЗАЦИЯ СИСТЕМЫ ДОПОЛНЕННОЙ РЕАЛЬНОСТИ В КОНТЕКСТЕ «ИНДУСТРИИ 4.0»

А. А. Голубкин[1], Р. Я. Пирмагомедов[2]

[1]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
[2]Университет Тампере

Дополненная реальность применяется не только как вариант развлечения, но и как вспомогательный инструмент в области маркетинга, медицины, строительства. В докладе предложен вариант реализации проекта в контексте промышленного интернета вещей (IIOT). Рассматривается архитектура, поставленные задачи, а также способ их реализации с указанием конкретных технологий.

дополненная реальность, смешанная реальность, индустрия 4.0.

Введение

В данной статье рассматривается реализация системы, дополненной реальности, которая позволяет увеличить эффективность производства, а также улучшить качество работы в контексте «Индустрии 4.0». Данный проект затрагивает работу на производственном цехе по работе в области строительства и металлургии, но при успешной реализации может быть использовать во многих других областях. В статье рассматривается архитектура проекта, основные технологии реализации, а также поставленные задачи и способы реализации.

Архитектура системы

Реализуемая система построена на архитектуре клиент-сервер, что позволит без проблем расширять задачи, а также без особых проблем переносить проект на разнообразные устройства.

В данной итерации, в качестве клиента будет выступать мобильный телефон с установленным приложением, в дальнейшем проект может быть перенесен на hmd (*Head-mounted display*).

Текущие мобильные устройства имеют достаточно вычислительной мощности, поэтому было решено, что все вычисления будут происходить на стороне клиента. Сервер будет выступать в качестве базы данных. Это позволит уменьшить размер клиентского приложения, а также расширять информационную базу, без необходимости регулярного обновления.

По мимо основного клиентского приложения, будет административное, для добавления и изменения информации на сервере.

Системные требования

Требования к клиентскому приложению указана в табл.

ТАБЛИЦА. Системные требования клиентского приложения

ОС	IOS	Android
Версия	IOS 11+	Android 7+
CPU	A9+	ARM 64-bit
Graphics API	Metal	OpenGL ES
Память	120 мб	120 мб

Требования к серверу:
• OS Linux.
• 25 гигабайт памяти.
• 3 гигабайта оперативной памяти.

Технологии реализации

Реализация клиентской части:

Было решено реализовать систему в виде кроссплатформенного приложения, что позволило увеличить скорость разработки, а также уменьшить различие приложения между разными операционными системами. Выбор стоял между такими технологиями как: flutter, unreal engine и unity, так как они одновременно поддерживают работу с дополненной реальностью, как на iOS, так и на Android.

Flutter простой кроссплатформенный язык, однако имеет мало библиотек для работы с AR, и очень часто в проект на flutter внедряют компоненты Unity, что может привести к непредвиденным ошибкам. Чаще всего проекты дополненной реальности на данном языке представляют собой прототипы или если необходим небольшой функционал. Также, на данный момент, не существует единой библиотеки для iOS, Android и HMD, что вынуждает писать несколько приложений. Помимо этого, текущие arkit_plugin и arcore_flutter_plugin не дают достаточного доступа к низкоуровневому управлению ресурсами [1].

Unity и Unreal поддерживают кроссплатформенную разработку на мобильные устройства, без необходимости писать несколько приложений. На данный момент обе технологии поддерживают фотореалистичную графику, что дает возможность обеспечить иммерсивное взаимодействие. Однако, Unity имеет гораздо больше пакетов и библиотек для работы с дополненной реальностью, поддерживает почти все доступные устройства (от iOS и Oculus до Windows Mixed Reality). По статистике 60 % AR – систем написаны на Unity [2].

Реализация серверной части:

Для реализации серверной части было решено использовать Java + Spring boot. Java Spring является модульным фреймворком, что позволяет подключать те компоненты, которые необходимы, а также, без особых проблем, перейти на микросервисную архитектуру. Основным минусом является высокий порог входа для начинающих разработчиков, а также сложность настройки отдельных компонентов.

Стек технологий:

• Spring – универсальный Java фреймворк.

• Spring rest – модуль фреймворка Spring для работы с Rest API.

• Swagger – библиотека для генерации документации к Rest API.

• Spring Security – модуль фреймворка Spring для защиты приложения.

Для использования сторонних библиотек, настройки зависимостей и сборки проекта используется фреймворк Maven. Происходит это за счет описания структуры в pom-файлах. Проект издается сообществом Apache Software Foundation и является частью Jakarta Project.

Реализация административного приложения

Для административного приложения было решено использовать C# + WPF. Windows Presentation Foundation (WPF) – это платформа пользовательского интерфейса для создания клиентских приложений для настольных систем [3]. Данный инструмент позволяет работать как с двухмерной, так и трехмерной графикой.

Для связи между клиентским, административным приложением и сервером используется REST API. Это архитектурный стиль взаимодействия компонентов в сети. Представляет собой http-запрос, где данные передаются в качестве параметров. Архитектура проекта представлена на рис. 1.

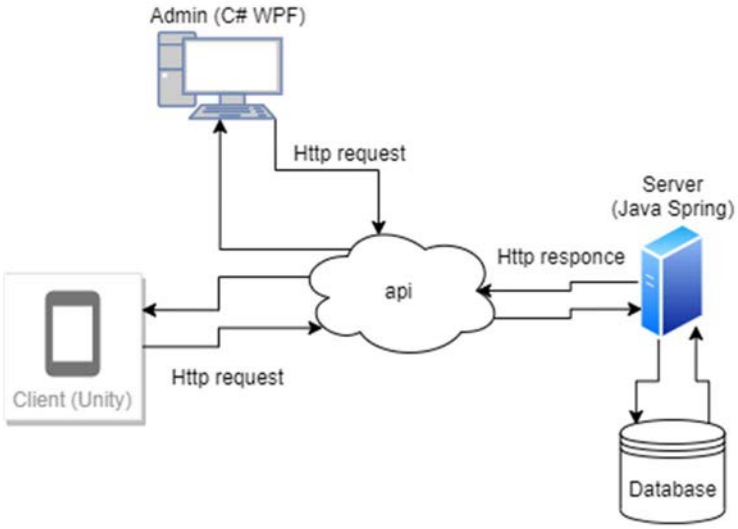


Рис. 1. Архитектура приложения

Поставленные задачи

На данный момент реализованная нами система поддерживает следующие функции:

1. Навигация по складу.
2. Система расположения станков.
3. Визуализация чертежей.
4. Система описания и обучения.
5. Взаимная работа нескольких людей.

Навигация по складу

Данный вариант использования позволяет хранить в базе данных информацию об определенных объектах и их позиции на складе. При сканировании маркера, на экране рисуется путь до необходимого места, с учетом позиции пользователя.

Из плюсов можно выделить возможность быстрой навигации по складу. Однако, появляется проблема при реализации в закрытых помещениях и барьерах в виде стеллажей.

Для реализации данной задачи было решено использовать библиотеку Mapbox [4]. Работу с данной задачей можно разделить на 3 фазы:

1. Импорт карты помещения. Загрузка чертежа, указания набора данных, содержащие информацию о стенах, комнатах, коридорах и других препятствий.
2. Визуализация карты в Unity, масштабирование и позиционирование.
3. Реализация навигации.

Система расположения станков

Данная задача была разделена на две подзадачи: работа с высокоточной моделью и работа с примитивами.

Первый вариант позволяет выводить высокоточную модель с информацией о габаритах дополнительной информации, что позволит учитывать удобство работы и отгрузки продукции. Однако, для этого необходимо иметь на сервере информацию и модель самого станка, что не всегда является возможным. По этой причине было решено сделать возможность реализации данной задачи без использования серверной стороны.

Второй вариант позволяет указать основные габариты и воссоздать прототип станка с помощью примитивов, полностью на стороне клиента. Это даст возможность за короткое время примерно спланировать местоположение новых объектов.

Визуализация чертежей

В данной задаче чертеж предстает маркером для дополненной реальности, при наведении на него камеры выводится 3д модель, которую можно рассмотреть со всех сторон. Для этого необходима предварительная загрузка модели на сервер. Пример реализации прототипа представлен на рис. 2.

Рис. 2. Реализация распознавания чертежей

Система описания и обучения

При наведении камеры на станок происходит вывод информации о состоянии сервоприводов, история использования, а также указание последовательности действий.

Первоначально на каждом станке будет находится маркер для сканирования. В последствии, при успешной реализации, маркером будет являться сам станок, который будет распознаваться с помощью машинного зрения.

Взаимная работа нескольких людей

Бывают случаи, когда компетенция работника, на данный момент недостаточно высока для решения определенной задачи, а более опытного нет по близости, или необходимо провести пояснение или обучение сразу нескольким сотрудникам. Для этого можно воспользоваться видео звонком. Однако это приводит к определенным трудностям: сложность визуализации

пояснения. Для этого можно использовать возможности дополненной реальности, где «оператор» выводит информацию на экран, дополняя и поясняя необходимые аспекты.

Для реализации было решено использовать библиотеку Agora вместе с AR foundation [5]. Первоначальная задача состоит в том, чтобы внедрить дополненную реальность в видео звонок и показывать элементы за счет screen sharing. В дальнейшем необходимо расширить данный функционал до полноценного ассистента с возможностью вывода информации на устройство клиента.

Заключение

В данной статье представлены следующие основные результаты:

- Было представлено описание проекта дополненной реальности, который может упростить работу в контексте «Индустрии 4.0».
- Были поставлены и описаны необходимые задачи.
- Описан выбор технологий для реализации.

Список используемых источников

1. Powloka M. Flutter AR – solutions overview // FiveDotTwelve. URL: https://fivedottwelve.com/blog/flutter-ar-solutions-overview/ (дата обращения: 05.11.2021).

2. Gajsek D. Unity vs Unreal Engine for XR Development: Which One Is Better? // Circuit Stream. URL: https://circuitstream.com/blog/unity-vs-unreal/ (дата обращения: 07.11.2021).

3. Начало работы с WPF // Microsoft. URL: https://docs.microsoft.com/ru-ru/visualstudio/designers/getting-started-with-wpf?view=vs-2022 (дата обращения: 08.11.2021).

4. Pavani A. Indoor navigation in AR with Unity // Medium. URL: https://blog.mapbox.com/indoor-navigation-in-ar-with-unity-6078afe9d958 (дата обращения: 08.11.2021).

5. Cheng R. Video Chat with Unity3D and AR Foundation – Part 3: Remote Assistant App // Agora. URL: https://www.agora.io/en/blog/video-chat-with-unity3d-ar-foundation-pt3-remote-assistance-app/ (дата обращения: 10.11.2021).

УДК 008.2
ГРНТИ 20.15.05

ИНФОКОММУНИКАЦИИ, КАК ОСНОВА ЦИФРОВОЙ ЦИВИЛИЗАЦИИ

А. В. Голышко

АО «НПО РусБИТех»

Роль современной отрасли связи в развитии современного общества является определяющей: трансформация сетей и систем связи (гиперконвергентный программно-определяемый мир); новые сетевые технологии и их теоретические основы (6G и др.); новые вызовы и реализация стратегии импортозамещения на примере АО «НПО РусБИТех»; цифровая цивилизация и ее гуманитарные сценарии развития.

инфокоммуникации, гибридная облачная инфраструктура, метавселенная.

В конце XX века сети связи стали интеллектуальными, а телекоммуникации и информационные технологии стали одним целым, что порождает в мировом сообществе новую реальность, причем отнюдь не только технологическую. Любое устройство становится и компьютером, и устройством связи. Модули связи, встроенные во все другие системы, становятся «новым электричеством», и потому микросхема и процессор закономерно считаются сегодня «ключами» к будущему. Вслед за интеграцией технологий и оборудования произошла сетевая интеграция на базе облачных технологий, появилась гибридная облачная инфраструктура.

В целом современный телеком пришел к практически оптимальной и простой структуре, выродившись в набор облаков, в рамках которых с помощью программно-конфигурируемый сетей (SDN), виртуализации сетевых функций (NFV) и, разумеется, искусственного интеллекта можно создать виртуальную телеком и ИТ-реальность под управлением даже не столь компетентных в данном вопросе специалистов. Дальнейшая оптимизация может включать в себя как дальнейшее совершенствование сетевого/операционного/бизнес управления, так и дальнейшую кастомизацию сервисов.

Сегодня с помощью, например, функционала «Network Slicing» операторы могут создавать множество сетевых слоев с определенным набором характеристик для каждого сервиса в отдельности. Иначе говоря, в одной физической сети путем конфигурирования сетевых элементов можно создать множество виртуальных сетевых слоев с разными требованиями SLA.

С прицелом в будущее все внимание направлено к крайне низкой задержке распространения сигнала, как это рассматривается в сетях 6G. Главное в них – сколько времени необходимо на реакцию и обучение сети. Типичное применение – аналитика на границе сети для Индустрии 4.0/5.0, например, граничные устройства Интернета Вещей (IoT), взаимодействующие с «дополненной реальностью», в том числе с голографическими изображениями в реальном времени. Своевременность доставки информации будет иметь решающее значение для сильно взаимосвязанного общества будущего. Новые приложения, которые интеллектуально взаимодействуют с сетью, также потребуют гарантированной пропускной способности, своевременности поступления и даже своевременности разработки под конкретную потребность. Иначе говоря, грядет гораздо более серьезный уровень кастомизации, подкрепленный гораздо более серьезными требованиями к услугам связи от операторов нового поколения.

Под операторами нового поколения понимаются теперь провайдеры услуг класса NaaS (Network-as-a-Service) вместе со всем набором других облачных услуг, включая не только полностью автоматическое предоставление кастомизированных сервисов с программно-настраиваемыми и управляемыми сетевыми метриками SLA, а также метриками вроде уровня безопасности, доступности, отказоустойчивости и т.п. Эти новые операторы будут исполнять роль операторов сквозных виртуальных слоев, в том числе и нарезанных с помощью Network Slicing и не имеющих собственных физических ресурсов, но обладающих гораздо более широким сервисным потенциалом, нежели операторы традиционные.

Со всем этим сервисным потенциалом надо уметь управляться, поэтому грядет процесс перехода от образованных людьми иерархических систем к «плоским» автономным системам управления, в которых человек будет выполнять лишь роль их разработчика. Новые операторы будут автономными, как, впрочем, и порождаемые ими в сквозных виртуальных слоях виртуальные сети. В действительности речь идет не столько о самих сетях, физических и виртуальных, сколько о новых процессах управления ими и предоставляемыми с их использованием сервисами. Это даст автономным интеллектуальным операторам снижение операционных затрат (особенно при организации сложных кастомизированных услуг с управляемым SLA) и более высокий уровень утилизации сетевых ресурсов.

В свою очередь, традиционные операторы со своим набором традиционных услуг связи характеризуются в целом низким уровнем автоматизации сетевого, операционного и бизнес-управления. Они будут играть роль операторов физических доменов, поддерживающих технологии SDN, NFV и пр., обладая набором стандартных открытых интерфейсов для взаимодействия с автономными операторами сквозных слоев.

Вот так ИТ-инфраструктура становится, с одной стороны, все более интегрированной и сложной, а, с другой, – превращается в единую телекоммуникационную среду, управление и пользование которой движется к интуитивно понятной простоте. При всем этом ИТ-инфраструктура становится критически важной для функционирования экономики и всего государства с учетом курса на цифровизацию и цифровую трансформацию всех сторон жизни общества. Тем важнее становится переход на ИТ-инфраструктуру отечественного происхождения.

С учетом Доктрины информационной безопасности РФ [1], утвержденной в 2016 г. Президентом Российской Федерации В.В.Путиным, следует различать цели и задачи, стоящие перед государством и бизнесом. И если бизнес сам волен решать, какие продукты ему следует использовать с учетом имеющихся у него частных рисков (преимущественно по части фрода), то государству следует учитывать максимальный набор рисков с учетом всего того, что входит в понятие «кибервойны». В понимании последней не может быть ни «выключаемых рубильником» авторами «открытых» кодов, ни какого бы то ни было «независимого» импортного производства микроэлектроники. Хорошо, что, хотя и с опозданием, но эта работа в РФ началась.

Отечественные разработчики ПО и оборудования для обслуживания государства должны быть отечественными не на бумаге, не на переклеенном шильдике, не по совокупности каких-либо баллов, а иметь либо коллективы разработчиков собственного кода в составе отечественных продуктов, либо помимо квалифицированного персонала – соответствующее технологическое оборудование на территории страны и желательно отечественного же производства. Собственно, так действует сейчас и АО «НПО РусБИТех», включая в свои перспективные продукты процессоры и ПО отечественной разработки и участвуя в разработках оборудования для радиоэлектронной промышленности РФ.

В том, насколько современная цивилизация зависит от телекоммуникаций, можно убедиться, представив, что случится, если вдруг отключить все, что связано с понятием «связь». А случится буквально все, начиная с остановки всего производства, энергетики, транспорта, финансов и заканчивая ломкой для многих и многих миллионов, страдающих социально-сетевой или игровой зависимостью. В темноте и холоде начнется голод, но уже не информационный, а самый настоящий. Что поделать – человечество само окружило себя такими рисками, погрузившись в глубокую зависимость от телекоммуникаций.

Кстати, в Национальной киберстратегии США от 2018 г. [3] прямо заявлено, что США должны доминировать в киберпространстве и задавать правила для остальных, Россия – потенциальный враг США номер один, и

к тому же американские технологии и открытый Интернет являются средством продвижения ценностей США по планете и интересов американских корпораций. Тем важнее сегодня для РФ ускорение процесса импортозамещения.

Голограммы и мультисмысловые коммуникации - следующие рубежи в коммуникации. Движение к будущему включает в себя развитие дополненной (AR) и виртуальной реальности (VR), где-то не на очень далеком подходе голография в реальном времени, начинается заселение виртуальных пространств (метавселенных) аватарами людей и даже государств, эти аватары уже могут прикоснуться к живому человеку, и последний почувствует это прикосновение, будучи одет в специальную одежду. Понятие «тактильный Интернет» уже используется специалистами. Различные сенсорные ощущения могут быть объединены с голограммами, и в материалах, посвященных сетям 6G уже используется термин «Internet of Skills» (Интернет навыков), когда появляется возможность передавать «знания и умения» через Интернет средствами VR-решений и с помощью голограмм. Новые знания будут приходить в виде откровения непосредственно из информационной среды.

Не только желание «поиграться в новое», но также и безысходность, слабость и безответственность также приведёт людей в виртуальную среду. Устал, разочаровался, не нашел себе места в реальной жизни – тебя ждут в виртуальной жизни. Там, в метавселенной [5], будут все удобства – круглосуточное наблюдение за сахаром, пульсом и давлением с немедленной лечебной реакцией в случае отклонений. Кто будет против? Пожилые первые встроятся в систему. Зрелые будут видеть шансы, которых нет в жизни. Молодые уже практически находятся там. Благодаря Интернету люди находят работу и деньги, которые не в силах найти вне сети, особенно когда государство выдавливает людей из пенсионного обеспечения. Это огромные новые возможности, которые непременно соблазнят граждан. А если метавселенная поможет обрести качества, способствующие карьере, то и говорить что-то против будет практически бесполезно. И ничего не будет удивительного, если потом какие-нибудь цифровые сектанты проведут аналогии существования граждан в метавселенной с существованием души в высших сферах. Американский изобретатель и футурист Раймонд Курцвейл предположил, что, переписав на компьютер память человека, можно организовать последнему настоящее бессмертие [6].

Если доступные развлечения, образование, заработки в метавселенных будут предоставлять цифровые компании, они естественно и закономерно заменят собой государство. В метавселенной уже есть свои деньги, и собственно гражданство может превратиться в фикцию. Вопрос «А зачем тогда нужно государство?» отпадёт сам собой. Все важнейшие вопросы люди бу-

дут решать без участия государства. Более того – государства даже при осуществлении социальной помощи будут зависимы от глобальных ИТ-компаний, а дальше и вовсе попадут в рабство. Граждан у государства уведут, как лошадь из стойла, причём уже без всякой эмиграции физических тел. Последние останутся по месту проживания, фактически находясь в собственности глобальных финансово-цифровых транснациональных корпораций.

Впрочем, с технической точки зрения в метавселенных пока не все так просто. Эффект виртуального присутствия нужно «шлифовать», а для этого потребуются вычислительные средства на несколько порядков более мощные, чем имеет место сегодня. И еще крайне важна чрезвычайно малая задержка сигнала. Ведь для комфортного едва ли не круглосуточного (с перерывами на еду и сон) пребывания в метавселенной необходим принципиально иной уровень реалистичности демонстрируемых пользователю цифровых объектов и взаимодействий между ними, чем тот, что доступен на сегодняшних и даже перспективных гаджетах и гарнитурах виртуальной/дополненной реальности. Не стоит забывать и про голографию, которая уже закладывается в сети 6G [4].

Вот так вместо научного, технологического и социального рывка в будущее, человечеству собираются всучить виртуальные игровые места, чтобы «лишние» не мешали «избранным».

Впрочем, это не все сценарии вероятного будущего, которые пишутся теми, кто позиционирует себя в качестве вершителей судеб планеты. В частности, один из идеологов «нового мирового порядка» – Жак Аттали [2] – описывает будущее, базирующееся на развитии инфокоммуникаций, как этакий «мир кочевников», основу которого составят «информационные кочевники» без стабильного адреса и семьи: они будут носить на себе (очевидно, в облаках) и в себе всё, что составит его социальное значение: смартфоны, аппараты самодиагностики и даже запчасти – сменяемые органы. Кочевник может продолжать общественную и частную жизнь, общаться с другими людьми и делать это независимо от своего местопребывания в данную минуту. Человеку-кочевнику придется трудиться постоянно, бесконечно, так как у него исчезнут представления о естественном делении суток на дневное и ночное время, как, в общем, и всякое понятие о времени. Впервые у человека не будет адреса. Переходя из одного «человейника» в другой, человек-«муравей» не почувствует разницы. Политологи называют Жака Аттали «серым кардиналом» Франции, масоном, близким к семейству банкиров Ротшильдов. Вся эта информация вложена в его уста не просто так.

Однозначно, что будущие инфокоммуникации радикально изменят правила игры. Отсидеться в бункере не получится. Где, к примеру, проходит

граница суверенного государства или свободы личности в киберпространстве? Какие желания возникают при получении способа инфокоммуникационного воздействия на каждого в этом мире? Быть может, получив громадный потенциал новых телекоммуникационных технологий, человечество оказалось не готово использовать его во благо? Существует ли какое-то мнение отечественного ИТ-сообщества по поводу использования киберпространства, отличное от зарубежного? К примеру, основой для него мог бы быть существующий комплект электронных госуслуг, который, по сути, является прологом к созданию цифрового государства. Интересна также техническая готовность отечественных социальных сетей к созданию прообразов метавселенных.

Учитывая сказанное выше, в наши дни приобретает особое значение системное комплексное образование, чтобы уметь ориентироваться в интегрированном мире ближайшего будущего и искать ответы на поставленные выше вопросы. Национальная концепция этого будущего в киберпространстве, в создаваемом цифровом государстве, должна быть разработана с учетом всего вышесказанного.

Список используемых источников

1. Доктрина информационной безопасности Российской Федерации. URL: http://www.scrf.gov.ru/security/information/document5/

2. Аттали Жак Краткая история будущего. СПб.: Издательский дом: Питер, 2014.

3. Стратегия национальной кибербезопасности Соединенных Штатов Америки. Сентябрь 2018 года. URL: http://d-russia.ru/wp-content/uploads/2019/01/National-Cyber-Strategy_USA_2018.pdf

4. Тактильное и голографическое будущее 6G. Возможности и проблемы сетей связи следующих поколений. URL: https://habr.com/ru/post/570510/

5. https://habr.com/ru/post/649969/

6. Рэй Курцвейл: люди смогут обмениваться телами и жить вечно. URL: https://playboyrussia.com/chtivo/rey-kurtsveyl-lyudi-smogut-obmenivatsya-telami-i-zhit-vechno-7319/

УДК 004.942
ГРНТИ 49.33.01

МОДЕЛИ АВТОРЕГРЕССИИ И ПРОИНТЕГРИРОВАННОГО СКОЛЬЗЯЩЕГО СРЕДНЕГО ARIMA С ПРИМЕНЕНИЕМ АВТОРЕГРЕССИОННОЙ УСЛОВНОЙ ГЕТЕРОСКЕДАСТИЧНОСТИ

А. А. Гребенщикова, В. С. Елагин

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Наиболее популярной моделью прогнозирования сетевого трафика являются модели авторегрессии и проинтегрированного скользящего среднего (ARIMA). Модель ARIMA является важным классом параметрических моделей, который позволяет описывать нестационарные ряды. Современные исследования показывают, что использование обычной модели ARIMA дает большую частоту ошибок по сравнению с комбинированной моделью ARIMA с другими методиками.

прогнозирование трафика, модели трафика данных, модели ARIMA, модели GARCH, самоподобность, мультифрактальность.

При построении моделей с определённым количеством неизвестных параметров очень важно учитывать такой фактор, как экономия затраченных математических ресурсов для поиска оптимальной модели. Данный аспект определяет использование итеративных подходов и осторожности при выборе параметров. Подробное рассмотрение итеративного подхода Бокса-Дженкинса и структуры моделей прогнозирования ARIMA/GARCH являются необходимым условием для будущего прогнозирования сетевого трафика.

Итеративный подход

Согласно методологии Бокса-Дженкинса [1], итеративная процедура построения моделей для фиксирования зависимостей изучаемых временных рядов состоит из трёх этапов, как изображено на рис.:

1. Идентификация. Подбор оптимального класса моделей на основе уже имеющихся данных.
2. Оценка. Подбор соответствующих параметров для построения модели.
3. Диагностика. Сопоставление модели имеющимся данным с целью выявления несоответствий.

Модель ARIMA

Модели авторегрессии и проинтегрированного скользящего среднего ARIMA (p, q) – это важный класс параметрических моделей, который позволяет описывать нестационарные ряды и классифицируется, как короткий прогноз (т. е. качественно осуществляет предсказание трафика только на несколько шагов вперёд). В качестве частных случаев включает в себя модели авторегрессии, скользящего среднего, смешанные модели авторегрессии-скользящего среднего и интеграцию всех трёх соответственно. Краткая запись модели описывается, как:

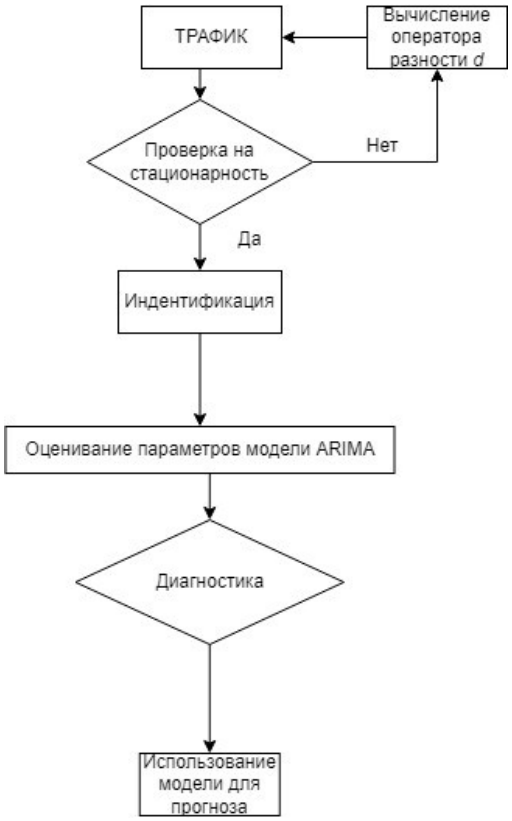


Рисунок. Итеративный подход

$$\varphi(B)(1-B)^d\beta_t = \theta(B)a_t, \qquad (1)$$

где β_t – временной ряд для анализа; α_t – белый шум; B – оператор сдвига назад ($B\beta_t = \beta_{t-1}$); φ() и θ() – полиномы степени p и q; d – порядок взятия последовательной разности ($\Delta\beta_t = \beta_{t-1} - \beta_t = (1 - B)^d \beta_t \ldots$).

Модель GARCH

Модель GARCH (p, q) именуется обобщённой и является одним из способов представления ARCH модели с большим числом лагов. Наиболее отличительной чертой GARCH является его условная дисперсия (меняется с течением времени) и обладание свойствами ARMA моделей [2, 3].

Общая модель GARCH для условной дисперсии α_t предполагает, что [1]:

$$\alpha_t = \sigma_t e_t, \qquad (2)$$

где e_t – последовательность независимых и одинаково распределённых случайных величин со средней равной нулю и дисперсией равной единице.

Модель GARCH (s, r) характеризует условную дисперсию ошибки прогнозирования α_t и записывается в общем виде, как:

$$\sigma_t{}^2 = \alpha_0 + \sum_{i=1}^{s} \alpha_i \alpha_{t-i}{}^2 + \sum_{j=1}^{r} \beta_j \sigma_{t-j}{}^2, \qquad (3)$$

где $\alpha_0 > 0$, $\alpha_i \geq 0$, $i = 1, \ldots, s - 1$, $\alpha_s > 0$, $\beta_j \geq 0$, $j = 1, \ldots, r - 1$, $\beta_r > 0$.

Следует отметить, что GARCH(1,1) модель является наиболее популярной и часто используемой среди остальных.

Модель ARIMA/GARCH

ARIMA-GARCH объединяет модель ARIMA с моделью GARCH для формирования нелинейной модели временных рядов. В общем виде такую модель можно записать, объединив выражения (1) и (2) в виде:

$$\varphi(B)(1-B)^d\beta_t = \theta(B)\sigma_t e_t,$$

где σ_t^2 описывается с помощью (3).

Характеристика дисперсии «условная» – подразумевает не только изменчивость с течением времени, но также и явную зависимость от прошедшей последовательности наблюдений [4, 5]. Соответственно, такое свойство моделей GARCH может фиксировать и объяснять характерные для сетевого трафика «всплески», что подтверждает гибкость моделей ARIMA/GARCH при моделировании самоподобного трафика с зависимостями в долгосрочной перспективе.

Заключение

Условная дисперсия моделей GARCH подразумевает возможность фиксировать и объяснять характерные для сетевого трафика «всплески», что может говорить о гибкости моделей ARIMA/GARCH при моделировании самоподобного трафика с зависимостями в долгосрочной перспективе. Таким образом, модель ARIMA с применением авторегрессионной условной гетероскедастичности является гибридной моделью прогнозирования сетевого трафика, представляет большой интерес для подробного изучения на реальных примерах сетевого трафика и в будущих исследованиях может продемонстрировать наилучшие результаты.

Список используемых источников

1. Box G. E.P ., Jenkins J. M., Reinsel G. C., Ljung G. M. Time series analysis: forecasting and control, 2015.

2. Бородич С. А. Эконометрика: учебное пособие для вузов. Мн.: Новое знание, 2004. 408 с.

3. Aganin A. Forecast comparison of volatility models on Russian stock market // Applied Econometrics. 2017, v. 48. pp. 63–84.

4. Rutka G. Network Traffic Prediction using ARIMA and Neural Networks Models // Electronics And Electrical Engineering, №4, 2008.

5. Привалов А. Ю., Благов А. В. Об использовании некоторых моделей самоподобного сетевого трафика в имитационном моделировании // Математическое моделирование. 2011. Т. 23. № 7. С. 114–128.

УДК 004.056.53
ГРНТИ 81.93.29

СПОСОБЫ АУТЕНТИФИКАЦИИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

В. Д. Губарев

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А Бонч-Бруевича

В статье рассмотрены способы аутентификации пользователя в информационных системах.

Цель статьи – выделить современные методы аутентификации в информационных системах и определить их положительные и отрицательные их стороны. Актуальность исследования объясняется повсеместным использованием в современном мире разнообразных информационных систем, нуждающихся в защите от несанкционированного доступа.

аутентификация, пароль, биометрическая характеристика.

Аутентификация – процедура проверки подлинности субъекта, которая позволяет достоверно убедиться в том, что субъект, предъявивший свой идентификатор, на самом деле является именно тем субъектом, идентификатор которого использует. Для этого он должен подтвердить факт обладания некоторой информацией, которая может быть доступна только ему одному (пароль, ключ, биометрия …).

Вид информации, предоставляемой информационной системе называется фактором аутентификации [1].

Факторы аутентификации разделяют на три категории:

1) На основе знания (пароль, PIN-код, парольная фраза);

2) На основе обладания чем-либо (физический ключ, магнитная карта, OTP-токен, цифровые водяные знаки [11–13]);

3) На основе биометрических характеристик (отпечатки пальцев, снимок сетчатки глаза, голос).

Также в случаях «строгого контроля» доступа в помещение может использоваться «четвёртая» категория – на основе места проведения процедуры. В данной работе эта категория рассматриваться не будет.

Возможно также одновременное использование нескольких факторов аутентификации (Многофакторная аутентификация).

Для каждого фактора используются свои методы аутентификации.

Первая категория

Парольная аутентификация – аутентификация на основе обладания некоторым секретным знанием [5, 6].

Пароли могут разделяться на постоянные, условно постоянные и временные.

Стойкость пароля зависит от его длины, алфавита, предельного количества попыток и других параметров.

Методы парольной аутентификации:

•На основе открытого пароля. Вводится имя пользователя и пароль, они отправляются в открытом виде (не используются криптографические методы шифрования) администратору (серверу аутентификации или иному механизму аутентификации), тот находит учетную запись пользователя и сравнивает пароли.

•На основе хэшированного пароля [7]. Механизм работы, как и у аутентификации на основе открытого пароля, но в данном случае с помощью хэш-функции вычисляется хэш-значение пароля. На проверку вместо пароля отправляется и сравнивается хэш-значение.

Из хэш-значения невозможно восстановление исходного пароля, при обладании полученным хэш-значением.

•На основе PIN-кода. Personal Identification Number – разновидность пароля, используемая в основном на локальном устройстве.

Разница между PIN-кодом состоит в области и условиях их использования.

PIN-код используется:

a) В локальном устройстве, ввод кода без использования клавиатуры этого устройства невозможен,

b) Если он не передаётся по сети и не может быть перехвачен.

Возможные угрозы и атаки [8, 9]:

▪Кража пароля. Злоумышленник может прочитать пароли пользователя из парольного файла. Для защиты используется хэширование пароля.

▪Подглядывание за набором пароля. Злоумышленник лично, с помощью технического устройства или программного обеспечения смотрит на процесс набора пароля. Для защиты используются неотображение пароля на устройстве вывода информации, ограничение доступа к устройству.

▪Подбор пароля. Использование личных данных для угадывания пароля. Для защиты используются правила формата пароля, ограничение попыток ввода.

▪Социальные методы обмана пользователя (социотехника). Злоумышленник представляется человеком, имеющим определённые права в системе (администратором или пользователем), и вынуждает пользователя или администратора изменить пароль на указанный им. Для защиты используются специальные политики смены паролей и нераскрытия паролей.

▪Принуждение. Различные угрозы или физическое принуждение пользователя с целью заставить открыть свой пароль. Для защиты используются специальные методы сигнализирования о принуждении

Вторая категория

Одноразовые пароли (OTP (one time password)-токены).

Для генерации паролей токены используют хэш функции или криптографические алгоритмы:

Симметричная криптография – пользователь и сервер используют один и тот же секретный ключ.

Ассиметричная криптография – в устройстве хранится закрытый ключ, а сервер аутентификации использует соответствующий открытый ключ.

Методы аутентификации с помощью OTP-токенов:

•«Запрос-ответ» (Challenge-response). Пользователь вводит свои данные, сервер отправляет ему случайный запрос, пользователь вводит запрос в свой токен, запрос шифруется с помощью ключа и отправляется на сервер, там ответы сравниваются и на основании правильности ответа аутентификация считается успешной.

•«Только ответ». Используя значения предыдущего запроса токен и сервер генерируют «скрытый» запрос.

•«Синхронизация по времени». Устройство и сервер генерируют пароль на основании внутренних часов.

•«Синхронизация по событию». Сервер и устройство ведут учёт аутентификаций и на основании этого числа генерируют OTP.

Также во второй фактор аутентификации входят физические идентификаторы:

•Физический ключ,

•Смарт карты,

•USB – ключи,

•Memory-карты,

•Touch memory.

Возможные угрозы и атаки [10, 11]:

▪Потеря/кража физического идентификатора. Защита от атаки: использование дополнительного метода аутентификации, PIN-коды в OTP-токенах

▪«Человек посередине». Перехват одноразового пароля, блокировка пользователя и вход в систему вместо него. Защита от атаки: использование метода «Запрос-ответ».

▪Нечестный администратор. Злоумышленник, являясь доверенным лицом делает дубликат токена. Защита от атаки: разделение ответственности при инициализации аутентификационных токенов.

Третья категория

Биометрические характеристики – измеримая физиологическая или поведенческая черта человека, которую можно использовать для установления его личности [12].

Биометрический образец – наблюдение выбранной биометрической характеристики.

В базе данных системы хранится цифровой биометрический образец. При получении доступа в информационную систему, человек вводит свой биометрический образец, система извлекает из него данные и сравнивает с уже имеющимися. На основании результата человек получает доступ или отказ в доступе.

Подразделяются на:

1) Физиологические – биометрические характеристики на основе данных, полученных путём измерения анатомических характеристик человека.

•Радужная оболочка глаз: полоски и бороздки в радужной оболочке глаза;

•Отпечаток пальца: расположение и направление уникального папиллярного узора пальца;

•Лицо: форма черепа, расположение носа, глаз, скул и т. д.;

•Кисть: высота, ширина костей, суставов и вен кисти, и пальцев;

•Сетчатка: сравнение расположения кровеносных сосудов на сетчатке.

2) Поведенческие – биометрические характеристики на основе данных, полученных путём измерения действий человека, основной чертой является протяжённость действия.

•Голос: тембр, громкость и манера произношения человека;

•Подпись (почерк) [13]: скорость, порядок линий, давление и внешний вид подписи;

•Компьютерный почерк (динамика нажатия клавиш на клавиатуре): замеряется скорость набора текста, длина пауз, манера письма, количество ошибок при вводе с клавиатуры.

Реализовать аутентификацию по биометрическим характеристикам можно как с помощью аппаратных (сканер отпечатка пальца, видеокамера, микрофон и т. д.), так и с помощью программных средств.

Возможные угрозы и атаки:

▪Подделка биометрической черты [14]. Изготовление копии физической отличительной черты пользователя и предъявление неё датчику.

Защита от атаки: снятие показателей с высоким уровнем детализации, использование более точной аппаратуры;

▪Воспроизведение поведения пользователя. Запись поведенческой черты и воспроизведение её на датчике.

Защита от атаки: изменяемое поведение – каждый раз при попытке аутентификации система требует различного поведения. Контроль человека за процессом аутентификации;

▪Угрозы пользователю. Угроза и способы борьбы с ней совпадают с пунктом принуждение в парольной аутентификации.

Заключение

В статье были разобраны и описаны методы аутентификации, часто использующиеся в современных информационных системах, указаны их принцип работы, преимущества и недостатки.

Список используемых источников

1. Афанасьев А. А., Веденьев Л. Т., Воронцов А. А., Газизова Э. Р., Додохов А. Л., Крячков А. В., Полянская О. Ю., Сабанов А. Г., Скида М. Н., Халяпин С. Н., Груздев С., Нахаев Ю. С., Шелупанов А. А. // Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам. Москва: Горячая линия – Телеком 2012. 530 с. URL: https://znanium.com/read?id=140493 (дата обращения: 21.03.2022).

2. Красов А. В., Верещагин А. С., Цветков А. Ю. Аутентификация программного обеспечения при помощи вложения цифровых водяных знаков в исполняемый код // Телекоммуникации. 2013. № S7. С. 27–29.

3. Красов А. В., Верещагин А. С., Абатуров В. С. Методы скрытого вложения информации в исполняемые файлы // Известия СПбГЭТУ ЛЭТИ. 2012. № 8. С. 51–55.

4. Штеренберг С. И. Метод вложения информации в исполнимые файлы и его структурный анализ по величине скрываемой информации // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2016. № 1. С. 37–42.

5. Юркин Д. В., Винель А. В., Таранин В. В. Анализ временных и сложностных характеристик парольной аутентификации в защищённых операционных системах семейства Unix // Информационно-управляющие системы. 2010. № 6 (49). С. 42–46.

6. Никитин В. Н., Юркин Д. В. Улучшение способов аутентификации для каналов связи с ошибками // Информационно-управляющие системы. 2010. № 6 (49). С. 42–46.

7. Ричард Э. Смит Аутентификация: от паролей до открытых ключей. Москва; Санкт-Петербург; Киев, 2002, 419 с

8. Красов А. В., Штеренберг С. И., Голузина Д. Р. Методика визуализации Больших данных в системах защиты информации для формирования отчетов уязвимостей // Электросвязь. 2019. № 11. С. 39–47.

9. Красов А. В., Штеренберг С. И., Фахрутдинов Р. М., Рыжаков Д. В., Пестов И. Е. Анализ информационной безопасности предприятия на основе сбора данных пользователей с открытых ресурсов и мониторинга информационных ресурсов с использованием машинного обучения // T-Comm: Телекоммуникации и транспорт. 2018. Т. 12. № 10. С. 36–40.

10. Миняев А. А., Красов А. В. Методика оценки эффективности системы защиты информации территориально-распределенных информационных систем // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2020. № 3. С. 26–32.

11. Буйневич М. В., Покусов В. В., Израилов К. Е. Способ визуализации модулей системы обеспечения информационной безопасности // Научно-аналитический журнал «Вестник Санкт-Петербургского университета Государственной противопожарной службы МЧС России». 2018. № 3. С. 81–91.

12. Евангели Александр Технологии биоидентификации и биометрический рынок // PC Week/RE. 2003. № 7. С. 24; 2003. № 10. С. 26. URL: https://www.computer-museum.ru/technlgy/bio_id.htm (дата обращения: 21.03.2022)

13. Сапиев А. З. Аутентификация пользователей сети на основе компьютерного почерка. URL: https://cyberleninka.ru/article/n/autentifikatsiya-polzovateley-seti-na-osnove-analiza-kompyuternogo-pocherka (дата обращения: 21.03.2022)

14. Жувикин А. Г., Коржик В. И., Леутин Е. И. Защита целостности баз данных цифровых отпечатков пальцев при помощи использования цифровых водяных знаков // Телекоммуникации. 2018. № 12. С. 2–12.

Статья представлена заведующим кафедрой ЗСС СПбГУТ, кандидатом технических наук, доцентом А. В. Красовым.

УДК 681.7
ГРНТИ 49.44.31

ИССЛЕДОВАНИЯ СЕТЕВЫХ РЕСУРСОВ И ПОКАЗАТЕЛИ ПРОИЗВОДИТЕЛЬНОСТИ МУЛЬТИСЕРВИСНЫХ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ

Р. Т. Гумбатов[2], Б. Г. Ибрагимов[1,2,3], Р. Ф. Ибрагимов[3], М. Б. Намазов[2], О. Г. Мирзоев[2]

[1]Азербайджанский Технический Университет

[2]Бакинский инженерный университет

[3]Институт систем управления Национальной академии наук Азербайджана

Проанализированы преимущества использования базовые принципы будущих сетей FN (Future Networks), для построения высокоэффективных мультисервисных телекоммуникационных сетей (МТС), при представлении широкий спектр дополнительных услуг. Предложена математическая модель производительности МТС с внедрением основной принципы FN, использующие физические, виртуальные, канальные, информационные, коммутационные и сетевые ресурсы. Модель производительности сетей, отличается от известных тем, что для обеспечения приемлемого качества QoS (Quality of Service) и QoE (Quality of Experience) в общей существующей NGN (Next Generation Network) архитектуре мультисервисных сетей связи общего пользования была использована новая инновационная технология и четыре целевых установки сетей FN. Чему

способствует разработка соответствующих имитационных моделей качества функционирование сетей связи для исследования и анализе показателей их производительности.

ограниченные ресурсы, самоподобный трафик, телекоммуникационная среда, IMS, показатель Хёрста, информационная безопасность, NFV, эффективность.

Стремительное развития инфраструктуры цифровой экономики и формирование стратегических планов «Дорожная карта цифровизации» требуют новые рациональные и глобальные подходы к построению МТС на основе базовой принципы будущих сетей FN с повышенной производительностью, использующие инновационные технологии. К ним относятся прежде всего информационные и телекоммуникационные технологии как SDN (*Software Defined Networking*) NFV (*Network Functions Virtualization*) IMS (*Internet Protocol Multimedia Subsystem*), искусственного интеллекта, WDM&DWDM, облачных вычислений, так и технологии построения распределенных сетей связи [1–3].

Учитывая изучаемые целевые установки для создания мультисервисных сетей FN на основе рекомендаций ITU-T, Y.3001 [4–6] и используемые вышеперечисленные инновационные технологии открывают новые возможности для оказания широкого спектра инфокоммуникационных услуг с учетом многочисленных требований параметров QoS и QoE.

Поэтому, задачи анализа показателей производительности МТС на базе FN при использовании информационные и сетевые ресурсы являются наиболее актуальными.

Производительность МТС характеризует многочисленных показатели как качества работы сети, надежности, стоимости системы так и эффективности использования физических ресурсов [7–9].

В данной работе рассматривается задачи исследование показатели производительности мультисервисных телекоммуникационных сетей с учетом сетевых ресурсов на базе перспективных технологии FN.

На основе вышеизложенного предположения рассмотрим вопросы построения МТС [1, 5] с коммутацией пакетов (ITU-T,Y.3000÷Y.3499) для оказания мультимедийные услуги и приложения. При этом, следует обратить особое внимание на показатели производительности сети связи с учетом многочисленных требовании QoS и QoE.

В частности, было установлено, что трафик такой сети обладает так называемым свойством самоподобия, т. е. выглядит качественно одинаково при почти любых масштабах временной оси, имеет память, а также характеризуется высокой пачечностью. Здесь, коэффициент пачечности сетей для заданного потока соответствует отношению пиковой интенсивности λ_i^n процесса поступления заявок на обслуживание к его среднему λ_i^c значению: $K_n(\lambda_i) = [\lambda_i^n / \lambda_i^c] \geq 1$.

В результате исследование показали [3, 7] теоретический расчет параметров системы распределения информации, предназначенной для обработки такого трафика, по классическим формулам дает некорректные и неоправданно оптимистические результаты. Однако, для оценки степени самоподобия трафика является использован параметр Хэрста – H .

Проведенные исследование показывают [5, 7], что измерение показателя Хэрста H применены семью методами: анализа дисперсии, нормированного размаха (R/S), периодограмм, абсолютных моментов, дисперсии остатков, Эбри-Вейча и Виттла. Установлена, что для всех методов реализаций сетевого трафика коэффициент $H > 0.5$, т. е. трафик относится к классу персистентных процессов [7]. С учетом показателя Хэрста производительность $E[П(\lambda_i, H)]$ сетей связи находится следующей зависимостью:

$$E[\Pi(\lambda_i, H)] = W[C_{\max}(\lambda_i), \eta_{эф}(\lambda_i, t), K(\lambda_i, H), I_{н.б}(\lambda_i), C_{ап}^{ээ}(\lambda_i)], \quad i = \overline{1,k}, \qquad (1)$$

где $\eta_{эф}(\lambda_i, t)$ – коэффициент эффективного использования сетевых ресурсов и учитывая канальные, виртуальные, информационные так и сетевые ресурсы определяется как:

$$\eta_{эф}(\lambda_i, t) = F[\eta_k(\lambda_i, t), \eta_b(\lambda_i, t), \eta_u(\lambda_i, t), \eta_c(\lambda_i, t)] \quad , \quad i = \overline{1,k}, \qquad (2)$$

$C_{ап}^{ээ}(\lambda_i)$ – экономическая эффективность и стоимость средств сетей с учетом λ_i при обслуживании *i*-го потока пакетов трафика мультимедийных услуг; $C_{\max}(\lambda_i, H)$ – максимальная пропускная способность с учетом λ_i и H ; $K(\lambda_i, H)$ – функция, учитывающая требования параметров QoS&QoE с учетом параметров λ_i и H ; $I_{нб}(\lambda_i)$ – функция, учитывающая показатели надёжности сети и информационной безопасности с учетом λ_i .

В (1) и (2), среди анализируемых характеристик сетей, особое место занимает экономическая эффективность и стоимость аппаратно-программных комплексов $C_{ап}^{ээ}(\lambda_i)$ при использовании разнородных ресурсов. Разнородный ресурс, является важнейшим показателем, используемым при исследовании производительности сетей связи.

Данная задача может решаться различными методами, при этом каждый обладает своими преимуществами. Учитывая важность постановки задачи, предлагается ММ с учетом комплексные показатели исследуемые сети.

Теперь можно рассмотреть описание и построения ММ сети связи. С целью построения МТС, в качестве инновационных технологий использованы концепция SDN, NFV и IMS [1–3], что открывают новые возможности для организации эффективной работы любые сети.

Для решения поставленной задачи предложена ММ для анализа показателей производительности МТС и выбрана как целевая функция- экономической эффективности и стоимости системы, которая описывается следующими целевыми функциями:

$$E[\Pi(\lambda_i, H)] = \mathrm{W}\{Arg\min_i[C_{ap}^{\text{ээ}}(\lambda_i, H)]\},\ i = \overline{1,k}, \quad (3)$$

при следующих ограничениях

$$N_k \le N_{k.\text{доп.}},\ E[T_v(\lambda_i)] \le E[T_{v.\text{доп.}}(\lambda_i)],\ C_{\max}(\lambda_i, H) \le C_{\max\text{доп.}}(\lambda_i, H),\ \ i = \overline{1,k}, \quad (4)$$

где $E[T_v(\lambda_i)]$ – среднее время задержки при передаче *i*-го потока пакетов; N_k – в сети количества каналов, аппаратно-программных комплексов и терминальных средств;

Формула (3) и (4) показывают сущность рассматриваемой ММ для дальнейшего исследования сети.

Следует отметить, что одним из важных задач при оказании QoS и QoE трафиков является эффективность управления и распределения ресурсами в МТС. В данной системе коммутатор и контроллер с протоколом OpenFlow является центральным узлом сети SDN, принимающий решения по всем вопросам маршрутизации.

Рассмотрим поведения ММ в общем в виде как многоканальную систему массового обслуживания с очередями. Данная система имеет общий буферный накопитель с емкостью $N_{\text{бн}}$ и максимальное количество обслуживающих аппаратно-программных комплексов и терминальных средств N_k. При этом длительность обслуживания потоков пакетов имеет функцию распределения $B(t) = P[B \le t]$ с моментами b_i, $i = \overline{1,k}$. При этом условие, которое является необходимым и достаточным для существования стационарного режима системы следующее:

$$\rho = \sum_{i=1}^{k}[b_i \cdot (\lambda_{i.n} + \lambda_{i.c}) / N_k] \cdot f(H_i) \le 1,\ i = \overline{1,k}\ , \quad (5)$$

где $f(H_i)$ – функция, учитывающая свойство самоподобности нагрузки [7] и $H \in (1/2;1)$, то можно представить $f(H) = 2H$.

В условиях допустимой загрузки $\rho_{i.\text{доп.}}$, максимальная пропускная способность сети при обслуживании *i*-го потока пакета самоподобного трафика, определяется следующим выражением:

$$C_{i.\max}(\rho_i \le \rho_{i.\text{доп.}}) = \frac{N_k}{E[L_{i.n}]} \cdot E[V] \cdot (\rho_{i.\text{вх}} + \rho_{i.\text{исх}}) \cdot f(H_i) \le C_{i.\max.\text{доп.}}(\lambda_i), \quad i = \overline{1,k} \quad , \qquad (6)$$

где $\rho_{i.\text{вх}}, \rho_{i.\text{исх}}$ – соответственно, коэффициент загрузки сетей связи и $\rho_{i.\text{вх}} \le \rho_{i.\text{исх}}$; $E[L_{i.n}]$ – средняя длина передаваемого *i*-го потока пакета, $i = \overline{1,k}$.

Из (5) и (6) видно, что $C_{i.\max}(\rho_i \le \rho_{i.\text{доп.}})$ в зависимости от $E[V]$, $f(H)$ и N_k при заданном условии $\rho_{i.\text{вх}} \le \rho_{i.\text{исх}}$ ограничена. Кроме того, на базе формулы (5) и (6) может быть рассмотрен способ реализации метода обеспечения качества обслуживания QoS и QoE путем динамического распределения пропускной способности сетей связи с помощью прогнозирования в условиях самоподобия мультисервисного трафика.

Проведенные исследование показывают [5–9], что в связи с резко растущим объемом передаваемого трафика, генерируемого в мультисервисных беспроводных сотовых сетях различными услугами и приложениями, возникает проблема нехватки частотного диапазона F_k.

Для решения такие задачи необходимо использование различных планировщиков - управления частотно-временными ресурсами. В качестве примеров таких механизмов на базе технологии SDN, LTE, NFV и NR можно привести планировщики Round Robin (RR) и Full Power (FP). Их работа, которых основан на различных вариациях параметров сетевых ресурсного блока – частоты F_k, мощности P_c и времени T [7–10].

Теперь, в частном случае, рассмотрим количественные характеристики эффективности использования сетевых ресурсов МТС при использовании технологии построения распределенных сетей связи технологии как SDN&LTE [9, 10].

Одним из критериев, позволяющих сравнить эффективность выделенной частотной интервал для передачи трафика, является отношение числа затраченных ресурсных блоков к объему переданной уникальной информации:

$$R_c(F) = \sum_{j=1}^{T} R_j(F) \cdot [\sum_{j=1}^{T} k_j]^{-1} \quad , \quad j = \overline{1,T}$$

где T – общее время работы сетей связи; $R_j(F)$ – число ресурсных блоков, использованных для передачи в *j*-м субкадре; k_j – число полезных бит, передаваемых в *j*-м субкадре.

Таким образом, в результате исследование предложен ММ общего типа с ожиданиями и получены аналитических выражения для оценки веротяностно-временных характеристик сетей связи, использующие технологии концепции FN при оказании услуг.

Учитывая возможные сценарии использования технологии концепции NGN и FN, а также исследование сетевых ресурсов, стоит ожидать расширения области возможного применения данной технологии SDN, LTE и NR с развитием сетей мобильной систем передачи данных для обеспечения приемлемого показателей QoS и QoE.

Список используемых источников

1. Ефимушкин В. А., Ледовских Т. В., Иванов А. Б., Шалагинов В. А. Роль технологий SDN/NFV в инфраструктуре цифровой экономики. Опыт тестирования и внедрения // Электросвязь. 2018. № 3. С. 27–36.

2. Мухизи С., Мутханна А. С., Кричек Р. В., Кучерявый А. Е. Исследование моделей балансировки нагрузки в программно-конфигурируемых сетях// Электросвязь. 2019. № 1. С. 23–29

3. Ibrahimov B. G., Humbatov R. T., Ibrahimov R. F. (2018). Analysis performance multiservice telecommunication networks with using architectural concept future networks // T-Comm. Vol. 12, no. 12. pp. 84–88.

4. Пшеничников А. П. Этапы цифровизации сетей связи // Методические вопросы преподавании инфокоммуникаций в высшей школе. 2019. № 2. С. 65–71.

5. Ибрагимов Б. Г., Гумбатов Р. Т., Ибрагимов Р. Ф., Исаев А. М. Анализ показателей производительности мультисервисных телекоммуникационных сетей будущего поколения с использованием технологий программно-конфигурируемых сетей // Вестник компьютерных и информационных технологии. 2019. № 5. С. 39–44.

6. Bianco B., Fajordo J. O., Cianonoulakis et. all. Technology pillars in the architecture of future 5G mobile networks: NFV, MEC and SDN // Computer Standarts & Interfaces. 2017. Vol. 54, Part 4. pp. 216–228.

7. Шелухин О. И. Моделирования информационных систем. М.: Горячая линия – Телеком, 2018. 516 с.

8. Ибрагимов Б. Г., Гасанов А. Г., Алиева А. А., Исаев А. М. Исследование показателей качества функционирования мультисервисных телекоммуникационных сетей на базе архитектурной концепции будущих сетей // Надежность и качество сложных систем. 2019. № 1 (25). С. 88–95.

9. Митрофанов С. А. Обзор сценариев использования широковещательной передачи в сетях LTE // Информационно-управляющие системы. 2017. № 1. С. 63–70.

10. Sopin E., Samouylov K., Vikhrova O., Kovalchukov R., Moltchanov D., and Samuylov A. Evaluating a case of downlink uplink decoupling using queuing system with random requirements // Lecture Notes in Computer Science. 2016. Vol. 9870. pp. 440–450.

УДК 004
ГРНТИ 20.15.05

ИССЛЕДОВАНИЕ И ТЕСТИРОВАНИЕ СМАРТ КОНТРАКТОВ В БЛОКЧЕЙН СЕТИ IOTA

К. А. Дворецков, А. А. Мартынюк,
К. Б. Миронов, П. А. Огорельцев, А. В. Помогалова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевич

Работа посвящена тестированию реализации смарт-контрактов в децентрализованной блокчейн-сети IOTA. Актуальность данной проблемы связана с ростом популярности интернета вещей и нужды увеличивающейся функциональности сети в связи с этим.. В рамках данной работы разрабатывается и тестируется приложение, разработанное на базе блокчейн-платформы IOTA, целью которого является демонстрация работы смарт-контрактов для умных устройств, а также тестирование работоспособности и стабильности данных смарт-контрактов.

блокчейн, IOTA, смарт-контракт, децентрализация, EVM.

В сети IOTA реализован протокол без «лидирующего узла», что позволяет всем пользователям создавать новые транзакции, тогда как протокол консенсуса в сети IOTA позволяет параллельно добавлять транзакции в блок, пока он находится на стадии добавления. Из-за этого сеть может обрабатывать большое количество операций одновременно, легко масштабироваться и иметь низкое время подтверждения, при том, что все транзакции выполняются бесплатно. Это необходимо для интеграции криптовалют в интернете вещей, что и является основной целью технологии [1].

На момент написания статьи основная сеть IOTA 1.5 работает на Hornet и Bee узлах (нодах), которые написаны на Go и Rust соответственно. Они не поддерживают смарт контракты, но разработка уже позволяет пользователям подключать свои устройства к основной сети и участвовать в ней. Одной из основных целей IOTA Foundation является полная децентрализация и реализация сети IOTA 2.0 с реализацией смарт-контрактов. В данный момент существует частичная поддержка языка Solidity и Ethereum Virtual Machine. В данный момент частичная поддержка смарт контрактах реализована на нодах GoShimmer в связке с Wasp нодой. В отличии от IOTA 2.0 DevNet GoShimmer не расчитан быть тестовой сетью с контролируемой средой, он является полноценной децентрализованной сетью, который каждый разработчик должен настраивать локально самостоятельно. GoShimmer основан на нодах основной сети – Bee и Hornet. В итоге разработки IOTA 2.0 и GoShimmer будут являться отдельными проектами, не похожими друг на

друга [2]. GoShimmer позволит создавать децентрализованные приложения с эффективным энергопотреблением, которая равняется менее, чем одной миллиардной от киловатта, а также не будет требовать комиссии за транзакции, в отличии от таких платформ, как Bitcoin и Ethereum [3].

Проект стремительно развивается и скоро будет доступна полная поддержка и реализация смарт-контрактов. Также с помощью блокчейн-сети IOTA, разработчики собираются работать с анализом больших данных.

Для обеспечения безопасности в блокчейне используется фреймворк ISC. ISC –это фреймворк для создания распределенных реестров; следовательно, он открыт для всевозможных конфигураций. Приведенный выше обзор стимулирования является основой для различных подходов к вопросу безопасности в цепочке для конкретных случаев использования.

Для создания децентрализованного приложения с помощью блокчейн платформы IOTA нужно настроить сеть на основе GoShimmer, который позволяет гибко настроить количество узлов и будущую масштабируемость сети. Поскольку на данный момент GoShimmer является лишь прототипом, IOTA Foundation не рекомендует основывать на нем конечные приложения [4]. За смарт контракты отвечает Wasp нода, которая подключается к GoShimmer сети. Данная нода поддерживает смарт контракты на основе Rust/WASM и частично поддерживает Solidity/EVM, но в будущем планируется поддержка всех виртуальных машин и полной поддержки языка Solidity. Wasp создан для подтверждения и запуска смарт-контрактов в цепь, при этом каждый пользователь сети может создать новую цепь, которая будет независима от других (рис. 1) [5].

Как говорилось выше, IOTA поддерживает возможность организации создания децентрализованных приложений, это возможно за счет смарт-контрактов IOTA с помощью которых можно определить свою цепочку и создать валидаторов для проверки транзакций. Валидатором будет являться реальное устройство, которое заинтересовано поддержать защиту целостности, проверив ее посредством участия в распределенном консенсусе. Валидатор идентифицируется в сети по своему открытому ключу, но не раскрывает каким образом будет проверять цепочку. Валидатор имеет один или несколько узлов для проверки своей цепочки. Каждый узел валидатора проверяет цепочку от его имени, которая ему принадлежит. Чтобы подтвердить цепочку, валидаторы объединяются в группы, называемые комитетом, далее на основе общего решения происходит фиксация цепочки в сети. Состав комитета для подтверждения может изменяться в зависимости от модели управления.

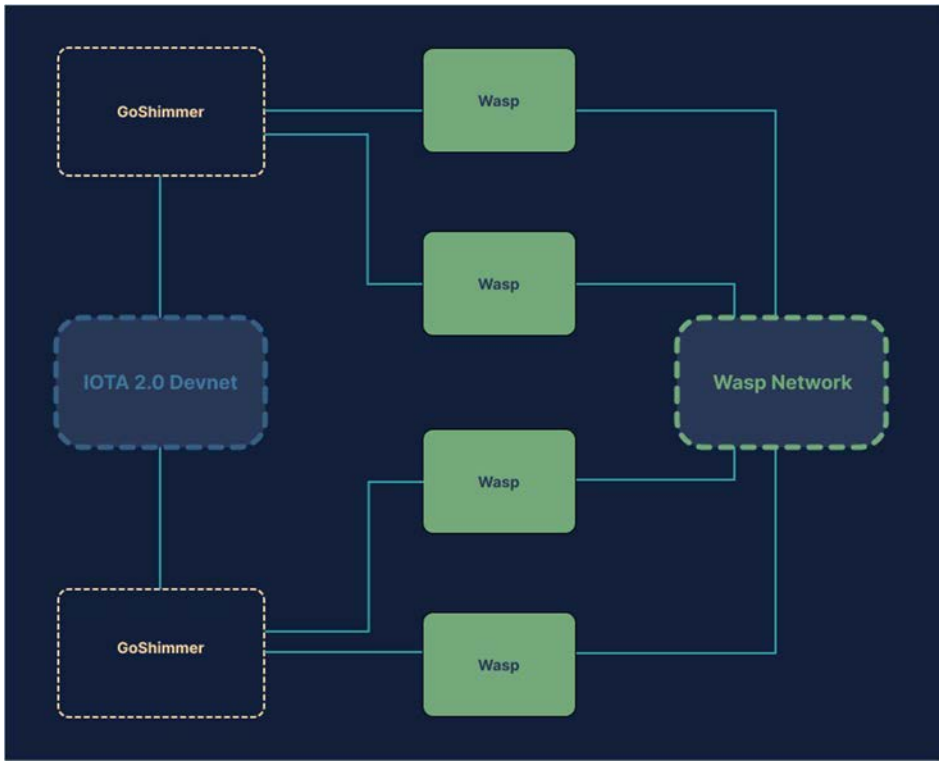


Рис. 1. Архитектура приватной сети IOTA

Для подтверждения используется анкерный механизм регистра UTXO на уровне L1, где находятся валидаторы, он дает следующие возможности:

– гарантирует глобальный консенсус относительно состояния цепи, подделать цепь невозможно;

– делает состояние неизменяемым и защищенным от несанкционированного доступа;

– делает переходы состояния управляемыми, атомарными и согласованными с остатком активов;

– делает состояние данных глобальным и объективным внутри цепочки, что является требованием для квази-Тьюринга полных смарт-контрактов.

Состояние данных цепочки являются набором пар ключ/значение. Каждый ключ и каждое значение пары являются произвольным массивом байтов. Пары ключ/значения состояния данных используются для реализации всех видов концепций блокчейн-транзакций: от обычных счетов, до специфических данных в смарт-контрактах.

ISC-концепция состояния цепи немного отличается от той же концепции в блокчейнах: состояние цепочки в ISC представляет собой общий набор пар ключ/значение, по сути, переменных состояния и его значения.

В цепочках ISC используется более эффективная модель обязательств по состоянию, используя так называемое дерево Веркле: дерево, основанное на векторных обязательствах, принятых узлами дерева для своих дочерних

узлов. Данные векторные соглашения обычно основаны на криптографии, отличной от хэш-функций, используемых в деревьях Меркла [6].

В качестве примера разработано приложение (рис. 2), позволяющее покупать товар и отслеживать статистику, какой товар является наиболее популярным.

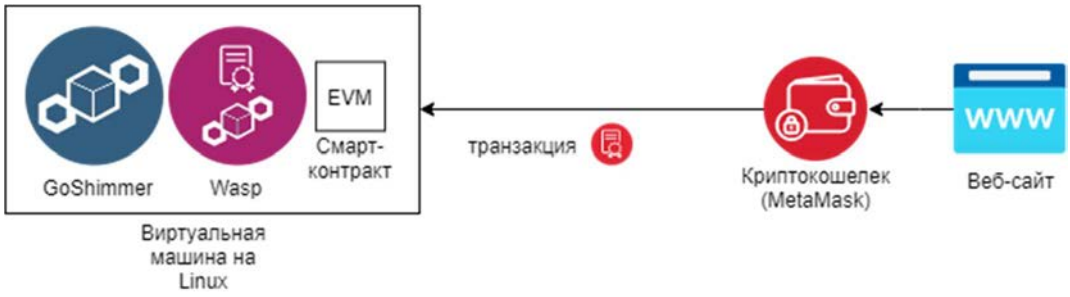


Рис. 2. Схема работы технической стороны проекта

В связи с отсутствием документации для внутренних смарт-контрактов нода WASP была подключена к виртуальной машине Ethereum, что позволило реализовать смарт-контракт на языке Solidity. Была реализована приватная сеть GoShimmer-WASP-EVM [4], способная выполнять смарт-контракты в децентрализованной сети. Далее был написан непосредственно сам смарт-контракт и создан сайт, взаимосвязь была налажена с применением библиотеки web3.js и кошелька Metamask. Это позволяет пользователям взаимодействовать с сетью и совершать транзакции непосредственно через графический интерфейс и веб-кошелек Metamask. На разработанном сайте для пользователя полностью реализован функционал для оплаты услуги и просмотра того, что он оплатил. Администратор со своей стороны также имеет возможность просмотра оплаты и статистики покупок, а также функционал для удаление и ручного добавления.

Функциональные возможности смарт-контракта:

1. Принятие оплаты за услугу и проверка на возможность оплаты;
2. Создание аккаунта после оплаты для сохранения данных;
3. Получение информации об определенном пользователе или что уже было оплачено;
4. Возможность удаление информации о пользователе и обо всех клиентах.

В рамках проведенного исследования было разработано полноценное приложение на базе приватной блокчейн-сети с установленным смарт-контрактом и интеграцией веб-интерфейса для взаимодействия с системой на базе программного клиента IOTA, а также оценена возможность применения текущей реализации системы для разработки маломощных решений с использованием смарт-контрактов.

Список используемых источников

1. Akhtar, Mohd & Rizvi, Danish & Ahad, Mohd & Kanhere, Salil & Amjad, Mohammad & Coviello, Giuseppe. Efficient Data Communication Using Distributed Ledger Technology and IOTA-Enabled Internet of Things for a Future Machine-to-Machine Economy // Sensors. 2021. N21 4354.
2. IOTA Foundation. IOTA x Shimmer x Assembly. 2021. URL: https://blog.iota.org/iota-shimmer-assembly (дата обращения: 27.03.2022)
3. Navin Ramachandran. Energy Benchmarks for the IOTA Network (Chrysalis Edition). 2021. URL: https://blog.iota.org/internal-energy-benchmarks-for-iota (дата обращения: 27.03.2022).
4. IOTA Foundation. GoShimmer Node. URL: https://wiki.iota.org/goshimmer/welcome (дата обращения: 27.03.2022).
5. IOTA Foundation. Wasp Node. URL: https://wiki.iota.org/smart-contracts/overview (дата обращения: 27.03.2022).
6. Evaldas Drąsutis IOTA Smart Contracts 2021. URL: https://files.iota.org/papers/ISC_WP_Nov_10_2021.pdf (дата обращения 27.03.2022).

Статья представлена
директором НИИ «Технологии связи», доцентом кафедры ИКС СПбГУТ,
кандидатом технических наук, доцентом В. С. Елагиным.

УДК 004
ГРНТИ 20.15.05

РАЗРАБОТКА ПЛАТФОРМЫ-АГРЕГАТОРА ДЛЯ СИСТЕМ ЛОЯЛЬНОСТИ С ПРИМЕНЕНИЕМ ТЕХНОЛОГИИ БЛОКЧЕЙН

К. А. Дворецков, А. А. Мартынюк, А. В. Помогалова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевич

Технология Blockchain считается наиболее инновационной и перспективной технологией нашего времени. Технология набирает обороты в самых разных сферах. Актуальность применения технологии обоснована неизменностью вносимой информации, обеспечением уровня безопасности активов пользователей в системе. Данная работа посвящена разработке платформы по агрегации систем лояльности для ритейл сегмента и созданию инструмента для хранения и использования цифровых карт лояльности, а также разработке нового функционала для работы с этим инструментом. Также в данной работе освещаются проблемы нынешних систем лояльности, как данные проблемы можно решить с применением блокчейн технологий.

блокчейн, децентрализованные приложения, система лояльности.

В современном мире большое количество внимания уделяется системам лояльности [5]. Многие компании ими пользуются с целью привлечения и удержания клиентов. На данный момент времени в системах лояльности существует ряд проблем [6], который необходимо решить. С помощью перевода карт для систем лояльности из привычного пластикового вида в цифровой с применением технологии блокчейн [2], сразу будут решены несколько насущных в данный момент времени задач:

– безопасность: вероятность доступа извне, использование бонусов другими, проведение не верифицированных операций;

– системы лояльности до сих подразумевают под собой выпуск пластиковых карт, каждый год сотни тысяч карт, что создает тонны мусорного пластика после окончания эксплуатации;

– дополнительные сложности при утери пластиковой карты: выпуск новой, восстановление при условиях;

– сложности с работой текущих сервисов: скорость работы текущих решений ниже средней;

– на рынке систем лояльности царит олигополия, без чистой конкуренции. Это вызывает застой, нехватку новых идей для совершенствования систем лояльности;

– ограниченность функционала: нехватка гибкости, различных интересных действий над бонусами, которые могут заинтересовать клиентов;

– у текущих решений низкая скорость работы.

Все вышеуказанные проблемы поможет решить система лояльности, разработанная на базе технологии блокчейн [1]. Благодаря применению технологии блокчейн обеспечивается безопасность системы в целом: в отношении некоторых персональных данных, как ограничив недоступностью к ним извне, так и невозможность использования, например, баллов третьими лицами, так как за это будет отвечать блокчейн, который способен принять решение о корректности операции по списанию: действиями с цифровой картой системы лояльности. Такая система не подвержена взлому. Она направлена на совершение верифицированных операций лицом, которому принадлежат бонусы.

Разработка нового функционала, необходимого пользователям [3]: перевод бонусов и их обмен на другие (между различными компаниями). Таким образом, новая система лояльности приобретает существенную гибкость по сравнению с другими: ненужные бонусы можно будет обменять на другие. Всё будет в одном месте, а именно в приложении для мобильного устройства: хранение и возможность использования бонусов пользователями.

Проводимое исследование и разрабатываемая платформа также предполагает упрощения в плане использования приложения для конечного

пользователя [3]. Пластиковые карты для систем лояльности станут полностью цифровыми, что уменьшит количество вторичного пластика с целью улучшения экологической ситуации. Ритейлер сможет легко и быстро организовать работу своей системы лояльности и также скорректировать её под себя при имеющейся необходимости.

Несмотря на то, что платформа-агрегатор для систем лояльности с первого взгляда может обладать некоторыми схожими с другими решениями, функционалом, однако разрабатываемый функционал будет реализован с помощью блокчейна [2], придающему платформе уникальность. Функционал содержит в себе:

– слуги по предоставлению возможности создать свою систему лояльности;

– размещение рекламных постов;

– доступ к функционалу для передачи (рис. 2) и обмена бонусами (рис. 3);

– выпуск и закрытие цифровых карт;

– карта будет выглядеть привычным образом, всегда виден баланс бонусов, можно будет воспользоваться штрих-кодом карты [4];

– выпуск кобренд-карты (единая карта у одного пользователя для двух или более фирм);

– просмотр профиля пользователя (рис. 1), с его данными и картами;

– клубы (получение привилегий, акции для «своих»). Пользователь может попадать в клуб как автоматически, так и по приглашению;

– выпуск и закрытие купонов (QR коды) и промокодов (расширенный функционал для фирм);

– поддержка полной истории действий с бонусами (с купонами и промокодами, если таковые присутствуют);

– возможность добавление карт для использования, у которых необходимо предоставить штрих код или номер (в этом случае не будет поддержки истории, однако быстрый доступ без пластика будет обеспечен);

– биржа обмена бонусами с возможностью поиска доступных лотов и фильтрацией;

– возможность создания лота на бирже обмена;

– перевод бонусов пользователю по его ID.

Проводимая разработка предоставляет гибкое решение для бизнеса, учитывая пожелания для компаний. Компании смогут на свое усмотрение изменить некоторые установки. Например, при обмене бонусов они могут задать нижнюю цену для своих бонусов, для предотвращения их возможного обесценивания или манипуляции.

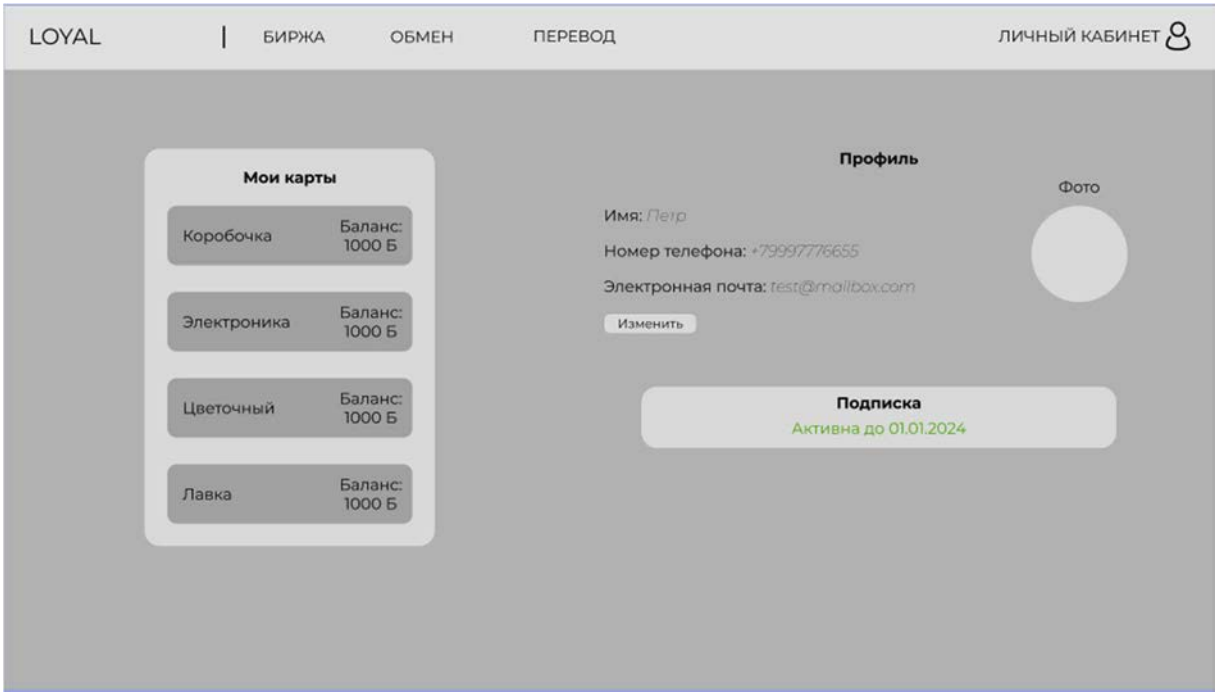


Рис. 1. Макет профиля пользователя

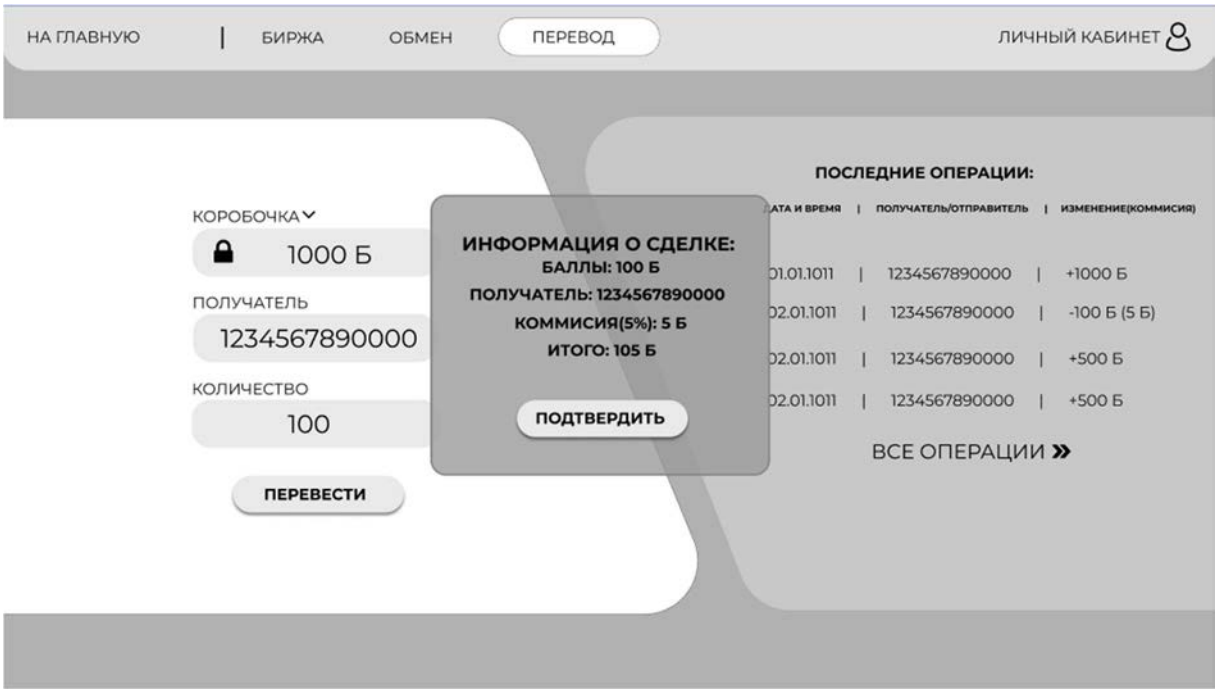


Рис. 2. Макет процесса перевода бонусов

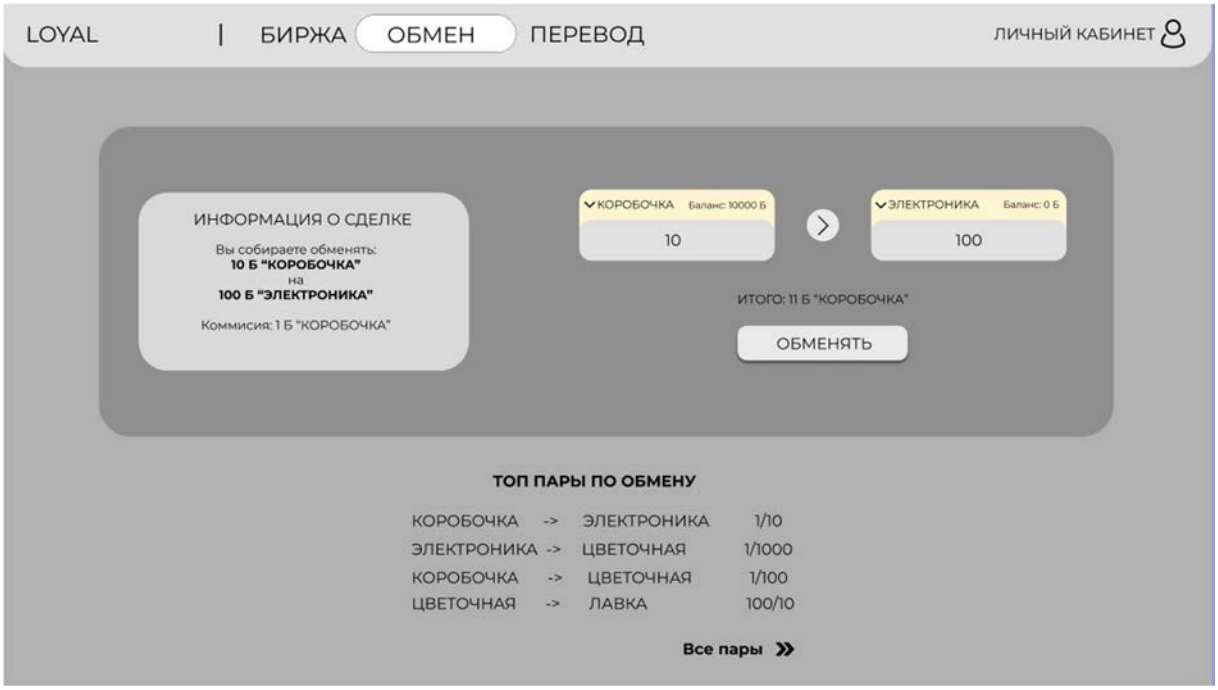


Рис. 3. Макет процесса обмена бонусами

Главная мотивация использования новой платформы лояльности для компаний – приток клиентов, их привлечение нестандартной системой лояльности, учитывающей нужды клиента, и популярной технологией блокчейн. Данное решение служит опорой для бизнеса компании и, в дальнейшем, станет стимулятором его роста.

Список используемых источников

1. Какие бывают программы лояльности и как их внедрять. URL: https://www.carrotquest.io/blog/programma-loyalnosti/ (дата обращения: 25.03.2022).

2. Блокчейн: что нам стоит кейс построить? URL: https://habr.com/ru/post/449986/ (дата обращения: 25.03.2022).

3. DApps: если я добавлю функционал, придут ли пользователи? URL: https://habr.com/ru/post/568480/ (дата обращения: 25.03.2022)

4. Система быстрых платежей. URL: https://habr.com/ru/company/nspk/blog/586876/ (дата обращения: 25.03.2022).

5. Что такое программа лояльности. URL: https://netology.ru/blog/loyalty-sale (дата обращения: 25.03.2022).

6. Программы лояльности: плюсы, минусы, варианты. URL: https://www.nic.ru/info/blog/loyalty-programs/ (дата обращения: 25.03.2022).

Статья представлена
директором НИИ «Технологии связи», доцентом кафедры ИКС СПбГУТ
кандидатом технических наук, доцентом В. С. Елагиным.

УДК 004.056.5
ГРНТИ 49.44.31

АНАЛИТИЧЕСКАЯ МОДЕЛЬ МЕХАНИЗМА ЗАЩИТЫ КРИТИЧЕСКИХ ТЕЛЕКОММУНИКАЦИОННЫХ ИНФРАСТРУКТУР

М. М. Джавадова[2], Б. Г. Ибрагимов[1], Т. Г. Мамедов[3], М. Я.Оруджова[1]

[1]Азербайджанский Технический Университет
[2]Азербайджанский архитектурно-строительный университет
[3]Военная академия Вооруженных сил Республики Азербайджан

Проанализированы модели и механизмы защиты критических телекоммуникационных инфраструктур с учетом информационно-технического воздействия на системы связи и характеристик защиты информации системы телекоммуникации и управления важного объекта в критических инфраструктурах. На основе анализа и уточнения требования эффективности технических средств системы защиты информаций предложен новый подход к построению аналитической модели и механизма защиты критических телекоммуникационных инфраструктур. В данной работе исследуется новый подход с целью оценки характеристик телекоммуникационных систем, функционирующих в критических инфраструктурах и управления важного объекта в условиях воздействия непреднамеренных различных источников угрозы безопасности.

критическая инфраструктура, *информационная безопасность, система связи и управления, система безопасности и защиты информации, система телекоммуникации.*

В настоящее время обеспечение безопасности, управления и защиты критических телекоммуникационных инфраструктур стало в ряд важнейших стратегических задач, которое должно обеспечивать каждое государство в целях повышения качества защиты.

Бурное развитие единой информационной инфраструктуры и единой многооператорской среды на основе программы цифровой экономики требует новые фундаментальные принципы и адекватные подходы к построению высокоэффективных систем телекоммуникационных инфраструктур на базе архитектурной концепции следующих NGN (*Next Generation Network*) и будущих сетей FN (*Future Network*), использующих перспективные и инновационные технологии [1].

Одним из реальных путей решения проблемы для защиты критических телекоммуникационных инфраструктур и управления безопасностью, а также управления критически важного объекта системы телекоммуникации является широкое внедрение в практику строгих методов математического моделирования, среди которых доминирующее положение занимают

аналитические модели и методы, которые базируются на теории мультисервисных сетей и систем массового обслуживания.

Действительно, когда речь идет «о защите критически важных объектов, основной задачей системы информационной безопасности является обеспечение» их «нормального функционирования без существенных нарушений, последствия которых и определяют категорию значимости телекоммуникационной системы, используемой в этих процессах, а категория значимости – состав мер защиты» [1, 2].

В настоящее время вопросы безопасности телекоммуникационных и информационных систем объектов критической инфраструктуры приобретают важное значение.

Актуальность проблемы обеспечения эффективности информационной безопасности в государственных информационных системах и в критических телекоммуникационных инфраструктурах обоснована высоким спросом на системы такого класса.

Отметим, что эффективность системы защиты критических телекоммуникационных инфраструктур, многооператорских сред и государственных информационных систем в значительной степени зависит от уровня ее безопасности и устойчивости функционирования.

Учитывая требования эффективности технических средств системы защиты информаций и выбор критерии для анализа и оценки характеристик важного объекта системы телекоммуникации необходим новый подход. С целью создания нового подхода формализована процедура оценки эффективности технических средств системы защиты информации в критических телекоммуникационных инфраструктурах, которых можно представить вектором критериев. Эту процедуру, векторы критерий и функциональные зависимости показателей эффективности на основе нового подхода можно описать следующим образом:

$$E_{EF}(\lambda_i,t) = W[K_{\text{ИБ}}(\lambda_i,t), C_{EE}(\lambda_i), U(\lambda_i,t)], \quad i=\overline{1,n}\ , \qquad (1)$$

где $K_{\text{ИБ}}(\lambda_i)$ – функция, учитывающая критерии информационной безопасности функционирования программно-аппаратных средств системы защиты критических телекоммуникационных инфраструктур и государственных информационных систем при обслуживании i-го потока пакетов трафиков с интенсивностью λ_i, $i=\overline{1,n}$ в момент времени t; $C_{\text{ЕЕ}}(\lambda_i)$ – функция, учитывающая экономическую эффективность системы защиты критических телекоммуникационных инфраструктур при обслуживании i-го потоков пакетов трафиков, $i=\overline{1,n}$; $U(\lambda_i,t)$ – функция, учитывающая критерии устойчивости функционирования программно-аппаратных средств системы защиты кри-

тических телекоммуникационных инфраструктур и государственных информационных систем при обслуживании *i*-го потока пакетов трафиков, с интенсивностью λ_i, $i=\overline{1,n}$.

Выражение (1) определяет сущность рассматриваемого нового подхода с помощью которого выбраны и формализованы критерии оценки технических средств системы защиты информации в критически важных объектах телекоммуникационных инфраструктурах при выполнении требуемых телекоммуникационных процессов. Кроме того, в (1) особое место занимает среднее значение стоимости в группе системы защиты информации аппаратно-программных комплексов критических телекоммуникационных инфраструктурах $E[C_{\text{ЕЕ}}(\lambda)]$, которые являются функциональные, устойчивые и защитные характеристики [3–5].

Экономическая стоимость системы защиты аппаратно-программных комплексов критических телекоммуникационных инфраструктур [4–6]:

$$C_{\text{ЕЕ}}(\lambda)=\max_i[C_{i.AP}(\lambda)] \text{ при } C_{i.AP}(\lambda)\geq E[C_{AP}(\lambda)],\quad i=\overline{1,n}. \qquad (2)$$

Аналогично, низкая стоимость *i*-го системы защиты информации аппаратно-программных комплексов $C_{i.AP}(\lambda)$ критических телекоммуникационных инфраструктур при обслуживании потока пакетов трафиков с интенсивностью λ выражается следующим:

$$C_{EE}(\lambda)=\min_i[C_{i.AP}(\lambda)] \text{ при } C_{i.AP}(\lambda)<E[C_{AP}(\lambda)],\quad i=\overline{1,n} \qquad (3)$$

С учетом (2) и (3) можно определить среднее значение стоимости в группе системы защиты информации аппаратно-программных комплексов критических телекоммуникационных инфраструктур $E[C_{\text{ЕЕ}}(\lambda)]$, которое определяется следующим выражением:

$$E[C_{\text{ЕЕ}}(\lambda)]=\frac{1}{N_{AP}}\cdot\sum_{i=1}^{N_{AP}}C_{i.ap}(\lambda)\ ,\quad i=\overline{1,n}\ , \qquad (4)$$

где N_{AP} – количество в группе системы защиты информации аппаратно-программных комплексов в критических телекоммуникационных инфраструктурах и государственных информационных системах.

На основе предлагаемого подхода построена математическая модель подсистем безопасности и защиты информации в системах телекоммуникации и управления важного объекта в критических государственных инфраструктурах [1, 7, 8]. К такой системе предъявляются довольно жесткие требования по надежности, методы обеспечения которых прописаны

в рекомендациях G.983 МСЭ-Т. Выход из строя различных элементов критических систем доступа в разных узлах сказывается на имидже многооператорской среды.

В работе [1, 2, 4] рассмотрены возможности управления безопасностью критических информационных инфраструктур и предложены новые подходы к построению модели на фиксированный список угроз, а также обоснована возможность построения курса безопасности на основе мониторинга событий безопасности. В работе [2, 3, 6] изложен метод для защиты критических телекоммуникационных инфраструктур в целях повышения качества защиты. Помимо этого, данная задача широко освещена авторами ряда научных публикаций [1-5] для управления важного объекта в критических телекоммуникационных инфраструктурах.

Целью данной работы является разработка нового подхода к построению аналитической модели оценки характеристик телекоммуникационных систем, функционирующих в критических инфраструктурах и управления важного объекта в условиях воздействия непреднамеренных различных источников угрозы безопасности.

Для реализации поставленной задачи предложены аналитическая модель и механизм защиты критических телекоммуникационных инфраструктур с использованием эффективного метода защиты и управления критически важного объекта, которые описываются следующим образом:

$$E[F_j(t, A_i)] = W\{\arg\max_j \ [Y_j(A_i, t)] \ , \ j = \overline{1, N} \ , \ \ i = \overline{1, n}\} \qquad (5)$$

при следующих ограничениях

$$K_{of.}(\lambda_i) \le K_{of.\text{доп.}}(\lambda_i) \, , \ \mathrm{C}_{\max}(\lambda_i, t) \ge \mathrm{C}_{\max.\text{доп.}}(\lambda_i, t) \, , \ M_j(t, \lambda_i) \le M_{j.\text{доп.}}(t, \lambda_i) \, , \qquad (6)$$

где $Y_j(A_i, t)$ – в телекоммуникационной сфере, ожидаемая величина ущерба ИКТ-инфраструктуры и управления критически важного объекта к моменту времени t – при преднамеренном и деструктивном информационно-техническом воздействии на системы связи; $\mathrm{C}_{\max}(\lambda_i, t)$ – пропускные способности аппаратно-программных комплексов систем защиты критических телекоммуникационных инфраструктур с учетом скорости поступления входящего потока λ_i при обработке i-го трафика, $i = \overline{1, n}$; $M_j(t, \lambda_i)$ – функция, учитывающие эффективные показатели защищенности системы в критических телекоммуникационных системах и государственных информационных инфраструктурах с интенсивностью λзащиты информации в момент времени t. $K_{i.o}(\lambda_i)$ – коэффициент опасности функционирования системы обслуживании i-го потока пакетов трафиков с интенсивностью λ, $i = \overline{1, n}$;

Выражения (5) и (6) определяют сущность рассматриваемого нового подхода с учетом комплексных показателей механизма защиты критических телекоммуникационных систем и управления важного объекта в критических инфраструктурах при деструктивном информационно-техническом воздействии на системы связи. Кроме того, выражения (5) и (6) характеризуют комплекс вопросов по обеспечению безопасности и защите окружающей среды от различных внешних и внутренних угроз.

Рассмотрим случай, когда система защиты окружающей среды от различных внешних и внутренних угроз в системе защиты информации является идеальным $K_i^*(\lambda_i)$. Идеальной системе защиты информации соответствует вектор, в котором все значения критериев равны единице $\sum_{i=1}^{n} K_i^*(\lambda_i) \to 1$. Для оценки эффективности системы защиты информации критических телекоммуникационных инфраструктур вводится скалярная величина, равная Евклидову расстоянию $E_b(D)$ между наилучшим вектором и вектором критериев, полученному при обслуживании *i*-го потока пакетов [2, 5, 7, 9].

С учетом (5) и (6) Евклидово расстояние между наилучшим вектором и вектором критериев для *j*-й группы системы защиты информации в критических телекоммуникационных инфраструктурах рассчитывается по формуле:

$$E_i(D) = \sqrt{\sum_{j=1}^{N} [K_{i,j}^*(\lambda) - K_{i,j}(\lambda)]^2} \quad , \quad j = 1,...,N \quad , \quad i = \overline{1,n} \qquad (7)$$

Выражение (7), характеризует возможное состояние системы защиты информации критических объектов, для которой расстояние до наилучшего вектора окажется наименьшим, можно считать наиболее эффективным для защиты информации в критических телекоммуникационных системах.

Список используемых источников

1. Ерохин С. Д., Петухов А. Н., Пилюгин П. Л. Событийно-ориентированная политика безопасности и формальная модель механизма защиты критических информационных инфраструктур // Труды учебных заведений связи. 2019. Т. 5. № 4. С. 99–105.

2. Давыдов А. Е., Максимов Р. В., Савицкий О. К. Защита и безопасность ведомственных интегрированных инфокоммуникационных систем. М.: Воентелеком, 2017. 536 с.

3. Ибрагимов Б. Г., Мамедов Т. Г. Исследованиее характеристик защиты информации системы телекоммуникации и управления важного объекта в критических инфраструктурах // Всероссийская НТК «Телекоммуникационные и вычислительные системы» (13–15 декабря). МТУСИ, Москва, 2021. С. 170–173.

4. Воробьев В. И., Рыжков С. Р., Фаткиева Р. Р. Защита периметра облачных вычислений // Программные системы: теория и приложения. 2015. Т. 6, № 1. С. 61–71.

5. Ибрагимов Б. Г., Мамедов Р. М., Мамедов Т. Г. Исследования эффективности волоконно-оптических линий связи с использованием квантовой технологии // Сборник трудов XV – Международной отраслевой научно-технической конференции "Технологии Информационного Общества" (03–04 марта). МТУСИ, Москва. Т. 1, 2021. С. 37–39.

6. Гринберг А. С., Горбачев Н. Н., Тепляков А. А.Защита информационных ресурсов государственного управления – М. : ЮНИТИ, 2003. – 327 с.

7. Anisimov V. G., Zegzhda P. D., Anisimov E. G., Bazhin D. A. A Risk-Oriented Approach to the Control Arrangement of Security Protection Subsystems of Information Systems // Automatic Control and Computer Sciences. 2016. Т. 50. № 8. С. 717–721.

8. Хорошко В. А. Методы и средства защиты информации. М.: Юниор, 2003. 504 с.

9. Senderov S. M., Yusifbeyli N. A., Rabchuk V. I., Huseynov A. M., Nasibov V. Kh., Guliyev G. B., Vorobev S. V., Smirnova E. M. Modern problems of energy security of the Caspian regions of Russia and Azerbaijan // International Conference Green Energy and Smart Grids. 2018. Vol. 69. pp. 5–9.

УДК 004.491.42
ГРНТИ 81.93.29

ИССЛЕДОВАНИЕ ШИФРОВАЛЬЩИКА GANDCRAB

Д. С. Дмитриева, А. В. Красов, В. М. Пилипова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Программы-шифровальщики относятся к классу троянцев-вымогателей – это вредоносное ПО, которое вносит несанкционированные изменения в пользовательские данные или блокирует нормальную работу компьютера. Для расшифровки данных и разблокировки компьютера злоумышленники обычно требуют денежного перевода (выкупа). Основной целью данной исследовательской статьи является поэтапное знакомство с развитием одной из таких программ-шифровальщиков – GandCrab, занявшего 40% рынка в пик активности, нюансами работы, а также показательный разбор данного шифровальщика в зависимости от уровня подготовки.

шифрование данных, история вируса, версии программного продукта, пользовательская информация

Введение

Из определения класса троянцев-вымогателей, главным критерием успеха для создателей обычно является количество заработанных на этом денег. Разработчики GandCrab заявили, что собираются «уйти на заслуженную пенсию», так как в общей сложности выкупы принесли преступникам более 2 миллиардов долларов.

На момент написания статьи было выпущено 5 версий данного шифровальщика. Давайте коротко взглянем на историю развития версий GandCrab, чтобы увидеть общую картину.

Рис. 1. Версии GrandCrab

Как видите, всего существует пять версий вредоноса. Все они являются ответом на появление дескрипторов, то есть дешифраторов данных. Актуальной версией на момент написания статьи является GandCrab V5.2.

Исследование вредоноса

В результате неосторожного скачивания зараженного файла на рабочем столе появляется подозрительный документ формата txt, а все файлы оказываются зашифрованы.

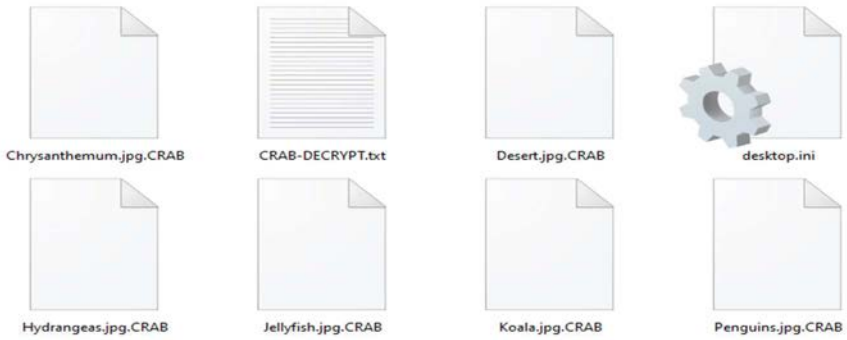


Рис. 2. Подозрительные файлы, скачанные из интернета

При открытии txt файла, пользователь увидит это:

Рис. 3. Содержимое .txt файла GandCrabv3

Коснемся вопроса геополитики разработчиков. И здесь интересно: разработчики не работают с СНГ регионом. Проявляется это в том, что GandCrab не работает с системой, в которой выставлен, к примеру, русский.

Причем именно язык системы, а не выставленная раскладка.

Предположим, вы захотели получить экземпляр вируса (в целях исследования), какие Ваши действия?

Например, нас интересует версия GandCrab v.4. Для этого переходим на virusign и ищем необходимый нам вирус.

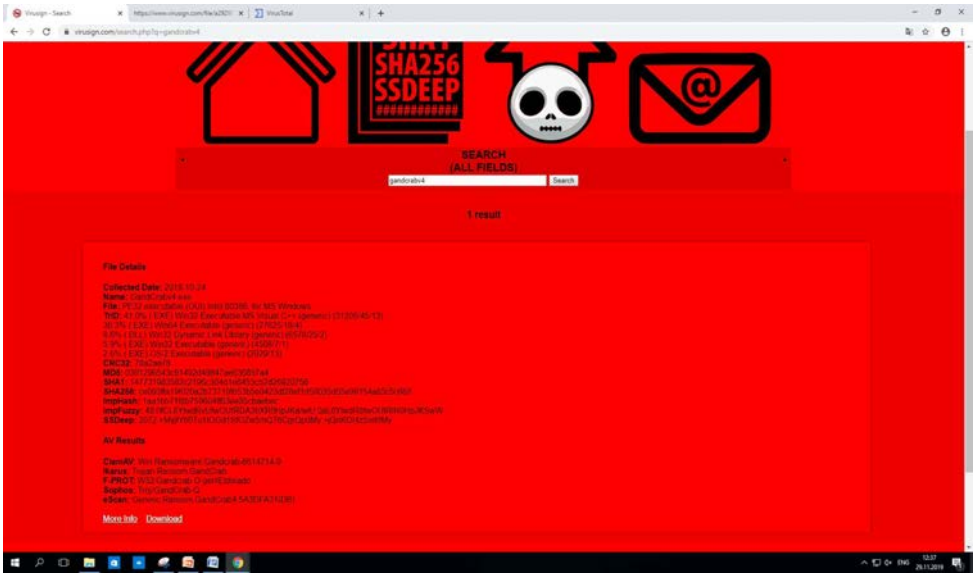


Рис. 4. Поиск необходимой версии вируса на сайте virusign.com

Однако мы не можем полагаться только на название, так как под одним именем могут скрываться разные версии вредоноса. Для более точного нахождения вируса, нужно знать его хэш-функцию. Для этого используем ресурс VirusTotal.

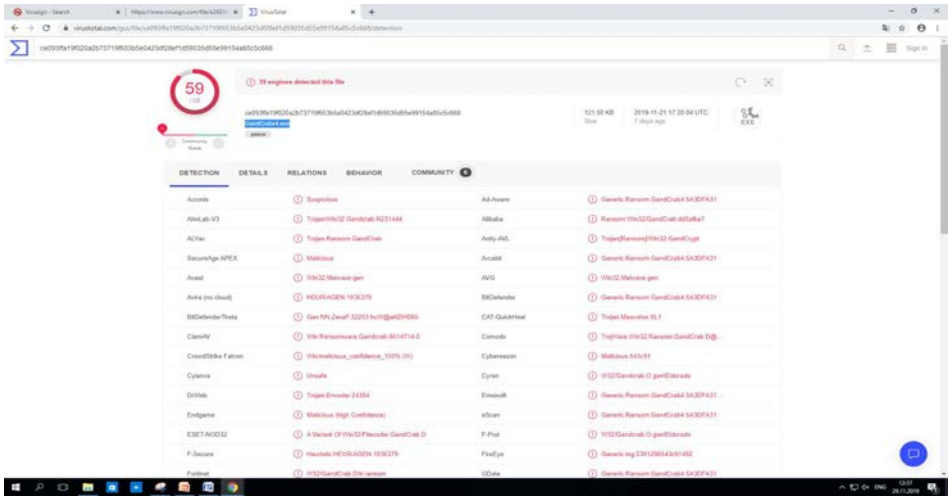


Рис. 5. Определение версии вируса с помощью интернет-ресурса VirusTotal

Также необходимо учесть, как минимум три нюанса:

1) Имеет смысл пользоваться версиями старше v4.3, так как ее сложно дизассемблировать, также для ранних версий вируса можно использовать инструмент «Песочница» от Microsoft – старшие версии знают об этой уязвимости. Более разумно использовать VirtualBox или VMware для исследования.

2) Старшие версии поддерживают Windows Server 2003 и Windows XP.

3) Возможно несколько вариантов исследования вирусов:

– (Для продвинутых пользователей) Если мы используем VMware, у нас появляется возможность изучать дампы файла гостевой системы в основной ОС с помощью специальных утилит. Подробное описание подобного исследования [1].

– (Для любителей) Мы можем использовать в том числе VB, в этом случае мы ограничимся утилитой Program Hacker.

Составим предполагаемую схему работы:

1) Сбор информации жертвы. Не работает с русской версией системы.

2) Отправка данных пользователя. В коде вируса есть адреса скомпрометированных сайтов, к которым он последовательно подключается и по протоколу Post пытается передать необходимые данные о пользователе.

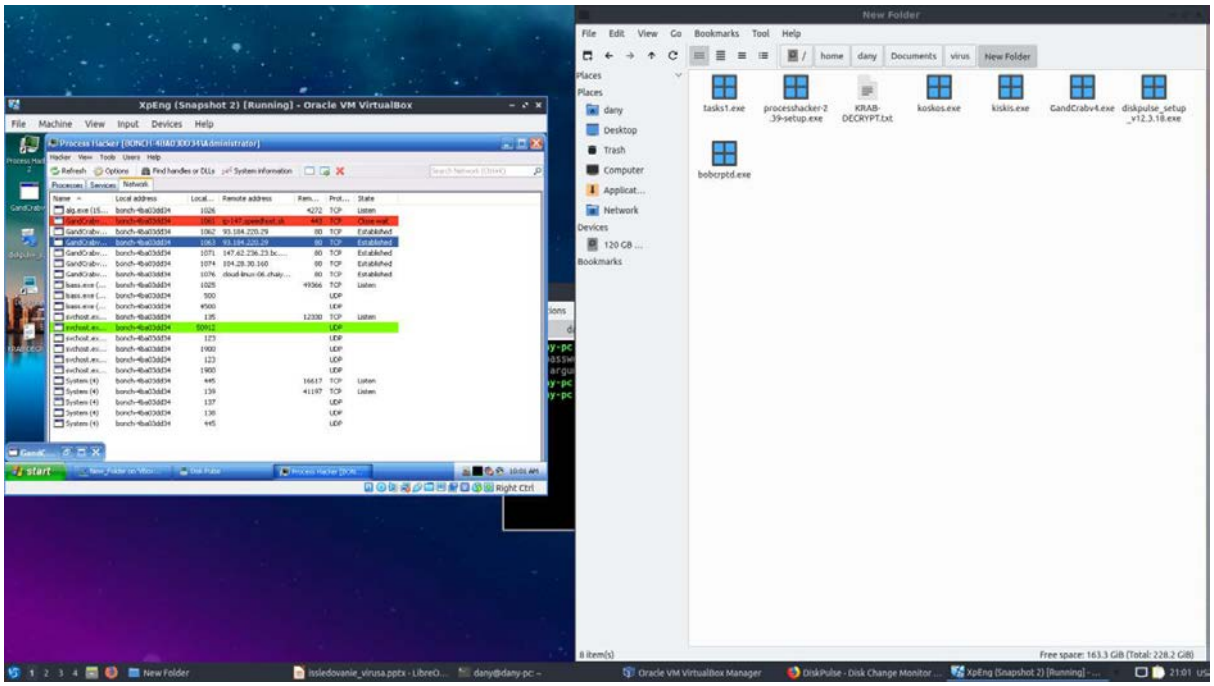


Рис. 6. GandCrab, создание соединений для передачи данных о пользователе

Включим сниффер, чтобы увидеть пакеты, отправляемые шифровальщиком. Откроем для примера пакет, содержащий информацию о пользователе.

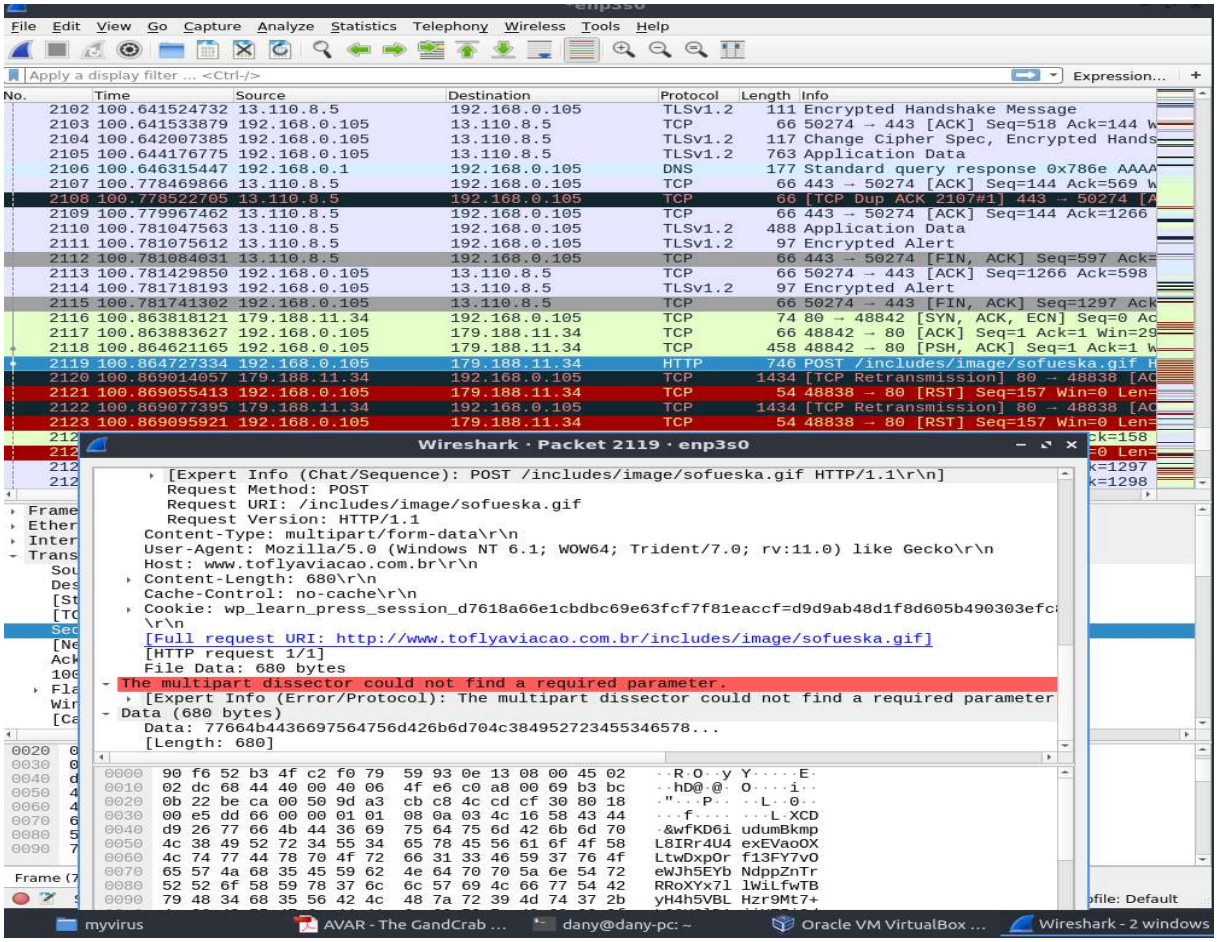


Рис. 7. Информация о пакете с данными пользователя

1) Шифрование файлов. Отсутствие доступа к файлам и появление на рабочем столе файла с инструкцией (записка о выкупе).

2) Удаление теневых копий, удаление точек восстановления. Пройденные нами этапы показывают нам примерную картину работы шифровальщика. Если вы увлекаетесь дизассемблированием, можете прочитать [2]. Это продвинутый уровень, однако статья носит обзорный характер, поэтому продолжим.

В качестве начального ПО для изучения данной сферы можем порекомендовать IDA PRO, так как она может определять название функции. Пример работы с IDA PRO над вирусом GandCrabv4:

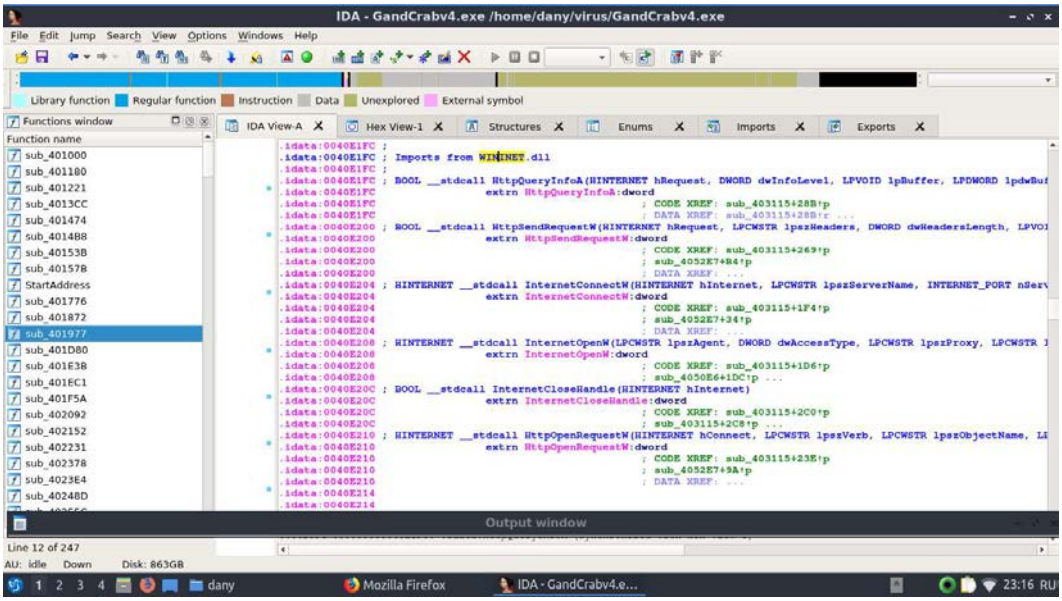


Рис. 8. Программа IDA PRO

Заключение

Основной целью данной статьи было познакомить с развитием вируса, принципами его работы, а также показать пример разбора данного шифровальщика в зависимости от уровня подготовки.

Список используемых источников

1. GandCrab 4.0 Technical Analysis and Cracking. URL: https://medium.com/@coding-karma/gandcrab-4-0-technical-analysis-and-cracking-422a3f4768dc

2. Unpacking GandCrab Ransomware. URL: https://secrary.com/ReversingMalware/Unpacking-GandCrab/

УДК 004.056.53
ГРНТИ 81.93.29

ГОЛОГРАФИЯ КАК СОВРЕМЕННЫЙ СПОСОБ ЗАЩИТЫ ИНФОРМАЦИИ

Д. С. Дмитриева, А. В. Красов, В. М. Пилипова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье рассматриваются признаки подлинности различных активов и аутентификация по ним. Подделка документов и ценных бумаг существует с древних времён

давно и постоянно совершенствуется. Именно поэтому очень важно установить подлинность всевозможных активов. В ходе работы было определенно, что наиболее устойчивой к подделке является голографическая защита.

подлинность документа, признак подлинности, голографическая защита, голограмма.

Подделка документов и ценных бумаг существует с древних времён и постоянно прогрессирует совместно с развитием технологий их создания. Поэтому в наш век подделок очень важно установить подлинность документа, ценной бумаги или другого актива.

Аутентификация документов – сложный и трудоемкий процесс, основанный на сравнении с функциями безопасности, которые действуют как стандарты. В этой процедуре различают оперативный и всесторонний контроль подлинностях [1]. Тщательный контроль подлинности проводят специфические специалисты с использованием особенностей распознавания подлинности. На практике широко используется оперативный контроль, который осуществляется путем изучения определенных средств защиты. В настоящее время подделка средств защиты осуществляется настолько качественно, что отличить подделку от оригинала зачастую невозможно. Для повышения точности определения подлинности документа используется большое количество многообразных признаков (от 10 до 30). Постоянная подделка применяемых средств защиты подлинности определяет задачу разработки новых, более продвинутых функций, и в результате со временем количество используемых функций в оперативном управлении постоянно увеличивается, а сам процесс идентификации достоверности усложняется. Это накладывает свой отпечаток на количественный и качественный набор опознавательных признаков, методы их идентификации, аппаратную конструкцию устройств контроля подлинности и их программное обеспечение [2, 3].

Набор признаков, по которым устанавливается подлинность проверяемого документа, формирует специальное информационное поле. В качестве признаков подлинности используются разные свойства полиграфической продукции, реализованные на специальных материалах с помощью голограмм, оптические эффекты, УФ- и ИК-люминесценция и т. д.

Если установлено N признаков подлинности, то итоговая вероятность того, что этот документ является подлинным, может быть определена в соответствии со следующим выражением:

$$W = \log_2 \prod_{i=1}^{N} 2^{Kipi},$$

где K – весовой коэффициент i-го признака;

p – вероятность присутствия или отсутствия i-го признака.

Вероятность того, что данный документ является подлинным, определяется условием нормализации:

$$A\sum_{i=1}^{n} K_i^p = 1,$$

где A – нормировочный коэффициент.

Очевидно, что для однородных признаков:

$$A = 1/N.$$

Существуют простые и сложные признаки определения подлинности. Простые образуются только с помощью какого-либо одного технологического процесса или путем выполнения определенного набора измерительных операций. Для простых признаков определения подлинности весовой коэффициент равен единице, а для сложных – весовой коэффициент может значительно отличаться от единицы.

Голографическая защита визуальной информации сегодня считается одной из самых устойчивых к подделкам. Плотность записи идентифицируемой информации в голографическом процессе намного выше, чем у всех других методов хранения данных, в связи с этим, точно подделать голографические изображения весьма сложно. Голографическая защита хороша тем, что носит комплексный характер. Одна голограмма может сочетать в себе различные степени защиты, каждая из которых рассчитана на свой уровень идентификации: от визуального восприятия на уровне потребителя продукта до экспертного использования специального оборудования с использованием методов амплитудно-фазового кодирования, скрытого и аналогового, а также компьютерного – синтезированных голограмм.

В настоящее время есть большое количество технологий создания защитных голограмм. В этой статье рассмотрим радужную голограмму.

Радужные голограммы имеют хорошее визуальное качество, а цвет определяется геометрией, а не химией. При освещении источником белого (широкого спектра) света пропускающая голограмма будет рассеивать все длины волн света в изображении. Однако, поскольку красные волны длиннее, они отклоняются больше, чем синие длины волн, и поэтому изображение будет иметь некоторое цветовое размытие – свет распространяется на изображение радуги. Радужная голограмма, записанная с горизонтальной эталонной полосы и воспроизводимая светом сверху, будет иметь горизонтальный параллакс, обеспечивающий пространственные качества при просмотре двумя глазами или движении из стороны в сторону. Но движение вверх и вниз не меняет пространственной перспективы, и зритель видит только изменение цвета (рис. 1).

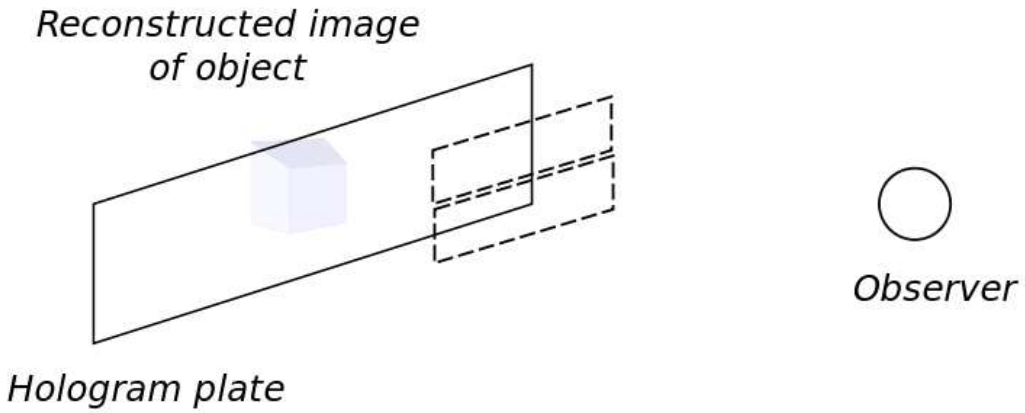


Рис. 1. Схема для просмотра радужной голограммы

Путем записи нескольких кодовых последовательностей под ахроматическим углом спектральные цвета могут быть рекомбинированы для создания изображений, которые являются беловатыми (ахроматическими) или смешанными по цвету (т. е. красный + зеленый + синий RGB). Такие голограммы используются для подтверждения подлинности документов, маркировки товаров, а также для банковских карт (рис. 1).

В настоящее время для защиты информации также используются водяные знаки. Водяные знаки – это изображения, полученные в результате процесса отлива бумаги, которые используются для защиты документов и денежных купюр (рис. 2).

Рис. 2. Пример водяного знака на денежных купюрах

В данной статье проведем сравнение голографической защиты и водяного знака (табл.).

ТАБЛИЦА. Сравнение защитных элементов

	Голографическая защита	Водяные знаки
Технология производства	Выполняются по различным технологиям, объединяет их большой объем передаваемой информации и сложность изготовления	Вдавливание в процессе изготовления металлического валика (ровнителя, эгутера, дендироли). Более сложный метод-тиснение
Затраты на производство	Большие	Большие
Просмотр	Изменение угла наклона изображения по отношению к источнику света меняет цвет	Видимые на просвет
Риск повреждения	Высокий риск повреждения голографических изображений, нанесенных на наружные поверхности	Низкий риск
Сроки изготовления	Быстрые	Быстрые
Характеристика фальсификации	Припрессовка фольги, использование металлизированной краски. Сложность подделки	Надрисовка, давление, пропитка маслоподобными веществами, гравировка

В статье была рассмотрена аутентификация документов как один из самых надежных способов защиты ценных бумаг от подделки. Было установлено, что голография, как один из самых надежных методов, существенно повышает уровень защищенности документов от подделывания за счет очень высокой плотности записи идентифицирующей информации.

Список используемых источников

1. Коншин А. А. Защита полиграфической продукции от фальсификации. М.: ООО «Синус», 2000. 160 с.

2. Садердинов А. А., Трайнев В. А., Федулов А. А. Информационная безопасность предприятия: учебное пособие. 2-е изд. М.: Издательско-торговая корпорация Дашков и К°, 2005. 336 с.

3. Малюк А. А. Информационная безопасность: концептуальные и методологические основы защиты информации: учебное пособие. М.: Изд-во Горячая линия – Телеком, 2004. 202 с.

4. Степанов Е. А., Корнеев И. К. Информационная безопасность и защита информации: Учебное пособие. М.: Изд-во ИНФРА-М, 2001. С. 23–24.

5. Гориленко А. Я. Современные методы защиты банкнот и ценных бумаг от подделки, Сер. IX, Изд-во. дело и полиграфия, 2002. Вып. X. С. 61–69.

УДК 004.7
ГРНТИ 49.33.29

ИССЛЕДОВАТЕЛЬСКИЕ АСПЕКТЫ В ПРОГРАММНО-КОНФИГУРИРУЕМЫХ СЕТЯХ

Ю. С. Дмитриева, В. С. Елагин

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье произведён анализ подходов к управлению сетевыми ресурсами в сети SDN. Для этого выполнен обзор научных работ российских и зарубежных авторов для выявления применяемых в них решений, а также их достоинств и недостатков. Методы, рассмотренные в научных статьях, систематизированы по следующим критериям: уровень применимости метода (физический, логический, сетевой), математическое моделирование, время реагирования, решаемый круг задач, доведение решения для практической реализации. В результате анализа обзора сделан вывод о неудовлетворительности решений, а также о необходимости создания нового метода со следующими характеристиками: широкая область применения, работающего на всех уровнях SDN.

SDN, программно-конфигурируемая сеть, OpenFlow, балансировка, сравнительный анализ.

Введение

Происходит развитие информационных технологий [1], постоянно растет потребность передачи разнородной информации; как следствие, растет и нагрузка на сеть [2]. Традиционная маршрутизация не справляется с ростом потребления трафика со стороны пользователей. Поэтому, была разработана технология передачи данных – программно-конфигурируемая сеть (*Software-Defined Network*, SDN), которая открыла к проектированию и администрированию сетевых ресурсов. Несмотря на полученные успехи оптимальность ее балансировки оказывается недостаточной. Таким образом совершенствование SDN-решений остается актуальной задачей. Для дальнейшего совершенствования необходимо выявить недостатки существующих решений, негативно влияющие на итоговую балансировку сетевых потоков. В интересах этого произведем обзор статей, посвященных различным способам управления потоками в сетях SDN, с систематизацией их характеристики. В случае невозможности модернизации существующих решений потребуется создание собственного, не только лишенного недостатков предыдущих, но и обладающего их преимуществами.

Обзор работ

Опишем кратко ход проведенного исследования. Была использована база научной электронной библиотеки eLIBRARY и реферативная база Scopus. Поиск наиболее характерных публикаций [3–26] производился по ключевой фразе «балансировка нагрузки в сети SDN».

Для сравнения были выбраны следующие критерии:

– первый критерий – работа на различных уровнях сети SDN (физический, логический, сетевой);

– второй критерий – математическое моделирование;

– третий критерий – время реагирования;

– четвертый критерий – решаемый круг задач;

– пятый критерий – доведение решения до практической реализации.

Для второго критерия введены следующие обозначения моделей: СМО* – авторская модель на базе СМО (Системы массового обслуживания), MQ (*Multilevel Queue*) – модель многоуровневой очереди, CPN (*Coloured Petri*) – модель графа раскрашенной сети Петри, K-CP – модель K-Center Problem, ТИ – модели из Теории игр, GCALB (*Generic Controller Adaptive Load Balancing*) – модель адаптивной балансировки нагрузки универсального контроллера, LBCP (*Load Balanced Controller Placement*) – модель размещения контроллера с балансировкой нагрузки, ГМ* – авторская модель на основе теории графов.

С точки зрения уровня применения метода было найдено 10 работ в которых балансировка нагрузки проходила на сетевом уровне, в 8-ми работах на физическом уровне и только в 3-х работах на сетевом уровне (рис. 1).

Авторы в своих работах применяют механизм многоуровневой справедливой очереди, авторские способы моделирования или авторские способы моделирования на основе СМО. Зарубежные авторы рассматривают метаматематическую модель на основе графа раскрашенной сети Петри и авторскую модель на основе теории графов. В статье [18] «Dynamic SDN Controller Load Balancing» применяются две математические модели: K-Center Problem (решает проблему кластеризации) и модель из Теория игр (минимизация нагрузки между кластерами). Подробно рассмотрены модели адаптивной балансировки нагрузки универсального контроллера и модель размещения контроллера с балансировкой нагрузки. Каждая модель представлена в единичном варианте. В 19 % рассмотренных научных статей применяется СМО.

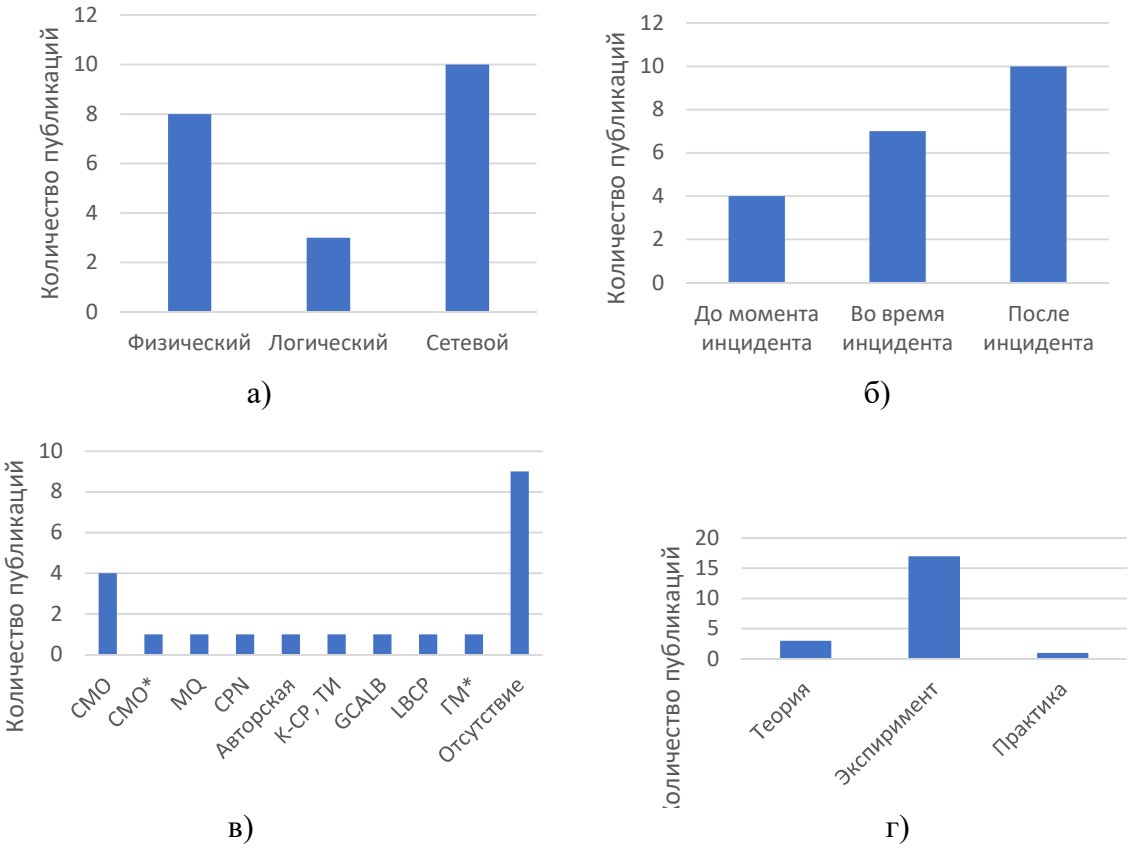


Рис. 1. Количество публикаций по критериям:
а) применимость методов в соответствии с уровнями SDN;
б) режим балансировки в виде времени реагирования;
в) наличие математической модели при балансировке нагрузки или указание ее отсутствия; г) степень исследования метода к управлению сетевыми ресурсами

С точки зрения реагирования, больше всего методов применимо после возникновения инцидента (10 работ), а только в 4 работах метод балансировки нагрузки начинает работать превентивно.

Большинство методов применимо для большого круга задач. Они рассмотрены в 75 % работ.

С точки зрения реализации, в преобладающем большинстве работ приведены реальные эксперименты, реализованные в сети mininet, несмотря на это до реальной практической реализации доведен только в единственной работе [13] «Балансировка нагрузки в защищенных сетях с использованием технологии SDN». Алгоритм балансировки нагрузки реализован на языке программирования Java в виде модуля для контроллера SDN с открытым исходным кодом с названием Beacon.

Исходя из сделанных выводов можно предположить не только недостаточность существующих решений, но и практическую невозможность их требуемой модернизации. Таким образом, предлагается создание нового (авторского) метода балансировки, основанного на следующих положениях:

реализация на логическом, физическом и сетевом уровнях SDN, балансировка до момента наступления инцидента, применимость для широкого круга задач.

Выводы

В статье проведен обзор научных статей на предмет различных методов по балансировке сетей SDN. В исследовании произведено сравнение предлагаемых решений по 5 критериям: уровень применимости, математическая модель, проактивность, круг применения и степень исследования. Исходя из сравнительного анализа работ, а также учитывая достоинства и нивелирующего недостатки существующих методов, были предложены основные положения нового (авторского) метода балансировки.

Метод должен работать на физическом, логическом и сетевом уровнях сети SDN, реагировать до момента наступления инцидента, а также применяться для широкого круга задач. Также, на логическом уровне в интересах кластеризации контроллеров возможно применение машинного обучения [27], что соответствует современным тенденциям по интеллектуализации процессов.

Таким образом, продолжением исследования должна стать разработка полноценного метода балансировки сетей SDN, доведение его до практической реализации и проведение необходимых экспериментов.

Список используемых источников

1. Волщуков Ю. Н., Волщуков М. Ю., Израилов К. Е., Романенко А. В. Визуализация информационного обмена в условиях концепции Industry 4.0 // Автоматизация в промышленности. 2020. № 8. С. 23–29.

2. Buinevich M., Izrailov K., Stolyarova E., Vladyko A. Combine method of forecasting VANET cybersecurity for application of high priority way // The proceedings of 20th International Conference on Advanced Communication Technology (Chuncheon, South Korea, 2018). IEEE, 2018. pp. 266–271.

3. Баскаков А. Е., Волков А. С. Алгоритм управления ресурсами транспортной программно-конфигурируемой сети связи // Труды МАИ. 2020. № 115. С. 6.

4. Волков А. С., Баскаков А. Е., Бахтин А. А., Горелик А. В. Метод управления ресурсами транспортной ПКС // Системы синхронизации, формирования и обработки сигналов. 2021. Т. 12. № 2. С. 4–10.

5. Рытов М. Ю., Калашников Р. Ю., Горелов А. А. Применение механизма многоуровневой справедливой очереди для снижения ущерба от атак отказа в обслуживании в программно-конфигурируемых сетях // Информация и безопасность. 2021. Т. 24. № 2. С. 253–260.

6. Данешманд Б. М. Анализ и оценка эффективности методов обеспечения качества обслуживания программно-конфигурируемых сетей стандарта 5G/IMT-2020 // Российский технологический журнал. 2021. Т. 9. № 5 (42). С. 14–25.

7. Агеева А. Д., Бирюкова Н. В., Мошков В. В., Елагин В. С. Транспортные программно-конфигурируемые сети // Modern Science. 2019. № 12-4. С. 291–301.

8. Маньков В. А., Краснова И. А. Алгоритм динамической классификации потоков в мультисервисной SDN-сети // T-Comm: Телекоммуникации и транспорт. 2017. Том 11. №12. С. 37–42.

9. Ибрагимов Б., Керимов В. Об одном подходе к оценке ресурсов в мультисервисных сетях связи на базе единого инфокоммуникационного пространства // IT-Технологии: развитие и приложения: XV Ежегодная Международная научно-техническая конференция: сб. докладов, Владикавказ, 12–14 декабря 2018 года. Владикавказ: Северо-Кавказский горно-металлургический институт (Государственный технологический университет), 2018. С. 283–293.

10. Елагин В. С. Динамическое управление нагрузкой в программно-конфигурируемых сетях // Труды учебных заведений связи. 2017. Т. 3. № 3. С. 60–67.

11. Амелянович А. В., Шпаков М. Н., Мутханна А. С., Буйневич М. В., Владыко А. Г. Централизованное управления потоками трафика в беспроводных локальных сетях на базе концепции SDN // Системы синхронизации, формирования и обработки сигналов. 2017. Т. 8. № 2. С. 31–35.

12. https://github.com/ramonfontes/vnd

13. Гузев О. Ю., Чижов И. В. Балансировка нагрузки в защищенных сетях с использованием технологии SDN // Системы и средства информатики. 2018. Т. 28, вып. 1. С. 123–138. DOI: https://doi.org/10.14357/08696527180110

14. Гузев О. Ю., Чижов И. В. SDN-балансировка нагрузки на криптографические маршрутизаторы при объединении центров обработки данных // Системы и средства информатики. 2018. Т. 28, вып. 1. С. 139–155. DOI: 10.14357/08696527180111

15. Братченко Н. Ю., Мочалов В. П., Яковлев С. В. Разработка имитационной модели системы управления качеством инфокоммуникационных услуг сетей SDN // Современная наука и инновации. 2019. № 3 (27). С. 44–53.

16. Пашков В. Н Распределенная отказоустойчивая платформа управления для программно-конфигурируемых сетей // Моделирование и анализ информационных систем. 2019. Т. 26. С. 101–121. DOI: 10.18255/1818-1015-2019-1-101-121

17. Sufiev, H.; Haddad, Y. A dynamic load balancing architecture for SDN. In Proceedings of the IEEE International Conference on the Science of Electrical Engineering (ICSEE), Eilat, Israel, 16–18 November 2016; pp. 1–3.

18. Hadar Sufiev, Yoram Haddad, Leonid Barenboim, José Soler: Dynamic SDN Controller Load Balancing. Future Internet 11(3): 75 (2019)

19. Controller Adaptive Load Balancing for SDN Networks. Wael Hosny Fouad Aly. College of Engineering and Technology.American University of the Middle East (AUM) Egaila, Kuwait. Arab Academy for Science and Technology (on leave). lexandria, Egypt (2019). http://dx.doi.org/10.1109/ICUFN.2019.8805922

20. Wael Hosny Fouad Aly, "Generic Controller Adaptive Load Balancing (GCALB) for SDN Networks", Journal of Computer Networks and Communications, vol. 2019, Article ID 6808693, 9 pages, 2019. https://doi.org/10.1155/2019/6808693. URL: https://www.hindawi.com/journals/jcnc/2019/6808693/

21. Yeganeh S. H., Tootoonchian A., and Ganjali Y. On scalability of software-defined networking // IEEE Communications Magazine, vol. 51, no. 2, pp. 136–141, February 2013.

22. Aly W. H. F. and Al-Anazi A. M. A., Enhanced CONTROLLER Fault Tolerant (ECFT) model for software defined networking // in Proceedings of the 5th IEEE International Conference on Software Defined Systems (SDS), Barcelona, Spain, April 2018.

23. Bharanidharan, C., Indira Gandhi, S. & Devapriya, R.D. An Enhanced Framework for Traffic Load Balancing and QoS Provisioning in SDN // Wireless Pers Commun 121, 3451–3472 (2021). DOI: 10.1007/s11277-021-08886-2.

24. Bala Rao. Poly-stable matching based scalable controller placement with balancing constraints in SDN // Computer Communications 154 (7). February 2020. DOI:10.1016/j.comcom.2020.02.053

25. Shi, Xiaojun, Yangyang Li, Haiyong Xie, Tengfei Yang, Linchao Zhang, Panyu Liu, Heng Zhang and Zhiyao Liang. “An OpenFlow-Based Load Balancing Strategy in SDN” Cmc-computers Materials & Continua 62 (2020): 385-398.

26. Vijaya S. Eligar, Nalini Iyer, Nihal N.D, Nikhil S.Hugar YashwantKumar P, Manjunath M.N. Load balancing using OpenDaylight SDN controller: Case study // International Research Journal on Advanced Science Hub, 2020, Volume 2, Issue 9, Pages 59-64. DOI:10.47392/irjash.2020.149.

27. Буйневич М. В., Ганов Г. А., Израилов К. Е. Интеллектуальный метод визуализации взаимодействий программ в интересах аудита информационной безопасности операционной системы // Информатизация и связь. 2020. № 4. С. 67–74.

УДК 004.056.53
ГРНТИ 49.33.29

РАЗРАБОТКА СИСТЕМЫ ПРОФИЛИРОВАНИЯ ПОЛЬЗОВАТЕЛЕЙ ДЛЯ VPN ПОДКЛЮЧЕНИЙ

А. Д. Докшин, А. В. Докшина, М. М. Ковцур, Э. Г. Костандян

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Сегодня большинство компаний внедряют технологии, благодаря которым работникам для выполнения своих обязанностей нет необходимости находиться на своем рабочем месте. Одной из таких технологий является VPN в корпоративной сети. Злоумышленникам также нет необходимости находиться внутри компании для взлома ее сети. Им достаточно получить данные любого сотрудника для успешной авторизации в корпоративной сети. Решение этой проблемы основано на использовании компанией системы профилирования каждого пользователя при подключении к корпоративной сети. Профилирование подразумевает определение пользовательского устройства, например, на основе MAC-адреса, версии операционной системы, браузера и местоположения пользователя в момент подключения к VPN серверу. В докладе подробно описан механизм применения процесса профилирования на базе шлюза безопасности pfSense.

VPN, удаленный доступ, безопасность беспроводных сетей, профилирование, шлюз безопасности, pfSense.

Пандемия, возникшая из-за короновирусной инфекции в 2020 году, оказала огромное влияние на многие аспекты жизни человека [1]. Студентам и офисным работникам в срочном порядке необходимо было разработать решение, благодаря которому они смогут учиться и работать, не выходя из своего дома. Наиболее подготовленным к новым реалиям оказались сотрудники IT-компании, так как они в срочном порядке смогли установить и

настроить в своей инфраструктуре VPN сервера [2]. Однако, использование VPN серверов, дало новую возможность злоумышленникам получить конфиденциальную информацию компании, осуществляя подключение к VPN серверу под видом легальных пользователей, используя учетные данные сотрудников, хранящихся на сервере [3].

С целью предотвращения вторжения злоумышленников в корпоративную сеть компании, в данной статье представлен механизм профилирования пользователей, осуществляющих подключение к VPN серверу [4]. Для реализации профилирования пользователей в лаборатории была создана модель, включающая в себя две независимые сети, объединенные между собой при помощи маршрутизатора. Данная схема представлена на рис. 1. Компьютер из сети «192.168.1.0» осуществляет подключение к сети «192.168.2.0» при помощи шлюза безопасности pfSENSE, который в свою очередь выполняет роль VPN сервера.

Рис. 1. Схема подключения

Основной целью профилирования в предлагаемом решении является предотвращение подключения пользователя с оборудования, отличающегося от того, что было использовано при первом сеансе связи [5]. При этом отслеживаются изменения версии и типа операционной системы, версии браузера, применяемого при Web-авторизации, а также региона, из которого осуществляется подключение. При первом подключении данные собираются и вносятся в специальную базу данных для дальнейшего сравнения с информацией, которая будет получена в результате профилирования. В случае изменения этих данных системный администратор может вычислить пользователя и отключить его от VPN сервера.

Для осуществления профилирования и сбора всей информации необходимо сформулировать основные шаги во время авторизации на VPN сервере [6]. На рис. 2 представлена подробная структурная схема авторизации.

После подключения к серверу пользователь видит на экране окно авторизации Captive Portal, в котором необходимо ввести уникальный логин и пароль. После подтверждения введенных данных пользователь может подключится к внутренним ресурсам сети. В свою очередь, одновременно с авторизацией в pfSense, заполняется информация о данном пользователе: IP-адрес, MAC-адрес, версия операционной системы, версия браузера и местоположение.

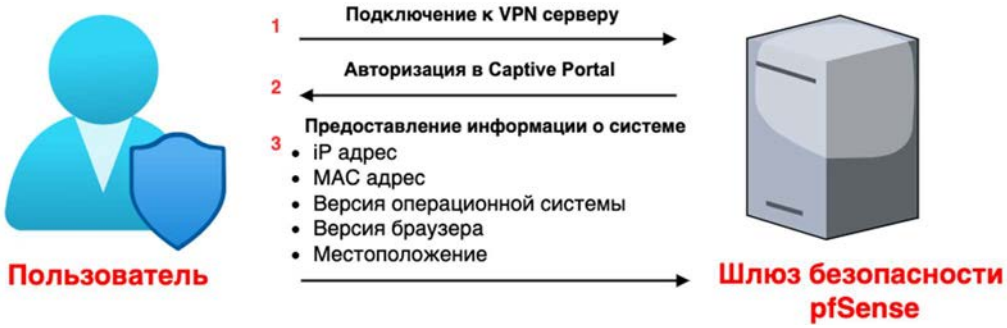


Рис. 2. Схема авторизации

Данная информация собирается для осуществления профилирования при повторных попытках авторизации пользователя в системе. Если пользователь осуществляет авторизацию, не меняя своего устройства, применявшегося при первом подключении, то авторизация пройдет успешно. Если же пользовательская информация, полученная при повторных попытках авторизации не совпадает хотя бы по одному из критериев, полученных в ходе первой авторизации, то этот пользователь не сможет авторизоваться до того момента, пока администратор не снимет с пользователя ограничение. Данный механизм может использоваться для выявления учетных данных, которые могли попасть в руки злоумышленникам. Структурная схема решения представлена на рис. 3.

Рис. 3. Схема авторизации

В WEB интерфейсе, представленном на рис.4, можно увидеть всю предоставленную пользователем информацию в процессе профилирования. После этого данная информация сравнивается с той, которая поступает при повторных авторизациях данного пользователя в системе.

Рис. 4. Web интерфейс pfSense

В качестве определения производительности предложенного решения и влияния профилирования на конечного пользователя проведен эксперимент и представлена математическая модель (1), в рамках которой рассчитывается время, которое необходимо потратить на все этапы авторизации с условием прохождения профилирования [7]:

$$T = t_1 + t_2 + t_3 + t_4, \quad (1)$$

где T – время авторизации пользователя (с), t_1(с) время подключения пользователя к серверу, t_2(с) время загрузки Captive portal, t_3(с) время проверки введенных пользователем данных для авторизации, t_4(с) время, за которое пользователь успешно подключится к внутреннему ресурсу сети [8].

При расчете производительности изменяется объем оперативной памяти шлюза безопасности pfSense. Результат расчета данной модели представлен в табл. 1.

ТАБЛИЦА 1. Время авторизации

RAM, Gb	t_1, с	t_2, с	t_3, с	t_4, с	T, с
2	6	3	5	1	15
4	6	3	5	1	15
6	6	3	5	1	15
8	3.5	3	2	1	9.5
16	3.5	2	2	1	8.5
32	2.5	2	2	1	7.5

Анализируя полученные данные из табл. 1, можно сделать вывод, что увеличение объема оперативной памяти VPN сервера, дает возможность значительно сократить время подключения к серверу, ускорить работу портала Web-авторизации, а также уменьшить время обработки данных.

Одним из важных критериев стабильной работы сервера является нагрузка при параллельной авторизации пользователей [9]. Для тестирования одновременно с разных компьютеров была произведена авторизация пользователей под своими уникальными учетными данными. Результат тестирования представлен в табл. 2.

ТАБЛИЦА 2. Нагрузка сервера

Количество авторизаций	CPU pfSENSE	Среднее время авторизации пользователя
0	2 %	9.5
4	5 %	9.5
6	5 %	10
10	10 %	10
15	15 %	10
18	15 %	15
25	15 %	15

Таким образом, можно сделать вывод о том, что VPN сервер с реализованным дополнительным профилированием каждого пользователя полностью справляется с нагрузкой при авторизации как одного пользователя, так и групп пользователей, осуществляющих параллельное подключение к VPN серверу [10].

В заключении, можно сделать вывод о том, что поставленная цель полностью достигнута и данное решение может быть внедрено в тестовом режиме в корпоративную сеть для уменьшения вероятности проникновения в сеть злоумышленника под видом легального пользователя.

Список используемых источников

1. Даньшина А. В., Докшин А. Д., Ковцур М. М. Разработка сервера аутентификации на базе операционной системы ASTRA LINUX // В сб.: Региональная информатика и информационная безопасность. Сборник трудов конференций: Санкт-Петербургской международной конференции и Санкт-Петербургской межрегиональной конференции. Санкт-Петербург, 2020. С. 262–265.

2. Ковцур М. М., Киструга А. Ю., Ворошнин Г. Е., Фёдорова А. Э. Исследование атак authentication failure и arp inject и методов их обнаружения в сетях семейства IEEE 802.11 // Информационные технологии и телекоммуникации. 2021. Т. 9. № 1. С. 87–98.

3. Ковцур М. М., Даньшина А. В., Докшин А. Д., Потемкин П. А. Исследование особенностей организации VPN для предоставления удаленного доступа // Заметки ученого. 2021. № 4-1. С. 76–80.

4. Красов А. В., Левин М. В., Цветков А. Ю. Метод управления трафиком в гибридной программно-определяемой сети // Информационные технологии и телекоммуникации. 2016. Т. 4. № 2. С. 53–63.

5. Сахаров Д. В., Красов А. В., Ушаков И. А., Бирих Э. В. моделирование защищенной масштабируемой сети предприятия с динамической маршрутизацией на основе IPv6 // Защита информации. Инсайд. 2020. № 1 (91). С. 51–57.

6. Штеренберг С. И., Москальчук А. И., Красов А. В. Разработка сценариев безопасности для создания уязвимых виртуальных машин и изучения методов тестирования на проникновения // Информационные технологии и телекоммуникации. 2021. Т. 9. № 1. С. 47–58.

7. Валиева К. А., Виткова Л. А., Чечулин А. А. Предварительная обработка информационных объектов в системах мониторинга сети интернет // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VIII Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2019. С. 197–201.

8. Абраменко Г. Т., Миняев А. А., Храмцов Д. О. Исследование атак и методов защиты беспроводных сетей при аутентификации по протоколу 802.1x // Актуальные проблемы инфотелекоммуникаций в науке и образовании X Юбилейная Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2021. С. 25–29.

9. Сахаров Д. В., Красов А. В., Ушаков И. А., Орлов Г. А. Защищенная модель программно-определяемой сети в среде виртуализации KVM // Электросвязь. 2020. № 3. С. 26–32.

10. Альшаев И. А., Красов А. В., Ушаков И. А. Исследование принципов работы протокола Openflow в программно-конфигурируемых сетях // Труды учебных заведений связи. 2017. Т. 3. № 2. С. 16–27.

УДК 004.71
ГРНТИ 49.33.29

МЕТОДИКА НАСТРОЙКИ ОБОРУДОВАНИЯ В ПРОГРАММНО-КОНФИГУРИРУЕМОМ СЕГМЕНТЕ СЕТИ

Е. П. Долгов, А. С. Осетрин

Академия Федеральной службы охраны Российской Федерации

Задача по обучению администраторов программно-конфигурируемых сетей является актуальным направлением исследований. В работе рассмотрены особенности архитектуры и настройки оборудования программно-конфигурируемых сетей. В ходе конфигурирования экспериментального стенда была разработана методика по его настройке. Полученные результаты описывают компоненты, необходимые для создания сети любой сложности.

программно-конфигурируемые сети, mininet, ryu, OpenvSwitch.

В целях повышения качества и надежности сетей органов государственной охраны рассматривается вариант внедрения в транспортную сеть с коммутацией пакетов технологии программно-конфигурируемых сетей.

Эта технология является относительно новой и на данных момент не получила достаточно широкого внедрения в существующие сети. В связи с этим возникла необходимость подготовки инженерного состава для работы с новой технологией, чтобы уменьшить время, требуемое для развертки инфраструктуры и минимизировать вероятность появления критических ошибок конфигурации сети.

Для настройки сетевого оборудования программно-конфигурируемых сетей необходимо понимать его архитектуру. Внутреннее устройство OpenFlow-коммутатора представлено на рис. 1 [1].

OpenFlow коммутатор состоит из одной или нескольких таблиц потоков и групповой таблицы, которые выполняют поиск и пересылку пакетов. Он также включает канал OpenFlow для внешнего контроллера. Коммутатор обменивается данными с контроллером, а контроллер управляет коммутатором по протоколу OpenFlow. Контроллер использует протокол OpenFlow для добавления, обновления и удаления записей потоков в таблицах потоков. Он может делать это проактивно или реактивно в ответ на пакеты, поступающие на коммутатор.

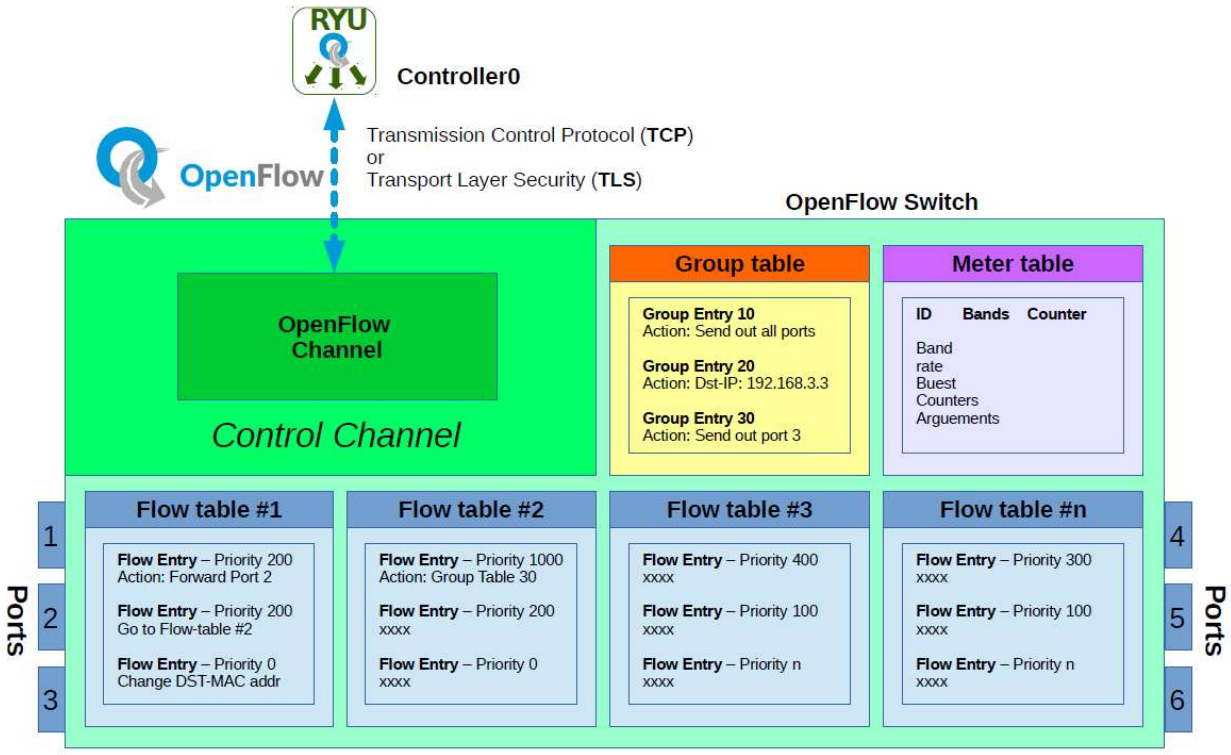


Рис. 1. Внутреннее устройство OpenFlow коммутатора

Каждая таблица потоков в коммутаторе содержит набор записей потока, и каждая запись потока, как показано на рис. 2, состоит из:

– Cookie: Это непрозрачное значение данных, выбранное контроллером. Это поле может использоваться им для фильтрации потока (0x0).

– Timeouts: максимальное временя простоя потока в коммутаторе.

– Hard timeout: Ненулевое значение, которое приводит к удалению записи потока через заданное количество секунд, независимо от того, сколько пакетов было сопоставлено. (hard_timeout=50)

– Idle timeout: Поле с ненулевым значением, которое приводит к удалению записи потока, если она не соответствует ни одному пакету в течение заданного количества секунд. (idle_timeout=20)

– Priority: Приоритет записи потока. (priority=1)

– Match fields: Для сопоставления пакетов. Они состоят из входного порта, полей заголовка кадра и пакета и, возможно, метаданных, указанных в предыдущей таблице. (in_port=1, dl_src=00:00:00:00:00:01, dl_dst=00:00:00:00:00:02)

– Instructions: Чтобы изменить набор действий или конвейерную обработку. Обычно выходной порт связан с потоком. (actions=output:2)

– Counters: Счетчики для сбора статистики. (duration=764.169s, n_packets=242538, n_bytes=13851836796)

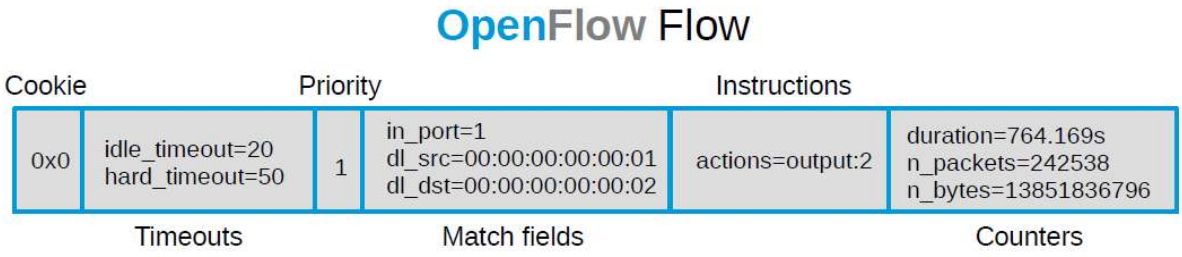


Рис. 2. Поля записи потока

Действие в примере указывает, что совпадающие пакеты должны пересылаться через порт 2 коммутатора. Действия, связанные с записями потока, также могут направлять пакеты в групповую таблицу. Групповые таблицы определяют дополнительные этапы обработки. Группы представляют собой наборы действий для лавинной рассылки, а также для более сложной переадресации, такой как наличие нескольких маршрутов в одну точку, быстрая пересылка и агрегация каналов. Групповые таблицы также можно использовать для отправки нескольких записей потоков с одним идентификатором, это обычно применяется для таких приложений, как IP-переадресация.

Групповые записи в групповой таблице имеют список действий, сгруппированных в сегменты. Действия в одном или нескольких сегментах применяются к пакетам, отправляемым в группу.

Записи таблицы счетчиков определяют счетчики для каждого потока. Эти счетчики позволяют OpenFlow реализовывать операции качества обслуживания (QoS), такие как ограничение скорости, и могут сочетаться с очередями для каждого порта для реализации сложных структур QoS, таких как DiffServ.

Mininet – это эмулятор сети, который создает сеть виртуальных хостов, коммутаторов, контроллеров и связей между ними [2]. Хосты Mininet работают под управлением стандартного сетевого программного обеспечения Linux, а его коммутаторы поддерживают OpenFlow для очень гибкой пользовательской маршрутизации и программно-определяемой сети.

Open virtual Switch (OvS) предлагает решение для программных коммутаторов, которое работает через OpenFlow и может использоваться в виртуализированных ситуациях, когда физический коммутатор не нужен. Архитектура OvS представлена на рис. 3 [3].

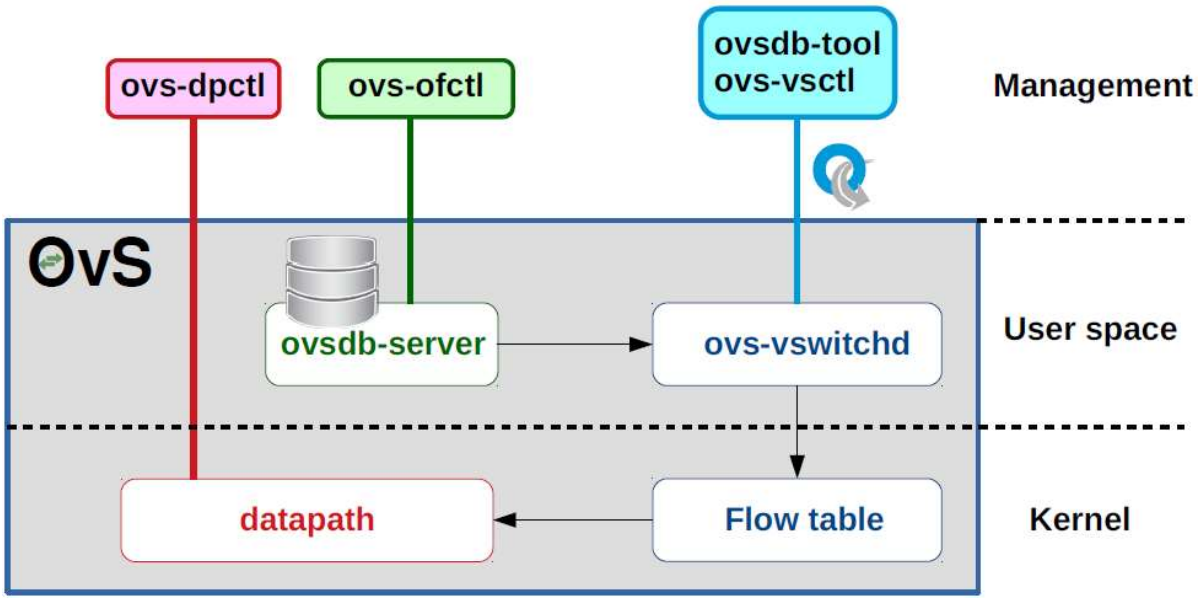


Рис. 3. Архитектура OvS

- **ovsdb-server:** Эта программа предоставляет интерфейсы удаленного вызова процедур (Remote Procedure Call – RPC) для одной или нескольких баз данных OpenvSwitch (OVSDB).
  - Она поддерживает клиентские соединения JavaScript Object Notation (JSON) RPC (JSON-RPC) через активные или пассивные сокеты домена TCP/IP или Unix. Она поддерживает базу данных таблицы коммутаторов и список внешних клиентов, которые могут общаться с «ovsdb-server».
  - Каждый файл OVSDB может быть указан в командной строке как база данных. Если ничего не указано, по умолчанию используется «/usr/local/etc/openvswitch/conf.db». Файлы базы данных уже должны быть созданы и инициализированы, например, с помощью «ovsdb-tool create».
  - Клиенты ovsdb могут использовать протокол управления ovsdb для управления таблицами OVSDB.

- **ovs-vswitchd:** Это основная программа пользовательского пространства OvS – демон, который управляет и контролирует любое количество коммутаторов OvS на локальном компьютере.
  - Он считывает желаемую конфигурацию OvS из программы ovsdb-server по каналу межпроцессного взаимодействия (Inter Process Communication – IPC).
  - Он также передает определенную статусную и статистическую информацию обратно в базу данных.
- **ovs-vsctl:** Это утилита для запроса и обновления конфигурации ovs-vswitchd (с помощью ovsdb-server). Конфигурация порта, добавление/удаление моста, связывание и тегирование VLAN — это лишь некоторые из параметров, доступных с помощью этой команды.
  - **ovs-vsctl** –: выводит текущую версию openvswitch.
  - **ovs-vsctl show:** выводит краткий обзор конфигурации базы данных коммутатора.
  - **ovs-vsctl list-br:** выводит список настроенных мостов.
  - **ovs-vsctl list-ports <bridge>:** выводит список портов на указанном мосту.
  - **ovs-vsctl list interface:** выводит список интерфейсов.
  - **ovs-vsctl add-br <bridge>:** создает мост в базе данных коммутатора.
- **ovs-ofctl:** Это инструмент командной строки для мониторинга и администрирования коммутаторов OpenFlow. Он используется для перечисления реализованных потоков в модуле ядра OVS.
  - ovs-ofctl add-flow <bridge> <flow>
  - ovs-ofctl add-flow <bridge> <match-field> actions=all
  - ovs-ofctl del-flows <bridge> <flow>
- **ovs-dpctl:** Это инструмент командной строки для создания, изменения и удаления путей данных OvS. Эта программа работает только с путями данных, которые реализованы вне самого ‘ovs-vswitchd’, такими как пути данных на основе ядра операционной системы.
- **ovsdb-tool:** Это консольная программа для управления файлами OVSDB. Она не взаимодействует напрямую с работающими серверами баз данных OvS.
  - ovsdb-client list-dbs
  - ovsdb-client list-tables
  - ovsdb-client get-schema
  - ovsdb-client list-columns
  - ovsdb-client dump

Таким образом, вышеописанные компоненты программно-конфигурируемой сети в совокупности позволяют построить любую топологию.

А также описанная методика позволит получить сетевым инженерам необходимые знания и умения, описанные в приказе министерства труда и социальной защиты Российской Федерации № 786н [4].

Список используемых источников

1. Ryu // Ryubook [сайт]. URL: https://osrg.github.io/ryu-book/en/Ryubook.pdf (дата обращения: 20.12.2021).
2. Mininet // mininet [сайт]. URL: http://mininet.org/ (дата обращения: 20.12.2021).
3. Open virtual switch // OpenvSwitch [сайт] URL: https://www.openvswitch.org/ (дата обращения: 10.08.2022).
4. Приказ Минтруд России №786н от 16.10.2020 «Об утверждении профессионального стандарта «Специалист по поддержке программно-конфигурируемых информационно-коммуникационных сетей» (Зарегистрировано в Минюсте России 21.12.2020 № 61658).

УДК 004.75
ГРНТИ 81.93.29

АНАЛИЗ ЗАЩИЩЕННОСТИ ОБЪЕКТОВ SD-IOV-BLOCKCHAIN

Е. А. Донсков, И. В. Котенко

Санкт-Петербургский Федеральный исследовательский центр Российской академии наук

Концепция SD-IoV (SDN интернета транспортных средств) является одним из передовых направлений, которое активно развивается и позволяет по-новому взглянуть на возможность применения интернета вещей в целом. Однако, наиболее актуальной проблемой является низкая безопасность систем интернета вещей. Для решения обозначенной проблемы исследователи предлагают интеграцию технологий SD-IoV и распределенного реестра. Целью данной работы является анализ защищенности объектов SD-IoV-Blockchain с точки зрения уровня защищенности системы в целом, а также защищенности части сети, в которой используется блокчейн. В работе рассматриваются уязвимости как с сетевой точки зрения, так и с программной, поскольку ключевым элементом являются смарт-контракты, используемые для повышения функциональности сети.

интернет транспортных средств, SD-IoV, блокчейн.

Каждая современная машина оснащена бортовым компьютером и большим количеством датчиков, которые собирают и обрабатывают различные виды данных в реальном времени. Согласно концепции интернета транспортных средств, производится постоянный обмен данными для повышения

безопасности водителей и получения лучшей конфигурации транспортной инфраструктуры. Поэтому наиболее актуальной проблемой является обеспечение безопасности систем интернета транспортных средств. Для решения этой проблемы исследователи предполагают интеграцию технологий SD-IoV и блокчейн. Последняя технология обеспечивает децентрализованную платформу для организации доступности приложений в реальном времени и установлении защищенного соединения между компонентами транспортной инфраструктуры. Также блокчейн обеспечивает конфиденциальность и работоспособность всех участников системы и всей инфраструктуры в целом с точки зрения доступности, стоимости, целостности и времени выполнения запросов. Каждый элемент в подобной системе представляет из себя узел, который может генерировать данные, обрабатывать их посредством процедуры майнинга или принимать актуальную информацию от приложений реального времени. Количество узлов ограничивается только пропускной способностью сети и напрямую влияет на качество предоставляемых услуг. Помимо горизонтальной масштабируемости решается проблема производительности централизованного сервера, который может представлять из себя узкое место всей инфраструктуры. Платформа блокчейн децентрализована и по умолчанию подразумевает распределение нагрузки и ролей. Несмотря на достоинства, системы SD-IoV с применением технологии блокчейн крайне уязвимы для атак ввиду своей самоорганизующейся природы и использования программных продуктов с открытым исходным кодом. На данный момент выделяются следующие типы атак на системы SD-IoV: атаки захвата контроля над сетью; атаки на ограничение доступности; атаки внедрения в структуру сети; атаки на конфиденциальность.

Рассмотрим *атаки захвата контроля над сетью.*

Атака Сивиллы является важной угрозой для любой децентрализованной платформы [1]. В ходе атаки злоумышленник использует множество сгенерированных аккаунтов или узлов для захвата контроля над сетью. Злоумышленник может отказаться от приема и передачи созданных блоков, успешно блокируя действия участников сети. Также возможен обман системы GPS путем отправки поддельных сигналов и ввода транспортное средство в заблуждение.

При *атаке 51 процента* в тот момент, когда злоумышленник контролирует более половины участников сети посредством атаки Сивиллы, он становится способен умышленно исключать и отменять транзакции пользователей и даже предотвращать добычу майнеров, что приводит к майнинговой монополии. Основными способами защиты от атак Сивиллы и 51 процента является заполнение сети реальными пользователями и использование в архитектуре платформы единого алгоритма консенсуса.

При *атаке с маскировкой* злоумышленник некоторое время действует как добросовестный пользователь, создавая хорошую репутацию, а затем использует свой аккаунт для совершения злонамеренных действий, вводя в заблуждение других участников сети. В некоторых вариациях злоумышленник может использовать идентификатор другого пользователя с хорошей репутацией. Такую атаку можно предотвратить, используя средства мониторинга и усиленную аутентификацию пользователей.

При *атаке червоточины* вредоносные узлы взаимодействуют друг с другом и создают скрытые скоростные каналы связи с целью контролировать поток трафика и получать конфиденциальную информацию [2]. Атаки червоточины имеют различные способы влияния на сеть среди которых изменение инкапусулированных пакетов, нарушение маршрутизации, создание ложного короткого пути, как частный случай нарушения маршрутизации и множественное повторение запроса пользователя.

Примером *атаки на ограничение доступности* является *отказ в обслуживании*, цель которого - вывод из строя центрального сервера, ответственного за обработку запросов, или одного или нескольких узлов сети блокчейн. Основным способом совершения атаки является генерация максимально возможного количества запросов.

Примером атаки внедрения в структуру сети является *атака «человек посередине»*. Она представляет пример перехвата данных в сети. Злоумышленник с легкостью может объявить себя главным узлом и перехватить конфиденциальную информацию.

Представим *атаки на конфиденциальность*.

Атака прослушивания представляет собой атаку, целью которой является сбор информации об участниках сети. Данный вид атак достаточно трудно отследить из-за их пассивного характера.

Атака повторного воспроизведения является достаточно редким случаем, который возможен при разделении блокчейн сети на текущую сеть и ее копию. В такой ситуации обработанные в одной сети транзакции можно модифицировать и выполнить в другой сети.

Пылевая атака представляет собой перевод на целевой счет небольшое уникальное количество средств, которые позволят неявно идентифицировать владельца кошелька. Затем по этому признаку после неопределенного числа переводов злоумышленник может отслеживать владельца целевого кошелька и даже получить доступ к конфиденциальной информации.

В качестве основных *методов защиты от атак* на системы SD-IoV выделяются: общие методы, а также методы, связанные с конфиденциальностью, репутацией и аутентификацией.

Представим ниже *общие методы*. В [3] разработан универсальный способ торговли энергией для электромобилей. Авторы предлагают использовать специальные токены для выполнения транзакций, вариативный метод

выбора узла майнера и в качестве алгоритма консенсуса - доказательство работы. В [4] исследуются проблемы безопасности, связанные с интеграцией туманных вычислений в интернет вещей и предлагается схема, в которой туманные узлы и алгоритм консенсуса контролируют использование энергии. В [5] вводится концепция интеллектуальной точки доверия к транспортным средствам. Предложенный способ усиливает конфиденциальность, обеспечивает быструю и безопасную связь между транспортными средствами, а также сохраняет и накапливает историю транспортного средства, создавая особые оцениваемые критерии репутации. В [6] используется децентрализованная модель безопасности для управления процессом зарядки электромобилей в интернете транспортных средств. Предложенная модель предполагает использование сети Lightning и особой логики, описанной в смарт контрактах. Данная сеть позволяет выполнять запросы с лучшей производительностью и более низкими затратами на вычисления. В [7] предложен механизм безопасности для инфраструктуры услуг подключенных автономных транспортных средств с использованием технологии блокчейна. Этот механизм основывается на машинном обучении и позволил значительно уменьшить количество поддельных запросов пользователей, компрометацию устройств и изменение скрытых данных пользователей. В [8] предлагается основанная на блокчейне архитектура безопасности для распределенного облачного хранилища. В основе лежит генетический алгоритм для решения проблемы размещения реплик файловых блоков между несколькими пользователями и несколькими центрами обработки данных в среде распределенного облачного хранилища.

Рассмотрим *методы, связанные с конфиденциальностью*. В [9] используется подход к безопасным платежам с сохранением конфиденциальности для сетей vehicle-to-grid на основе процедур регистрации и обработки данных. В [10] представлена методика по обновлению прошивки программного обеспечения на основе блокчейна и разработанного смарт-контракта для автономных транспортных средств. Смарт-контракт используется для обеспечения подлинности и целостности обновлений прошивки и, что более важно, для управления информацией об антивирусах. В [11] предлагается схема отзыва сертификатов для предотвращения внутренних атак в сетях интернета вещей. Предлагаемая структура блокчейна позволяет отслеживать право собственности на сертификаты и эффективно распространять обновления информации.

Опишем примеры *методов, связанных с репутацией*. В [12] предлагаются методы по улучшению безопасности в сетях интернета транспортных средств на основе блокчейна. Вводится процедура отбора майнеров путем репутационного голосования и стимуляции резервных майнеров к участию в проверке блоков. В [13] рассматривается схема безопасного поощрения на основе блокчейна, основанная на репутационном протоколе консенсуса для

достижения эффективного взаимодействия в автомобильной энергетической сети. Валидаторы выбираются на основе их оценки доверия, и каждый валидатор получает стимулы после успешного выполнения механизма проверки.

Представим примеры *методов, связанных с аутентификацией*. В [14] с помощью предложенных механизмов осуществляется аутентификация приложений, управление сетевыми ресурсами и контроль поведения приложений. Использована идея идентификационных карт для управления доверием приложений, а также механизм аутентификации на основе блокчейна. Кроме того, разработан и объяснен смарт-контракт, позволяющий реализовать эту систему. В [15] предлагается архитектура на базе блокчейна, позволяющая владельцу умного автомобиля создавать неизменяемую запись всех данных, называемых автобиографией автомобиля, сгенерированных за время его жизни. Доверие к этой записи гарантируется характеристикой неизменности блокчейна.

В рамках исследования был проведен сравнительный анализ основных видов и типов атак на компоненты интернета транспортных средств с применением технологии блокчейн. Также были рассмотрены базовые способы защиты от этих атак.

В качестве основных результатов исследования можно заключить, что существующие способы защиты от атак имеют недостаточную эффективность и требуют доработки и совершенствования.

Возможные подходы и инструменты, которые могут быть использованы для усовершенствования способов защиты, будут рассмотрены в дальнейших исследованиях авторов работы.

Работа выполнена при частичной финансовой поддержке РНФ (проект № 21-71-20078).

Список используемых источников

1. Buford J.F., Yu H., Lua E.K. P2P Networking and Applications. Morgan Kaufmann, 2009. pp. 319–340.

2. Parvathy K. Wormhole Attacks in Wireless Sensor Networks (Wsn) & Internet of Things (IoT) // International Journal of Recent Technology and Engineering (IJRTE), Vol.10, Isssue 1, 2021.

3. Chaudhary R., Jindal A., Aujla G.S., Aggarwal S., Kumar N. BEST: Blockchain-based secure energy trading in SDN-enabled intelligent transportation system // Computers & Security. 2019. pp. 288–299.

4. Li G., Wu J., Li J., Guan Z., Guo L. Fog Computing-Enabled Secure Demand Response for Internet of Energy Against Collusion Attacks Using Consensus and ACE // IEEE Access. 2018. pp. 11278–11288.

5. Singh M., Kim S. Introduce reward-based intelligent vehicles communication using blockchain // 2017 International SoC Design Conference (ISOCC). 2017. pp. 15–16.

6. Huang X., Xu C., Wang P., Liu H. LNSC: A Security Model for Electric Vehicle and Charging Pile Management Based on Blockchain Ecosystem // IEEE Access, Vol.6, 2018. pp. 13565–13574.

7. Rathee G., Sharma A., Iqbal R., Aloqaily M., Jaglan N., Kumar R. A Blockchain Framework for Securing Connected and Autonomous Vehicles // Sensors. 2019. 19(4). P. 3165.

8. Li J., Liu Z., Chen L., Chen P., Wu J. Blockchain-Based Security Architecture for Distributed Cloud Storage // 2017 IEEE International Symposium on Parallel and Distributed Processing with Applications. 2017. pp. 408–411.

9. Gao F., Zhu L., Shen M., Sharif K., Wan Z., Ren K. A Blockchain-Based Privacy-Preserving Payment Mechanism for Vehicle-to-Grid Networks // IEEE Network. Vol.32, Issue 6, 2018. pp. 184–192.

10. Baza M., Nabil M., Lasla N., Fidan K., Mahmoud M., Abdallah M. Blockchain-based Firmware Update Scheme Tailored for Autonomous Vehicles // 2019 IEEE Wireless Communications and Networking Conference (WCNC). 2019. pp. 1–7.

11. Lei A., Cao Y., Bao S., Li D., Asuquo P., Cruickshank H., Sun Z. A blockchain based certificate revocation scheme for vehicular communication systems // Future Generation Computer Systems. Vol.110, September 2020. pp. 892–903.

12. Kang J., Xiong Z., Niyato D., Ye D., Kim D.I., Zhao J. Toward Secure Blockchain-Enabled Internet of Vehicles: Optimizing Consensus Management Using Reputation and Contract Theory // IEEE Transactions on Vehicular Technology. Vol.68, Issue 3, March 2019. pp. 2906–2920.

13. Wang Y., Su Z., Zhang N. BSIS: Blockchain-Based Secure Incentive Scheme for Energy Delivery in Vehicular Energy Network // IEEE Transactions on Industrial Informatics. Vol.15, Issue 6, June 2019. pp. 3620–3631.

14. Mendiboure L., Chalouf M., Krief F. Towards a Blockchain-Based SD-IoV for Applications Authentication and Trust Management // 5th International Conference, IOV. 2018. pp. 265–277.

15. Ferdous M., Chowdhury M., Biswas K., Chowdhury N., Muthukkumarasamy V. Immutable autobiography of smart cars leveraging blockchain technology // The Knowledge Engineering Review. Vol. 35, No. 3. 2020.

УДК 004.021
ГРНТИ 49.33.29

РАЗРАБОТКА МОДЕЛИ СИСТЕМЫ ОПРЕДЕЛЕНИЯ МЕСТОПОЛОЖЕНИЯ БЕСПРОВОДНЫХ КЛИЕНТОВ СЕТЕЙ СЕМЕЙСТВА IEEE 802.11

В. Е. Дрепа, О. И. Кузьмина, А. А. Миняев

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Сервис определения местоположения занимает важную роль в современных сетях беспроводного доступа. Актуальность разработанной модели обоснована вопросами

безопасности сети, так как даёт возможность определить местоположение злоумышленника, в случае совершения атаки на беспроводную сеть. Кроме того, сервис может упростить поиск целевой аудитории, для которой необходимо настроить таргетированную рекламу, что подтверждает значимость разработанной модели в медиасфере. В статье представлено описание модели системы определения местоположения беспроводных клиентов сетей семейства IEEE 802.11. Рассмотрены компоненты данной модели и описан принцип их взаимодействия. Также в статье продемонстрирована возможная схема для реализации разработанной модели.

беспроводные сети, определение местоположения, RSS, fingerprinting.

Жизнь современного человека трудно представить без сервисов определения местоположения. Данные о геолокации пользователя используются в мобильных приложениях для вызова такси, браузерах, социальных сетях и т. д. В то же время сети беспроводного доступа достигают внушительных масштабов, а количество возможных атак [1–3] увеличивается. Определение местоположения устройства, с которого производится атака на беспроводную сеть, может быть одной из возможностей разработанной модели.

В основе существующих систем определения местоположения лежит Location-based service (LBS) – программный сервис, использующий данные о локации пользователя для управления различными функциями. К компонентам LBS принято относить устройство клиента, с помощью которого пользователь запрашивает необходимую ему информацию, компонент позиционирования, определяющий местоположение клиента, сеть связи, поставщик услуг и контента, который обрабатывает запросы пользователя.

Для определения местоположения клиента сети необходимо измерить расстояние от его устройства до сканирующего устройства, то есть сенсора. Основными методами [4, 5], позволяющими определить это расстояние, являются:

- метод по углу прибытия сигнала (*Angle of Arrival*, AoA);
- метод по времени прибытия сигнала (*Time of Arrival*, ToA);
- метод по разности времени прибытия (*Time Difference of Arrival*, TDoA);
- метод по уровню мощности принимаемого сигнала (*Received Signal Strength*, RSS).

В разработанной в ходе данного исследования модели системы определения местоположения используется метод позиционирования по радиоотпечатку, то есть Fingerprinting (рис. 1), основанный на измерении расстояния по RSS. Такой подход состоит из двух этапов. Первый этап, называемый офлайн этапом, включает в себя измерение RSS на расположенных заранее в разных точках карты сенсорах. Эти измерения называются радиоотпечатками. Каждой точке на карте соответствует своё значение радиоотпечатка, такая карта называется радиокартой. Второй этап, или онлайн-этап, включает в себя определение местоположения устройства клиента в реальном

времени по сопоставлению уровня мощности его сигнала с составленной на первом этапе радиокартой.

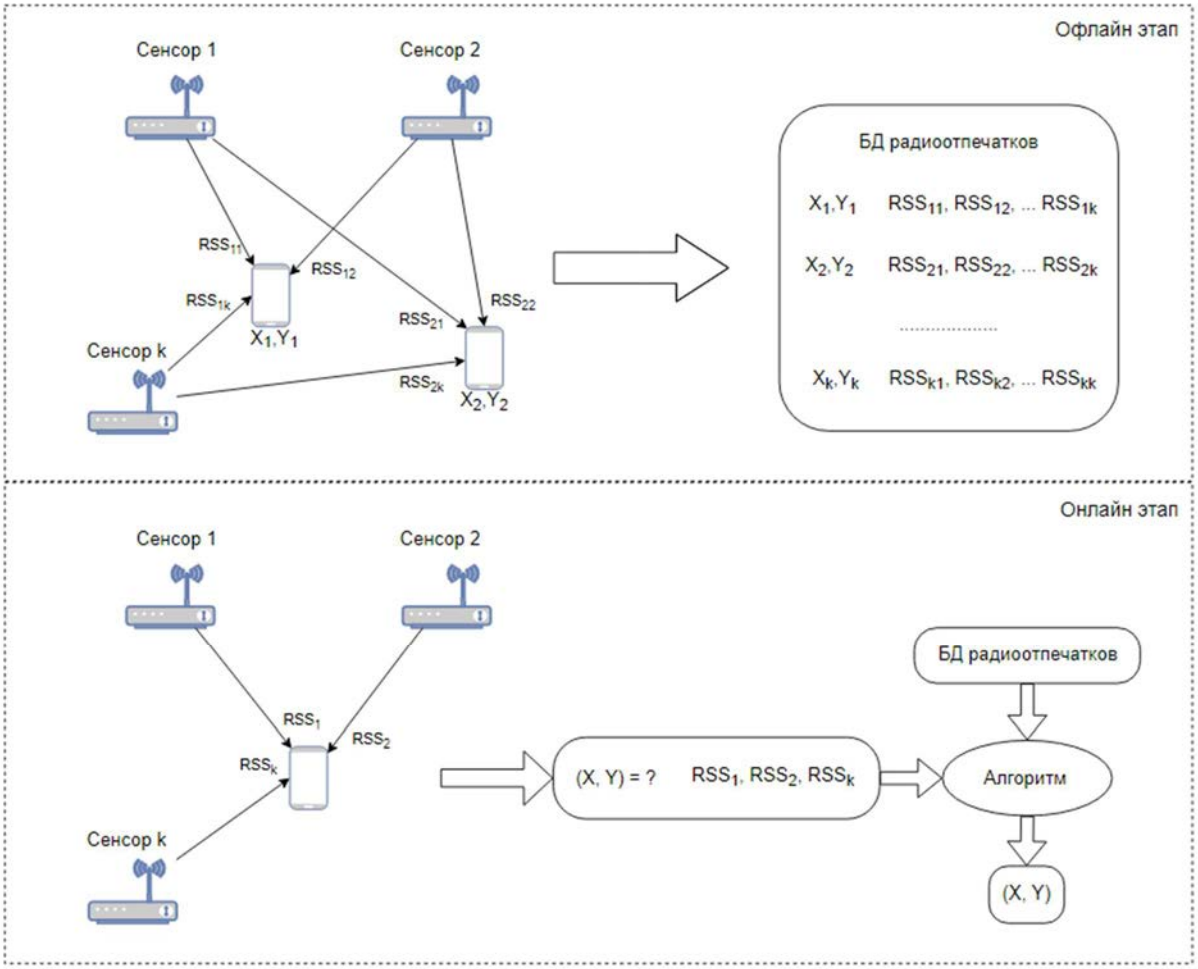


Рис. 1. Метод позиционирования Fingerprinting

Разработанная модель (рис. 2) состоит из устройств захвата информации, в качестве которых могут быть точки доступа в режиме захвата трафика, ноутбуки или микрокомпьютеры с беспроводными адаптерами. К компонентам модели также относится центральный коллектор, который обрабатывает информацию с устройств захвата и передаёт её в программный модуль. Результат программы отображается в базе данных, на основании которой строится графический интерфейс [6] для взаимодействия с пользователем.

Рис. 2. Разработанная модель системы определения местоположения беспроводных клиентов сетей семейства IEEE 802.11

Ранее уже упоминалось, что в разработанной модели используется метод Fingerprinting. Данный алгоритм описан в программном модуле позиционирования (рис. 3). На первом этапе работы программа получает на вход значения координат стен в помещении и значения координат расставленных сенсоров из составленной заранее базы данных, далее производится расчёт радиокарты. На втором этапе на вход программы поддаётся MAC-адрес устройства, местоположение которого необходимо определить. При условии совпадения уровня мощности сигнала, принятого от сенсора с рассчитанной мощностью из радиокарты, а также при совпадении идентификатора сенсора, в таблицу записываются координаты точек, где может находиться клиент с заданным MAC-адресом.

Рис. 3. Описание работы программного модуля позиционирования разработанной модели

Код программного модуля был написан на языке Python. На рис. 4 представлена блок-схема, в которой описана функция, определяющая местоположение устройства клиента по MAC-адресу и RSS.

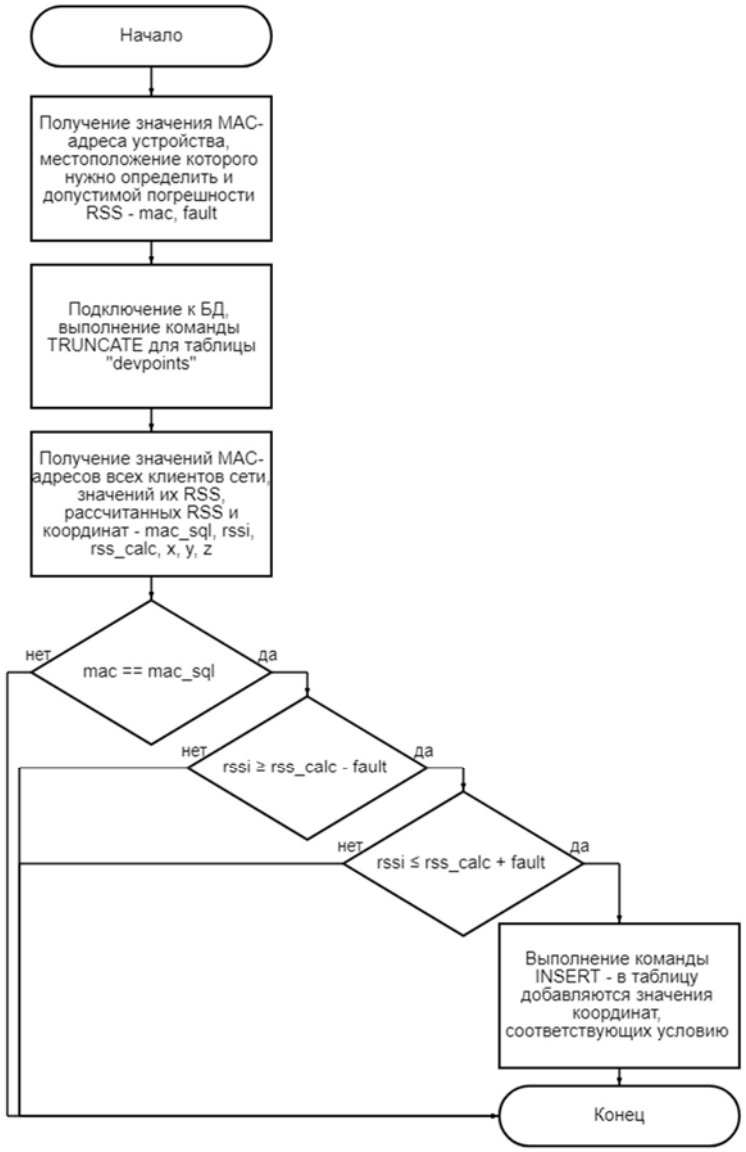


Рис. 4. Блок-схема, описывающая функцию определения местоположения устройства клиента по MAC-адресу и RSS

На рис. 5 представлен фрагмент полей записи БД, где записаны данные о координатах устройства с заданным MAC-адресом. В качестве СУБД использовалась MySQL.

id	loctime	device_mac	colour	mapid	x	y
147	NULL	3c:84:6a:0d:98:49	NULL	NULL	1	11.5
148	NULL	3c:84:6a:0d:98:49	NULL	NULL	1	11.75
149	NULL	3c:84:6a:0d:98:49	NULL	NULL	1.25	5.25
150	NULL	3c:84:6a:0d:98:49	NULL	NULL	1.25	5.5
151	NULL	3c:84:6a:0d:98:49	NULL	NULL	1.25	5.75
152	NULL	3c:84:6a:0d:98:49	NULL	NULL	1.25	6
153	NULL	3c:84:6a:0d:98:49	NULL	NULL	1.25	6.25
154	NULL	3c:84:6a:0d:98:49	NULL	NULL	1.25	6.5

Рис. 5. Фрагмент полей записи БД

На рис. 6 представлена возможная схема для разработанной системы определения местоположения клиентов беспроводной сети.

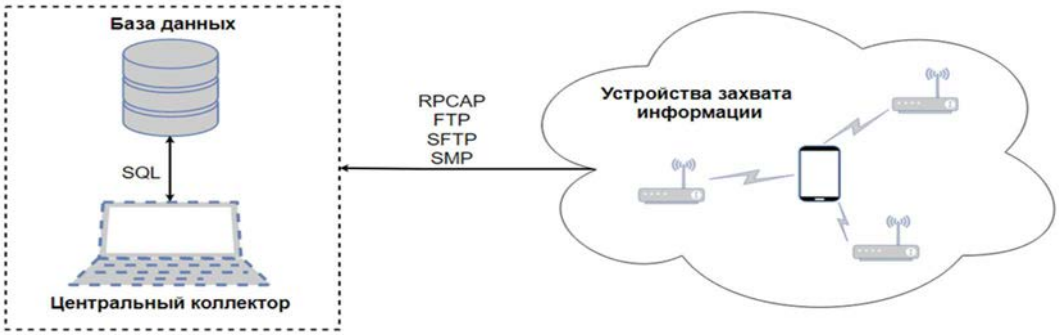


Рис. 6. Возможная схема для разработанной модели

Рассматривая решения LBS у вендоров, таких как Cisco, Huawei, и т. д., можно заметить, что их реализация труднодоступна из-за высокой стоимости оборудования и программного обеспечения. По этой причине в ходе данного исследования была разработана собственная модель системы определения местоположения, для которой не требуется больших денежных затрат.

Список используемых источников

1. Ахрамеева К. А., Ворошнин Г. Е., Ковцур М. М. Исследование уязвимостей оборудования MikroTik к атакам на беспроводные сети // Актуальные проблемы инфотелекоммуникаций в науке и образовании. X Юбилейная Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2021. Т. 1. С. 57–63.

2. Киструга А. Ю., Ковцур М. М., Оганесян А. Г. Исследование устойчивости точек доступа в режиме PSK к DOS атакам на беспроводную сеть // Актуальные проблемы инфотелекоммуникаций в науке и образовании. X Юбилейная Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2021. Т. 1. С. 485–489.

3. Ковцур М. М., Герлинг Е. Ю., Коновалова В. В., Киструга А. Ю. Исследование способов удаленного перехвата трафика в корпоративных сетях // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2021. № 4. С. 68–75.

4. Ковцур М. М., Киструга А. Ю., Петров В. А. Исследование методов дальнометрии в беспроводных сетях // REDS: Телекоммуникационные устройства и системы. 2021. Т. 11. № 4. С. 42–49.

5. Намиот, Д. Е. Сетевая пространственная близость между мобильными устройствами // International Journal of Open Information Technologies. 2021. Т. 9. № 1. С. 80–85.

6. Герлинг Е. Ю., Ковцур М. М., Фёдорова А. Э. Разработка веб-интерфейса для системы мониторинга беспроводных сетей семейства IEEE 802.11 // Актуальные проблемы инфотелекоммуникаций в науке и образовании. X Юбилейная Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2021. Т. 1. С. 224–228.

УДК 004.732
ГРНТИ 49.43.29

ОБЗОР РЫНКА КЛИЕНТСКИХ УСТРОЙСТВ С ПОДДЕРЖКОЙ ТЕХНОЛОГИИ WI-FI 6

Р. А. Дунайцев, А. В. Светова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье представлен обзор рынка клиентских устройств с поддержкой технологии Wi-Fi 6. Сравнивается скорость внедрения нового поколения Wi-Fi 6 (IEEE 802.11ax) в сравнении с предыдущим поколением Wi-Fi 5 (IEEE 802.11ac). Также определяются темпы роста и тенденции развития рынка Wi-Fi устройств. Кроме того, представлены доли брендов на рынке ноутбуков и Wi-Fi роутеров с поддержкой технологии Wi-Fi 6 в России по состоянию на 2022 год.

IEEE 802.11ax, Wi-Fi 6, Wi-Fi роутер.

В сентябре 2019 года Альянс Wi-Fi (*Wi-Fi Alliance*) начал официальную сертификацию оборудования на совместимость и соответствие стандарту IEEE 802.11ax [1]. Готовность участвовать в программе сертификации выразили компании ASUS, Broadcom, Cisco, Comcast, Intel, NETGEAR, Samsung, TP-Link, Xiaomi и др., после чего на рынке стали появляться устройства, поддерживающие данную технологию. Новые возможности Wi-Fi 6 существенно повышают общую производительность беспроводной локальной сети с большим количеством подключаемых устройств (смартфонов, планшетов, ноутбуков, Интернет вещей и т. п.). Если говорить о смартфонах, то Samsung Galaxy Note 10 стал первым в мире сертифицированным устройством с поддержкой технологии Wi-Fi 6. На данный момент практически все флагманы, вышедшие после 2019 года, имеют поддержку данного стандарта. Сюда можно отнести такие модели, как Apple iPhone 11, Samsung Galaxy S10, Xiaomi Mi 10, ZTE Axon 10s Pro и т.д. В основном в этой категории устройств лидируют компании Apple и Samsung [2].

Крупнейшие производители ноутбуков тоже заинтересовались данной технологией. Поддержка IEEE 802.11ax уже стала характеристикой, на которую потребители обращают все больше внимания при выборе ноутбука. Именно поэтому с середины 2019 года почти все новые устройства среднего и премиального сегментов оснащаются адаптерами поколения Wi-Fi 6. По данным, представленным на рис. 1, первое место по внедрению этой технологии занимает китайская компания Lenovo. В настоящее время ее доля составляет 22 % рынка. Второе и третье места занимают американские HP (21 %) и Dell (13 %) соответственно.

Но не только смартфоны, планшеты и ноутбуки получают поддержку IEEE 802.11ax. Современные бытовые устройства также комплектуются беспроводными адаптерами Wi-Fi 6. В частности, телевизоры Samsung (модели Q900 и Q950) также могут похвастаться поддержкой IEEE 802.11ax [3]. Однако стандарт еще только внедряется и, к сожалению, далеко не все устройства его поддерживают. Например, хотя в России концепция Интернета вещей (*Internet of Things*, IoT) набирает все большую популярность, пока нет ни одного устройства умного дома с Wi-Fi 6, хотя технически это вполне реализуемо. Также пока нет ни одной игровой консоли, ТВ-приставки, устройства дополненной реальности (*Augmented Reality*, AR) или виртуальной реальности (*Virtual Reality*, VR) с поддержкой Wi-Fi 6 [4].

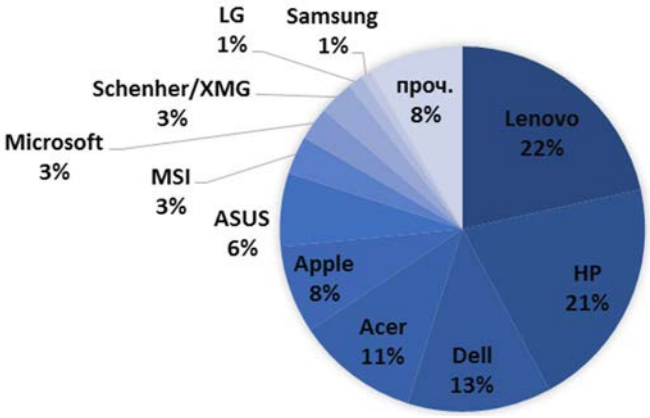


Рис. 1. Доли брендов на рынке ноутбуков с технологией Wi-Fi 6 в РФ на 2022 год

Тем не менее, можно заметить, что на рынке Wi-Fi оборудования успех обеспечивают такие параметры, как широкий ассортимент, доступность, предложение актуальных и востребованных решений. У каждого поставщика есть своя линейка моделей под различные запросы и требования потребителей [5].

Для наглядности проведем анализ лидирующих компаний по производству и продаже Wi-Fi роутеров с поддержкой Wi-Fi 6. При рассмотрении Wi-Fi роутеров, представленных в крупнейших российских торговых сетях, можно заметить, что наибольшую долю этого сегмента рынка занимает продукция китайской компании TP-Link. Ее доля составляет 23 % от общего объема продаваемых Wi-Fi роутеров. Второе место занимает продукция компании NETGEAR (15 %). Также в тройку лидеров входит компания Ubiquiti (11 %). Собранные из открытых источников данные представлены на рис. 2.

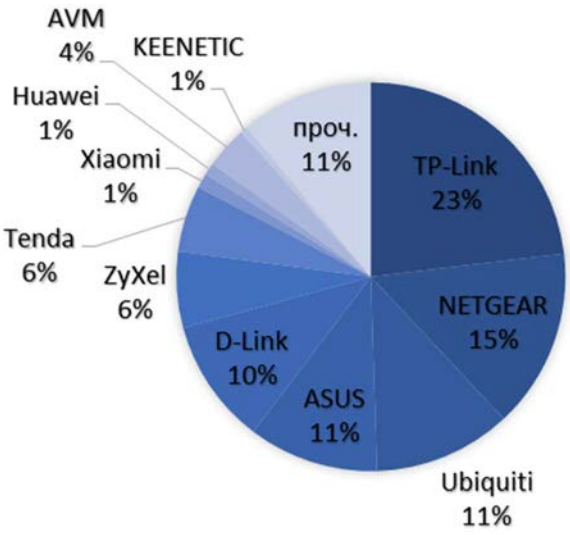


Рис. 2. Доли брендов на рынке Wi-Fi роутеров с технологией Wi-Fi 6 в РФ на 2022 год

Совершенно очевидно, что развитие технологий оказывает заметное влияние на динамику рынка и заставляет потребителей заменять старое оборудование на новое. На рис. 3 представлены темпы внедрения оборудования с поддержкой стандартов IEEE 802.11ac и IEEE 802.11ax. Важно отметить, что стандарт IEEE 802.11ax обратно совместим со всеми предыдущими поколениями Wi-Fi как в диапазоне 2,4 ГГц, так и в диапазоне 5 ГГц. Именно поэтому с появлением Wi-Fi 6 предыдущие версии не теряют своей актуальности.

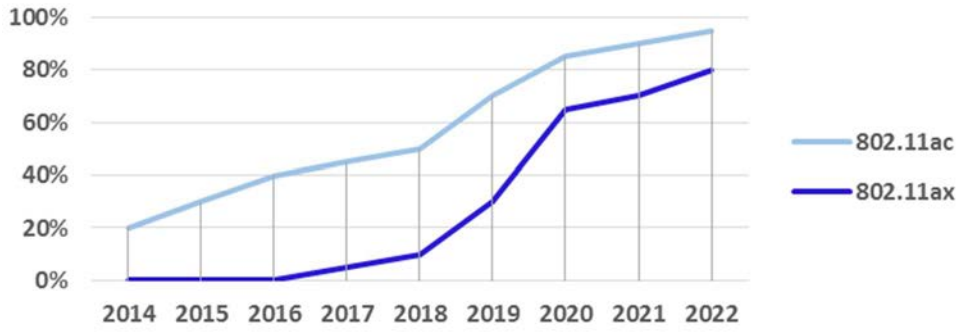


Рис. 3. Скорость внедрения Wi-Fi 6 в сравнении с предыдущим поколением Wi-Fi 5

Подводя итог, следует признать, что с ростом количества клиентских устройств Wi-Fi растет и популярность беспроводных локальных сетей. Новый стандарт IEEE 802.11ax позволит снизить задержки в доставке данных, увеличить скорость передачи, повысить общую пропускную способность сети и оптимизировать ее работу [6]. Разработчики уверены, что в ближайшее время спрос на устройства Wi-Fi 6 будет только расти. Наиболее популярными устройствами по-прежнему будут смартфоны, планшеты и ноутбуки, но технология найдет свое применением и во многих других видах оборудования [7].

Список используемых источников

1. Wi-Fi CERTIFIED 6 coming in 2019. URL: https://www.wi-fi.org/news-events/newsroom/wi-fi-certified-6-coming-in-2019 (дата обращения: 31.03.2022).

2. Что такое Wi-Fi 6 и какие устройства поддерживают. URL: https://journal.rozetka.com.ua/chto-takoe-wi-fi-6-i-kakie-ustroystva-podderzhivayut/ (дата обращения: 31.03.2022).

3. Samsung первой в мире показала телевизоры с поддержкой Wi-Fi. URL: https://www.ixbt.com/news/2020/03/05/samsung-wi-fi-6.html (дата обращения: 31.03.2022).

4. Wi-Fi 6 уже здесь: стоит ли переходить на Wi-Fi 6 в 2020 году? URL: https://www.thefastcode.com/ru-rub/article/wi-fi-6-is-here-should-you-upgrade-to-wi-fi-6-in-2020 (дата обращения: 31.03.2022).

5. Рынок Wi-Fi-роутеров: умеренный рост при завидной стабильности. URL: https://www.crn.ru/numbers/reg-numbers/detail.php?ID=132758 (дата обращения: 31.03.2022).

6. История возникновения Wi-Fi 6 глазами участника рабочей группы. URL: https://e.huawei.com/ru/products/enterprise-networking/wlan/wifi-6/201903181647 (дата обращения: 31.03.2022).

7. Экосмартфоны и Wi-Fi 6: семь технологических трендов 2022 года. URL: https://trends.rbc.ru/trends/industry/62022a909a79475e55c803c2 (дата обращения: 31.03.2022).

УДК 004.732
ГРНТИ 49.33.31

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ПРОВОДНЫХ ЛОКАЛЬНЫХ ВЫЧИСЛИТЕЛЬНЫХ СЕТЕЙ ПО ТИПУ СРЕДЫ ПЕРЕДАЧИ

В. С. Елагин, С. А. Обухов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Исследование посвящено сравнению типов проводных сред передачи, используемых в локальных вычислительных сетях (ЛВС). Сформулирована классификация ЛВС по типу канала передачи данных. Выбрана методика исследования по ряду критериев. Произведён сравнительный анализ сред передачи данных в ЛВС. Создана сводная таблица в целях обобщения данных анализа. Сделан вывод о преимуществе волоконно-оптической ЛВС над ЛВС на основе медной витой пары.

локально вычислительные сети, витая пара, оптоволокно, гибридные сети, среда передачи.

Локальная вычислительная сеть (ЛВС) – это система, обеспечивающая обмен данными между вычислительными устройствами, охватывающая небольшую территорию и использующая ориентированные на эту территорию средства и методы передачи данных [1].

Популярным способом классификации ЛВС является их классификация по масштабу производственного подразделения, в пределах которого действует сеть. Различают [2]:

– сети отделов;
– сети кампусов;
– корпоративные сети.

Современные проводные ЛВС можно классифицировать по типу канала связи:

– медные ЛВС, на основе витой пары;
– волоконно-оптические ЛВС.

Принципиальным требованием к сети является выполнение её основной функции – предоставить возможность пользователям доступ к разделяемым ресурсам всех компьютеров и устройств, подключенных к сети [3].

Производительность, эффективность, надежность, долговечность, совместимость, масштабируемость, универсальность, управляемость, защищенность – сопутствующие критерии, связанные с качеством выполнения основой задачи [4].

В общем случае сети целесообразно сравнивать по следующим критериям:

– пропускная способность;
– скорость передачи данных;
– максимальное расстояние передачи;
– защищённость;
– безопасность;
– устойчивость к воздействиям;
– долговечность.

С учётом изложенного, в произведено сравнение ЛВС с медной и ЛВС с оптической средой передачи.

Пропускная способность и скорость передачи данных

В сущности, скорость передачи сигнала во многом зависит от расстояния между оборудованием. При малой длине соединения, у медной витой пары и волоконно-оптического кабеля (ВОК), на данный момент приблизительно одинаковая пропускная способность от 100 до 112 Гбит/с [5].

При том, у витой пары такая пропускная способность технически реализована только через несколько параллельных каналов передачи и увеличение сечения жил кабеля. Витая пара категории *CAT*8, с полосой пропускания сигнала 1 600–2 000 МГц, способна обеспечить скорость передачи данных до 100 Гбит/с на дистанцию до 55 метров [6].

Экспериментальным путём уже были достигнуты более высокие показатели скорости по оптоволокну. Это возможно, например, при использовании одномодового волокна класса *OS2* при широкополосной передаче в диапазоне, объединяющем одномодовые окна прозрачности [7]. Такие эксперименты уже проводились японской корпорацией *NTT Communications* и другими исследовательскими лабораториями.

Резюмируя вышесказанное, резервы для уплотнения и роста пропускной способности в ВОК велики, в то время как в медном кабеле уже сказываются физические ограничения, связанные с энергопотреблением и тепловыделением активного оборудования.

Расстояние передачи

В отличие от медного кабеля, ВОК способен передавать данные на значительно более дальние расстояния, с большей скоростью и без потери сигнала. Это возможно благодаря передаче сигнала в форме световых лучей [8].

Максимальная длина витой пары, при которой она может обеспечить передачу сигнала без ощутимых потерь, составляет не более 100 метров между усилителями сигнала, согласно нормативам структурированных кабельных систем [9].

Оптический кабель свободен от ограничений, имеющихся у медного кабеля. ВОК может передавать сигнал на расстояние свыше 100 метров. Так, расстояние возможной передачи сигнала зависит от типа применяемого оптического кабеля, структуры сети и длины волны, и оно варьируется в пределах от 550 метров для многомодового кабеля, и до 40 километров для одномодового кабеля [5, 10, 11].

Устойчивость к воздействиям

Оптоволоконный кабель гораздо менее подвержен воздействию различных факторов окружающей среды, чем медный кабель, таким как температура и электромагнитные колебания.

ВОК можно прокладывать рядом с промышленным и технологическим оборудованием, в помещениях с повышенной влажностью. В то время как при параллельной прокладке минимальное расстояние между витой парой и силовым кабелем должно составлять не менее 12,5 сантиметров [9].

При необходимости включения в ЛВС нескольких отдельностоящих зданий использовать медную витую пару «по воздуху» строго не рекомендуется. Во время грозы при отсутствии должного заземления и экранирования могут возникнуть сильные наводки на сигнал, что повлечет выход из строя активного оборудования компьютера (сетевая карта, материнская плата) в составе ЛВС. Риск возникновения аналогичной ситуации в случае с ВОК отсутствует.

Защищённость и безопасность сети

ВОК имеет повышенные показатели безопасности. Оптическое волокно не передает электричество, не даёт излучений, поэтому оптические сигналы почти невозможно перехватить. При совершении попытки «вторжения» в линию и создания поврежденного участка, это легко отследить благодаря приостановке светового потока, приводящей к прекращению передачи информации [12, 13].

Разорванное или поврежденное оптическое волокно может быть оперативно обнаружено с помощью ряда методов контроля, включая контроль фактической передачи мощности или передачи пилот-сигнала.

При передаче сигнала по витой паре используется электричество, в этом случае поток данных возможно перехватить.

Повреждённый медный кабель способен вызвать короткое замыкание. Оперативно обнаружить место износа медного кабеля невозможно, так как отсутствуют такие эффективные методы мониторинга, поиска и локализации разрыва, как в оптических сетях.

Долговечность

Продолжительность эксплуатации медного кабеля на порядок меньше из-за процессов окисления и деградации металла в процессе эксплуатации и старения. Следовательно, долговечность витой пары меньше, сеть нужно обслуживать чаще, в том числе заменять составляющие на новые по истечению допустимого срока эксплуатации (5 лет).

Срок службы волоконно-оптических кабелей при соблюдении указаний по эксплуатации и при отсутствии воздействий, превышающих допустимые, составляет не менее 25 лет [6].

Удобство монтажа

Для соединения большого количества компьютеров и других стационарных устройств необходимо ветвление кабеля.

В настоящее время известно лишь несколько способов ветвления оптоволоконной системы, но они сложны в реализации и дороги в исполнении. Сращивание оптоволокна требует специальной подготовки и инструментов. Цена самих соединителей и инструментов достаточно высока [14].

Срастить витую пару существенно проще и дешевле. Медную сеть легче масштабировать, она более универсальна в плане возможности изменения конфигурации сети и подключения дополнительного оборудования.

В то же время оптический распределительный шкаф занимает значительно меньше рабочего пространства (компоненты расположены более компактно), что облегчает обслуживание узла связи.

На основании вышеизложенного и ряда других параметров, создана сводная таблица для анализа данных.

ТАБЛИЦА. Сравнение медной и оптической среды передачи

Параметр	ВОК	Медная витая пара
Пропускная способность	60 Тбит / с и выше	10 Гбит / с
Максимальное расстояние передачи	2 км – многомодовый ВОК 40 км – одномодовый ВОК	100 метров
Скорость передачи на большие расстояния	10 Гбит/с	1 Гбит/с

Параметр	ВОК	Медная витая пара
Шум	Не влияет	Восприимчивость к электромагнитным, радиочастотным помехам перекрестным помехам и скачкам напряжения
Безопасность	Не восприимчив к сжатию	Восприимчивость к сжатию
Обработка	Легкий, тонкий диаметр, высокая способность к растяжению	Тяжелый, большой диаметр, строгие требования к растяжению
Продолжительность эксплуатации	25 лет	5 лет
Вес (бухта 305 метров)	1,81 кг	17,7 кг
Потребляемая энергия	2 Вт на пользователя	> 10 Вт на пользователя
Будущее	Переход к настольному ПК	Внедрение *CAT*8

Опираясь на данные в таблице, можно сделать вывод о превосходстве ВОК в ЛВС над медным кабелем.

Список используемых источников

1. Максимальная длина витой пары. URL: https://clck.ru/eYE37 (дата обращения: 23.03.2022).

2. Витая пара или оптоволокно – что выбрать? URL: https://anlan.ru/articles/vitaya-para-ili-optovolokno-chto-vybrat (дата обращения: 23.03.2022).

3. Пескова С. А., Кузин А. В., Волков А. Н. Сети и телекоммуникации: учеб. пособие для студ. высш. учеб. заведений. 2-е изд., стер. Москва : Издательский центр «Академия», 2007. 352 с.

4. Волоконно-оптическая линия связи. URL: https://clck.ru/eYDqz (дата обращения: 23.03.2022).

5. Локальная вычислительная сеть (ЛВС). Разработка и установка. URL: http://rina.pro/napravleniya-deyatelnosti/sistemy-elektrosvyazi/lokalnaya-vychislitelnaya-set (дата обращения: 23.03.2022).

6. Фокин В. Г. Оптические системы передачи и транспортные сети: учеб. Пособие. Москва : Изд-во ЭКО-ТРЕНДЗ, 2008. 272 с.

7. 8 бесспорных преимуществ современных оптоволоконных кабелей. URL: https://clck.ru/eYDy5 (дата обращения: 23.03.2022).

8. Принцип построения вычислительных сетей. URL: http://math.gsu.by/wp-content/uploads/courses/networks/r1.4.html (дата обращения: 23.03.2022).

9. Гольдштейн Б. С., Соколов Н. А., Яновский Г. Г. Сети связи: учебник для вузов. СПб. : Изд-во БХВ-Санкт-Петербург, 2010. 400 с.

10. Пропускная способность и скорость распространения сигнала в локальной сети URL: https://clck.ru/eWUW9 (дата обращения: 23.03.2022).

11. Иоргачев Д. В., Бондаренко О. В. Волоконно-оптические кабели и линии связи: инженерная энциклопедия ТЭК. Москва : Изд-во ЭКО-ТРЕНДЗ, 2002. 277 с.

12. УПИС лекции СПбГУТ. URL: https://studfile.net/preview/6330990/ (дата обращения: 23.03.2022).

13. Одномодовое волокно: о типах и применениях. URL: https://community.fs.com/ru/blog/single-mode-fiber-os1-vs-os2-what-is-the-difference.html (дата обращения: 23.03.2022).

14. Каков срок службы оптического кабеля? URL: https://vols.expert/faq/ (дата обращения: 23.03.2022).

УДК 004.946
ГРНТИ 47.63.35

ТЕХНИЧЕСКИЕ ОСОБЕННОСТИ И ОБЛАСТИ ПРИМЕНЕНИЯ СМЕШАННОЙ РЕАЛЬНОСТИ, ОТЛИЧИЯ ОТ ВИРТУАЛЬНОЙ И ДОПОЛНЕННОЙ РЕАЛЬНОСТИ

В. С. Елагин, Г. И. Юрьев

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Смешанная реальность (Mixed Reality, MR) может быть использована для дополнения реальности различными способами, например, для наложения аннотаций и данных для обучения или анализа, или для предоставления виртуального 3D-контента, совместно используемого несколькими пользователями находясь в одном физическом пространстве. В мире смешанная реальность применяется уже в течение нескольких лет, но ее использование все еще довольно ограничено. В этой статье представлен обзор технологии смешанной реальности, сфер применения и потенциала развития. Дан обзор данной технологии и того, что она может дать человеку, описано почему эта технология интересна обществу, и представлены некоторые актуальные вопросы и проблемы Mixed Reality как технологии.

смешанная реальность, голограмма, виртуальный контент, информационное взаимодействие, технологические возможности.

В последние годы технологии VR, AR и MR стремительно совершенствовались. «Виртуальная реальность» (VR) относительно хорошо известна и определяется как предоставление пользователю полностью сгенерированной компьютером виртуальной 3D-среды. Но «смешанная реальность» (MR) тесно связана с «дополненной реальностью» (AR), и оба эти понятия могут означать несколько разных вещей. И все эти понятия являются частью объединённого термина «расширенная реальность» (XR).

Итак, под «смешанной реальностью» подразумевается применение технологии для добавления виртуального контента, укорененного в физиче-

ском мире, реалистичным образом. Это включает в себя естественное взаимодействие с таким контентом. Голограммы – это трехмерные виртуальные объекты, созданные компьютером, которые выглядят и действуют так, как будто они являются частью реального мира. Голограммы остаются на месте, когда человек ходите вокруг них, их можно рассматривать под любым углом, они закрывают реальные объекты позади них, любые звуки, издаваемые ими, кажутся исходящими из их местоположения. В некоторых случаях на голограммы может даже влиять освещение реального мира, чтобы усилить их интеграцию с реальностью.

Дополненная реальность (AR) имеет много общего с тем, что названо о смешанной реальности, но ключевое различие заключается в том, что контент AR обычно накладывается поверх реальности и вместо шлема смешанной реальности используется мобильный телефон или планшет. Если не использовать шлем MR, то виртуальный контент представляется человеку менее реалистичным и захватывающим. MR-шлем позволяет более реалистично и практично взаимодействовать и обеспечивает большее погружение в другую реальность. Взаимодействие с голограммами в MR обычно осуществляется с помощью жестов рук, голосовых команд или взгляда.

Технология MR находится в стадии разработки уже довольно долгое время, но еще не стала популярной отраслью. В течение некоторого времени ходили слухи, что Apple и Facebook могут представить аналогичные продукты в ближайшем будущем, что было бы хорошо с точки зрения конкуренции, а значит, выбора и цены, но были опубликованы лишь некоторые фрагменты информации.

В январе 2020 года главный научный сотрудник Facebook предсказал, что потребуется «5-10 лет», чтобы технология AR была достаточно развита для массового внедрения [1]. Под термином AR здесь подразумевались «очки дополненной реальности». Но 5–10 лет – это не очень большой срок для технологии, которая в настоящее время имеет лишь очень ограниченное и часто экспериментальное применение. За короткий период времени в несколько лет смешанная реальность прошла путь от «интересной концепции» до чего-то, что уже представляет ценность и уникальные возможности.

Несмотря на то, что устройства MR ещё не получили широкого распространения, отчасти из-за высокой стоимости устройства, за прошедшие годы было проведено довольно много экспериментов и исследовательских проектов по использованию в разных сфера. В некоторых случаях это уже привело к регулярному использованию. Но потенциал применения технологии в образовании и исследованиях гораздо больше.

Так, например, колледж Фрисландии использует приложениемдля изучения анатомии человека и обучения первой помощи. А Центр инноваций

Лейденского университета разработал приложение AugMedicine для интерактивной визуализации компьютерных томограмм в смешанной реальности для обучения студентов-медиков случаям трансплантации.

Лаборатория «4D Research Lab» Амстердамского университета использовала AR и MR в серии экспериментов по обучению и пониманию археологии, истории и наследия. В Университете Утрехта было проведено исследование по визуализации рентгеновского излучения для обучения радиационной безопасности с использованием смешанной реальности [2]. Университет Вагенингена участвует в многолетнем исследовательском проекте по изучению дополнительных преимуществ MR для сельского хозяйства [1]. Исследователи из VU Amsterdam оценили HoloLens 1 как средство предоставления голографических 3D подсказок для облегчения замирания походки у людей с болезнью Паркинсона [3], где возможности отслеживания использовались для анализа движений человека.

Также некоторые другие примеры, не относящиеся непосредственно к академическим учреждениям, но демонстрирующие различные аспекты MR:

- Приложение Microsoft Designing Holograms представляет собой учебное пособие по ряду аспектов разработки смешанной реальности. Инструкция представлена в виде 3D-макета комнаты с анимированным пользователем и объектами для объяснения концепций MR. Затем переплетается с применением этих концепций в реальной комнате, в которой присутствует пользователь. Таким образом, виртуальная среда обучения легко сочетается с ее применением в реальном мире.
- Apollo 11 Mission AR – это короткий документальный фильм в смешанной реальности о миссии Apollo 11 по исследованию Луны. Он отличается красивой графикой и анимированными 3D-моделями, достигнутыми благодаря потоковой передаче контента на HoloLens.
- Kippy's Escape – это игровое введение в смешанную реальность в виде простой игры, в которой игроку предстоит узнать, как провести 3D-фигуру через ряд препятствий. Она интуитивно обучает некоторым из доступных видов взаимодействия рук с HoloLens.
- Разработка компанией Velicus, представляет собой приложение HoloLens для сертифицированного обучения сердечно-легочной реанимации и AED в смешанной реальности. Новизна заключается в том, что обучение, достаточно хорошо соответствует реальному обучению, чтобы обеспечить сертификацию.

Широкое разнообразие приведенных примеров дает некоторое представление о том, что возможно с помощью MR. На более общем уровне смешанная (и дополненная) реальность в академической среде часто используется для обеспечения новых способов обучения и взаимодействия, для развития новых практических навыков безопасным и/или более доступным

способом, для обеспечения новых форм совместной работы или для того, чтобы люди могли использовать обработку изображений и данных для дополнения и анализа реальных сцен.

Особыми преимуществами MR-шлема являются:

•Уникальное сочетание реальности с виртуальным контентом естественным образом. Количество отображаемого виртуального контента может быть выбрано в соответствии с конкретным приложением. Это может быть от нескольких небольших виртуальных аннотаций на реальном объекте (например, виртуальное указание основных компонентов лабораторного оборудования) до большой виртуальной сцены с множеством компонентов и сложным взаимодействием.

•Пользователи по-прежнему могут воспринимать и взаимодействовать с реальным миром. Это особенно важно для безопасной навигации и взаимодействия с другими пользователями, находящимися рядом. Для последнего MR позволяет реалистично и естественно взаимодействовать. Это контрастирует с VR, где из-за цели полного погружения пользователя в виртуальный мир для воплощения пользователей требуется неестественное и ограниченное решение.

•Многопользовательские приложения особенно могут использовать преимущества сочетания обычной физической среды с общим контентом MR. Участники могут выбрать свой собственный вид общего виртуального контента или даже внести личные коррективы. А с помощью усовершенствованной так называемой «привязки» становится возможным поместить виртуальный контент в фиксированное физическое место, даже на длительный период времени. Закрепленный контент могут просматривать, редактировать или взаимодействовать с ним несколько пользователей, одновременно или в разные моменты времени.

•Благодаря используемой технологии прозрачного дисплея, пользователь всегда воспринимает некоторые части реального мира, что сводит к минимуму вероятность тошноты или других физических эффектов. Использование MR-шлема очень похоже на ношение пары современных очков, в отличие от полного погружения в виртуальную реальность, которое может быть более дискомфортным.

Конечно, в применении и использовании MR есть и некоторые недостатки:

•Естественное взаимодействие рук – на самом деле нуждается в более глубоком технологическом развитии, чтобы стать действительно надежной и оправдать возложенные надежды. В настоящее время его можно использовать, но неправильное распознавание движений рук или пользовательский интерфейс, не оптимизированный для такого взаимодействия, приводят к разочарованию пользователей.

•К использованию MR-устройств в целом придется привыкать, поскольку методы взаимодействия в настоящее время не полностью интуитивны, а некоторые задачи требуют обучения. Поэтому MR-устройства меньше подходят для повседневного использования и/или использования без обучения.

•Цена устройств MR всё ещё относительно высока, что препятствует масштабному развертыванию (например, в аудитории студентов) и делает их менее привлекательными, чем VR, с экономической точки зрения.

•Современные устройства MR также не обладают такими же графическими возможностями, как (потребительские) устройства VR, если только не выбрать устройство MR, привязанное кабелем к ПК, как Varjo XR-3. Но это ограничивает свободу движений пользователя и требует дополнительного оборудования при использовании.

•В настоящее время MR-устройства несколько громоздки и относительно хрупки. Для массового внедрения это должно быть существенно улучшено.

У смешанной реальности есть большой потенциал для использования в образовании и исследованиях. Различные эксперименты и области применения, которые уже были перечислены выше – это лишь небольшая часть.

Как и любая новая технология, её внедрение на начальном этапе сдерживается высокой стоимостью, отсутствием широкого распространения устройств и соответствующего опыта. Шлем смешанной реальности не является исключением. В настоящее время HoloLens 2 стоит около 3 500 долларов США, что примерно в десять раз превышает цену обычного устройства VR. Поэтому неудивительно, что Microsoft в настоящее время рекламирует HoloLens как «технологию смешанной реальности для бизнеса» [6]. Но технология имеет большой потенциал в областях, не связанных с бизнесом, таких как образование и исследования в различных областях. Виртуальная реальность на данный момент является более зрелой в плане технологий, приложений и внедрения.

Список используемых источников

1. Balendonck, 2019, Met een AR-bril de kas in. URL: https://www.wur.nl/nl/nieuws/Met- een-AR-bril-de-kas-in.htm (дата обращения: 29.03.2022).

2. Facebook’s Chief Scientist: Mass Adoption of AR Is Years Away. URL: https://www.theinformation.com/articles/facebooks-chief-scientist-mass-adoption-of-ar-is-years-away (дата обращения: 27.03.2022).

3. Geerse et al., 2020, Quantifying Spatiotemporal Gait Parameters with HoloLens in Healthy Adults and People with Parkinson's Disease, Sensors, volume 20, June 2020. URL: https://www.mdpi.com/1424-8220/20/11/3216 (дата обращения: 29.03.2022).

4. HoloLens, MSc Thesis, University of Utrecht. URL: http://dspace.library.uu.nl/handle/1874/363579 (дата обращения: 29.03.2022).

5. Klunder, 2018, Visualizing X-ray radiation levels with the Microsoft.

6. Microsoft HoloLens 2 For precise, efficient hands-free work. URL: https://www.microsoft.com/en-us/hololens (дата обращения: 25.03.2022).

УДК 004.056
ГРНТИ 81.93.29

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ТЕХНОЛОГИЙ ФОРМИРОВАНИЯ РАСПРЕДЕЛЕННЫХ РЕЕСТРОВ

А. В. Елфимов, Д. В. Кушнир

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Статья посвящена механизмам, лежащим в основе формирования распределенных реестров и, в частности, блокчейна и хешграфа. Основное внимание уделяется сравнительному анализу различных принципов достижения консенсуса в распределенном реестре и как они могут повлиять на возможность хранения и безопасности данных. Также в статье рассматривается влияние технологии построения распределенного реестра на область его применения.

блокчейн, направленный асинхронный граф, хеширование, хешграф.

В мире существует огромное количество систем так или иначе связанных с хранением данных. В большинстве своем такие системы являются централизованными. При централизованном хранении, в случае выхода из строя центрального узла, пострадают все звенья сети. Это в свою очередь приведет к издержкам, в том числе финансовым, так как вся сеть на некоторое время будет недоступна. Решение этого вопроса привело к системам резервирования, дублирования, т.е. хранения данных на многих устройствах, но в подавляющем числе случаев подразумевается единый центр контроля над такими системами. Возможность отказа от единого центра в системах управления данными привела к новым возможностям, и новый импульс – это направление получило с технологией блокчейн, которая стала широко известна недавно, когда Сатоши Накамото [1] представил миру как можно совместить технологию блокчейн и финансовую систему.

Блокчейн описывает цепочку блоков (числовых контейнеров), в которых может храниться информация самого разного вида: транзакции, контракты, документы о собственности [2–4]. Связь между блоками заключается в том, что вычисление хеша при формировании каждого блока использует в качестве части входных данных значение хеш-функции от заголовка предыдущего блока. Копии цепочек обычно хранятся на нескольких

устройствах и консенсус достигается необходимостью затрачивать значительные ресурсы на формирование блоков, что делает практически невозможным внесение изменений в уже внесённые данные. На рисунке 1 представлена структура блокчейна, связь каждого блока с предыдущим реализуется в заголовках блоков.

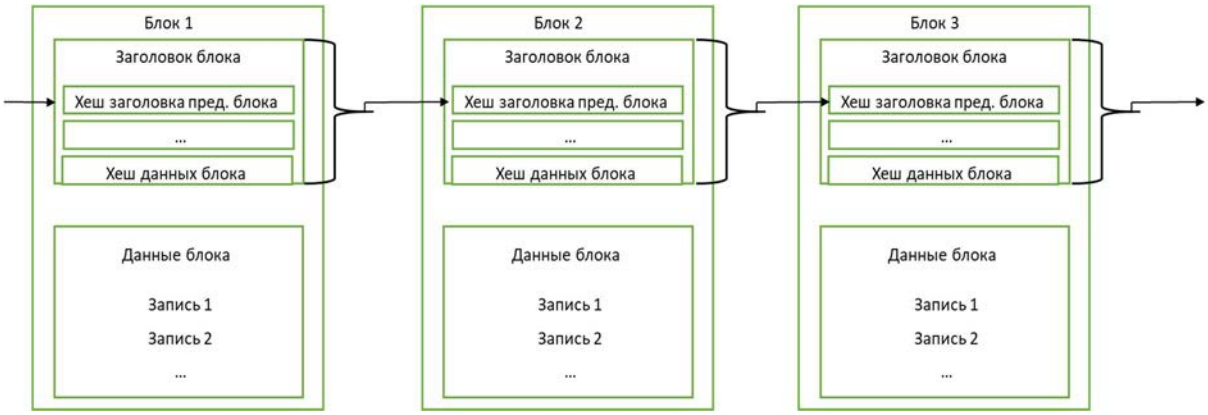


Рис. 1. Структура блокчейна

В различных реализациях распределенных реестров, и, в частности, основанных на блокчейне, существует возможность создавать контракты. Наиболее известным примеров такого решения являются смарт-контракты в системе Etherium. Смарт-контракты являются обычными контрактами, содержащими в себе набор функций и данных. Эта технология может применяться в сфере здравоохранения, где необходимо отследить цепочку перемещения лекарственных средств от завода до больницы. Смарт-контракты могут значительно ускорить традиционный документооборот, что позволяет сэкономить время и исключить любое вмешательство. Главным преимуществом применения блокчейна должна быть доступность и безопасность, так как эти факторы способствуют эффективности внедрения.

Помимо блокчейна, на сегодняшний день существуют другие разновидности распределенного реестра, такие как направленные асинхронные графы – DAG (*directed acyclic graph*) или Hashgraph [5]. Разработчики этих реестров попытались устранить недостатки блокчейна и увеличить производительность сети.

Направленный асинхронный граф является разновидностью технологии распределенного реестра, который отличается структурой записи и асинхронностью. В качестве блоков в DAG выступает уже сама информация (транзакция, запись)

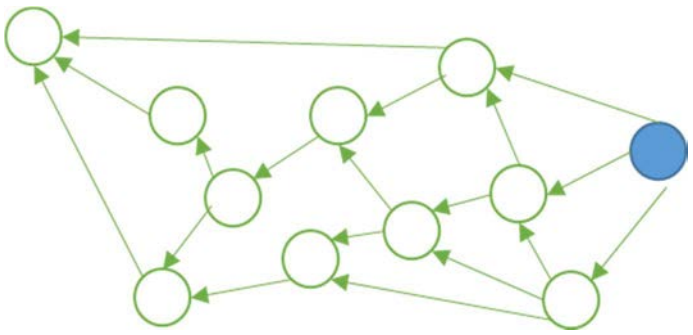


Рис. 2. Структура DAG

и хеш предыдущей информации. На рис. 2 представлена структура асинхронного графа.

Структура асинхронного графа построена на частичном порядке, связь можно описать как иерархию родитель-ребенок. Если любые данные могут быть достигнуты переходами по ссылкам «родитель-ребёнок», то можно отследить порядок в цепочке.

Чтобы разрешить неоднозначность, полагаются на так называемых провайдеров порядка. Их задачей является отправка данных в сеть с соблюдением порядка. Провайдеры порядка – это доверенные пользователи, и вся сеть полагается на то, что эти провайдеры не будут нарушать правила порядка.

Если рассматривать с финансовой точки зрения, то в случае, если имеется возможность установить порядок между двумя переводами, тратящими одну и ту же монету (по связям родитель-ребёнок), то все ноды сразу отклоняют такую попытку двойной траты.

К достоинствам DAG можно отнести высокую скорость обработки данных, небольшие требования по производительности узлов для записи данных в реестр, возможность достижения цензуроустойчивости и масштабируемость, которая достигается из-за отсутствия единой точки записи данных. Можно отметить и недостатки, например, наличие большого трафика в начале работы сети. Незначительное количество недостатков связано с новизной технологии. Однако уже есть решения, основанные на асинхронных направленных графах. Одним из наиболее известных решений является система IOTA. Разработчики взяли эту технологию с целью пересмотра блокчейна и обеспечения применимости технологий распределенного реестра в IoT (*Internet of Things*) [6].

Еще одним типом распределенного реестра является хешграф (*hashgraph*) [7]. За основу нового типа достижения консенсуса был взят DAG и информация в этой технологии записывается в распределенный реестр нелинейно.

В хешграфе консенсус достигается получением единого набора предков для интересующего события за счет обмена информацией о событиях по протоколу Gossip, а взаимосвязь реализуется включением в информацию о событиях двух хешей предыдущих событий. Такое построение распределенного реестра не требует больших объемов передаваемых данных и обеспечивают большие скорости обмена.

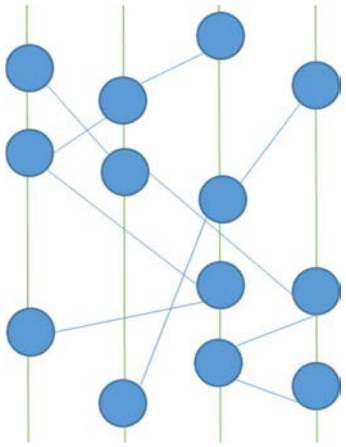


Рис. 3. Структура хешграфа

Работу хешграфа можно описать следующим образом (рис. 3):

● Информация о транзакции отправляется двум случайным узлам, которые, в свою очередь, передают их другим двум узлам – и так далее, экспоненциально увеличивая охват, пока не наберется нужное количество проинформированных нод, которых будет достаточно для верификации транзакции.

● Транзакции записываются в хронологическом порядке – можно отследить их историю.

● Система является устойчивой к действиям мошеннических нод, если их количество не превышает трети от всех участников.

К преимуществам хешграфа можно отнести большую скорость обработки транзакция, устойчивость к распределенным атакам, эффективное достижение консенсуса и меньшее влияние производительности отдельных узлов на запись данных в реестр.

Хешграф является относительно недавней разработкой и его исследования продолжаются. Активное использованиие на данный момент является проблематичным, так как технология является запатентованной, но предполагается предоставление возможности использования для всех в ближайшем будущем.

Сферы применения распределенных реестров весьма широки. Одной из возможностей является их применение для обеспечения безопасности IoT-устройств. Самой главной угрозой для IoT является DDOS-атаки. Незащищенные устройства становятся легкой мишенью для взлома и проведения атаки киберпреступнику. Распределение обработки транзакций и событий поможет сделать распределенные атаки малоэффективными. Так как в рассматриваемых системах распределенный реестр защищен от несанкционированного изменения, это обеспечивает доверие и прозрачности хранимой в нем информации. Однако стоит отметить, что проблема масштабируемости актуальна как для блокчейна, так и для IoT-устройств, хешграф сможет помочь в обеспечении безопасности и масштабируемости хранения данных.

Также хешграф имеет преимущества перед блокчейном по алгоритму консенсуса. Так в блокчейне майнер – главное лицо, который решает включать эту транзакцию в блок или нет, что приводит к некоторой централизации. Хешграф реализует подход, в котором валидаторы обязаны включить все транзакции и обработать их. Однако, несмотря на свои недостатки, в настоящее время, наиболее исследованной технологией остается именно блокчейн и для текущих проектов он является предпочтительным для большинства решений [8, 9]. Дальнейшие исследования новых видов распределенного реестра позволит приблизить их внедрение и приведет к реализации их потенциальных преимуществ.

Список используемых источников

1. Табернакулов А., Койфманн Я. Блокчейн на практике. Москва : Альпина Паблишер, 2019. 257 с.
2. Лелу Л. Блокчейн от А до Я : все о технологии десятилетия / пер. с фр. А. Н. Степановой с предисловием Уильяма Могайара. Москва : Бомбора : Эксмо, 2018. 248 с.
3. Могайар, Уильям. Блокчейн для бизнеса / предисл. Виталика Бутерина ; [пер. с англ. Д. Шалаевой]. Москва : Издательство «Эксмо», 2018. 224 с.
4. Винья П., Кейси М. Машина правды : блокчейн и будущее человечества / перевод с английского Марии Сухотиной. Москва : Манн, Иванов и Фербер, 2018. 317 с.
5. Атака 51 %: как она устроена и чем опасна – 2021. URL: https://media.sigen.pro/materials/6466/ (дата обращения: 21.12.2021).
6. Nothing-at-Stake Problem. URL: https://smithandcrown.com/glossary/nothing-stake-problem/ (дата обращения: 21.12.2021).
7. Что такое консенсус отложенного времени PoET. URL: https://crypto-fox.ru/faq/algoritm-konsensusa-poet/ (дата обращения: 21.12.2021).
8. Hedera: A Public Hashgraph. Network & Governing Council. URL: https://hedera.com/hh_whitepaper_v2.1-20200815.pdf (дата обращения: 22.12.2021).
9. От блокчейна к DAG: избавляемся от посредников – 2019. URL: https://habr.com/ru/company/obyte/blog/477032/ (дата обращения: 22.12.2021).

УДК 004.77
ГРНТИ 49.38.99

ИНДУСТРИЯ 4.0 ДЛЯ ЭЛЕКТРОННОГО ЗДРАВООХРАНЕНИЯ

Д. В. Ермоленко, К. Х. Киличева, А. С. А. Мутханна

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича

Подход eHealth 4.0 вынесен из хорошо известной индустрии 4.0 или так называемой четвертой промышленной революции. Ее основная цель произвести скачок в производственном секторе путем оцифровки. Будущее управление здравоохранением станет более своевременным и персонализированным, поскольку новые технологии позволят отдельным лицам осуществлять мониторинг своего здоровья с помощью кибер физических систем. Принципы проектирования индустрии 4.0 соединяют физический и виртуальный мир в режиме реального времени. Для этого мобильная сеть следующего поколения 5G обеспечит интеллектуальную среду для организации медицинских услуг, чтобы государственные и частные компании могли пересмотреть свои перспективы и методы. Технологические разработки в области больших данных и индустрии 4.0 по отдельности привлекают огромное внимание ученых и отраслей промышленности. Тем не менее, подробное исследование больших данных, касающихся здравоохранения, все еще отсутствуют в имеющейся литературе. В статье излагается новый подход к достижению эффективных показателей, связанных с выявленными исследовательскими проблемами.

eHeath, Индустрия 4.0, 5G, IoT, блокчейн, облачные вычисления.

Введение

Технический прогресс оказывает значительный вклад практически во все сегменты человеческой жизни. Современные системы производства, интеллектуальные сети, вкупе со сферой здравоохранения [1], науки, городского траффика и транспорта, безусловно, упрощают нашу жизнь. Индустрия 4.0, или четвёртая промышленная революция, описывает трансформацию и эволюцию промышленного производства за счет оцифровки новых технологий. Концепция промышленной революции изменялась в течение нескольких десятилетий. Сейчас благодаря Индустрии 4.0 на свет появилось новое измерение, где с помощью новых систем промышленный рынок вышел на совершенно иной уровень, подобного которому раньше не существовало. Идея промышленного интернета была обозначена в 2012 году в купе с Big Data [2] и Интернетом вещей (IoT). Аналитики подсчитали, что порядка 45 % всей экономики мира смогли бы получить выгоду из промышленного Интернета.

Этапы промышленной революции

Промышленную революцию можно разделить на четыре этапа. Первая промышленная революция, известная как Индустрия 1.0, началась в конце 1800-х годов и включала ручное использование механических инструментов, в основном в легкой промышленности. Центральной моделью второй революции была электрификация, которая позволила наладить массовое производство. Третья революция характеризовалась цифровизацией за счет использования микроэлектроники и автоматизации, благодаря чему стало возможным гибкое производство. Программируемые машины, такие как сетевые компьютеры (NCS) и программируемые логические контроллеры (PLCs) использовались для производства многих продуктов. Четвертая и нынешняя революция является самой значимой, так как состоит из систем и полезных технологических методов, таких как IoT, анализ больших данных (BDA), облачные вычисления, блокчейн и искусственный интеллект (ИИ). На рис. показаны составные части будущего здравоохранения.

Тенденции рынка, а также научная литература свидетельствуют о роли здравоохранения [3] в качестве движущей силы основных столпов, поддерживающих концепцию I4.0. Действительно, IoT используется для дистанционного мониторинга во всех его аспектах, что позволяет осуществлять медицинское обслуживание в различных условиях, начиная от долгосрочного ухода за пожилыми людьми и наблюдения на дому до систем неотложной медицинской реабилитации. Поскольку эти установки производят все боль-

шие и большие объемы самых разнообразных данных, обеспечивая высокоскоростной захват, обнаружение и анализ, для извлечения из них ценности требуются технологии и архитектуры больших данных нового поколения. Это еще больше подталкивает к переходу на облачные архитектуры, необходимые для безопасной и надежной обработки требований как к обработке, так и к хранению для анализа этих больших объемов данных.

Рисунок. Обзор ключевых качеств Здравоохранения 4.0

Мониторинг физиологических и патологических сигналов

Парадигма интернета вещей, поддерживаемая прогрессом, достигнутым в технологиях мобильной связи, а также в носимых устройствах и сенсорных устройствах, наряду с доступностью облачных и облачных ресурсов по требованию и технологий больших данных, способна обеспечить ценную основу для поддержки приложений повсеместного мониторинга. Полученная в результате структура поддерживает сбор медицинских записей, потенциально обеспечивая генерацию статистической информации, связанной с состоянием здоровья, и предоставление новых типов облачных сервисов, способных заменить или дополнить существующие информационные системы больниц. Такого рода автоматизированные подходы гарантируют

значительное снижение риска возникновения ошибок по сравнению с методами, требующими ручного вмешательства. Системы дистанционного мониторинга пациентов состоят из трех основных компонентов: 1) аппаратное обеспечение для зондирования и сбора данных для сбора физиологических и двигательных данных; 2) коммуникационное оборудование и программное обеспечение для передачи данных в удаленный центр; 3) методы анализа данных для извлечения клинически значимой информации из физиологических данных и данных о движении. Внедрение передовых медицинских и экологических датчиков, таких как акселерометры и гироскопы, датчики температуры и влажности, а также датчики ЭКГ, глюкозы и давления позволяют постоянно контролируйте физиологическое и физическое состояние пациентов. Устройства интернета вещей могут передавать эти данные в удаленные центры обработки данных, где может быть выполнена интеграция данных для использования, казалось бы, бесконечного хранилища, масштабируемых возможностей обработки, а также высокой доступности услуг, предоставляемых облаком.

Самоуправление, мониторинг состояния здоровья и профилактика

Индустрия 4.0 поддерживает конкретные решения для самостоятельного управления. Ясно, что технологии больших данных позволяют осуществить переход от лечения к профилактике, что также является одной из особенностей, определяемых медициной. Исследователи выяснили, как создавать интеллектуальные сервисы, выходящие за рамки простых функций, таких как отображение измеренных данных и временное хранение данных, но способных обеспечивать эффективную обратную связь для отдельных лиц. Например, эти решения могут реализовывать алгоритмы, помогающие предотвращать заболевания путем выявления модифицируемых факторов риска и разработки мероприятий по изменению поведения в отношении здоровья. Лечение хронических заболеваний является еще одним из наиболее важных примеров такого самоуправления в интересах здоровья. Например, рассматривая лечение и профилактику диабета и ожирения, эти системы способны предлагать рекомендации по обучению и расширению возможностей для правильного питания и планировать фитнес-программы.

Реабилитация

В соответствии с оказанием медицинской помощи, реабилитация на дому, как ожидается, принесет значительную экономию средств для систем здравоохранения и улучшит качество жизни пациентов. Аналогичным образом, технологии позволят обнаруживать и отслеживать перемещения людей, связанных с реабилитационной практикой. В отличие от обычных решений для жизни с помощью вспомогательных средств, реабилитация на

дому характеризуется рядом специфических ограничений и требований, а также связанными с ними решениями, включающими объединение данных с несколькими датчиками в режиме реального времени и обратная связь для пациентов, интегрируемая в виртуальную реальность. Ключевая функция, связана с биологической обратной связью: измерение физиологической активности и других параметров, передаваемых самим пользователям. Эта практика эффективно позволяет пациенту контролировать и изменять свою активность с конечной целью улучшения своего здоровья и работоспособности.

Заключение

Четвёртая промышленная революция привела к совершенно новым идеям и изменениям в подходах для каждой отрасли, аналогично предыдущим промышленным революциям. Парадигма Индустрии 4.0 породила инновационные подходы, открыв новые пути развития сектора здравоохранения. Различные технологии, такие как IoT, BDA, блокчейн, искусственный интеллект и облачные вычисления, позволили осуществить значительные изменения и способствовали развитию здравоохранения [4]. Путем анализа и исследования соответствующей литературы, мы узнали и обсудили подходы и применение этих новых методов с точки зрения развития отрасли. С появлением Индустрии 4.0 и новых технологий, которые стали доступны с ее помощью, модели каждой отрасли меняются и совершенствуются.

Список используемых источников

1. Industry 4.0 Applications for Medical/Healthcare Services - Shuva Paul, Muhtasim Riffat, Abrar Yasir, Mir Nusrat Mahim, Bushra Yasmin Sharnali, Intisar Tahmid Naheen, Akhlaqur Rahman, Ambarish Kulkarni. DOI: 10.3390/jsan10030043.

2. Industry 4.0 and Health: Internet of Things, Big Data, and Cloud Computing for Healthcare 4.0 – Giuseppe Aceto, Valerio Persico, and Antonio Pescape. DOI: 10.1016/j.jii.2020.100129

3. A Business Model of Russian E-Health Based on Process Integration of Industry 4.0: The Development of Indicators for Information Communication – Aleksandra Butneva.

4. What Is eHealth (4): A Scoping Exercise to Map the Field - Claudia Pagliari, David Sloan, Peter Gregor, Frank Sullivan, Don Detmer, James P Kahan, Wija Oortwijn, Steve MacGillivray. DOI: 10.2196/jmir.7.1.e9

УДК 004.51
ГРНТИ 81.93.29

МЕТОДЫ ОЦЕНКИ ЗАЩИЩЁННОСТИ ЧЕЛОВЕКО-КОМПЬЮТЕРНЫХ ИНТЕРФЕЙСОВ ДЛЯ ПРИЛОЖЕНИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

К. Н. Жернова

Санкт-Петербургский Федеральный исследовательский центр Российской академии наук

Для информационной безопасности разрабатываются приложения с использованием современных типов интерфейсов, таких как сенсорные экраны и виртуальная реальность. Однако новые типы интерфейсов также не лишены уязвимостей, посредством которых можно осуществлять атаки на чувствительные данные пользователей приложений. Кроме того, эти уязвимости малоизучены, поэтому требуется оценка их критичности. Уязвимости интерфейсов отличаются от уязвимостей компьютерной сети, по этой причине требуется вводить новые параметры для уязвимостей и модифицировать существующие. В данном докладе предлагаются методы оценки защищённости интерфейсов для приложений информационной безопасности на основе сенсорных экранов и виртуальной реальности.

человеко-машинное взаимодействие, информационная безопасность, оценка защищённости, пользовательские интерфейсы, визуализация данных, сенсорные экраны, виртуальная реальность.

Введение

Для работы с интерфейсами приложений информационной и компьютерной безопасности используются различные средства визуализации обрабатываемых данных. Также в области визуальной аналитики информационной безопасности применяются различные способы оценки визуальных интерфейсов для того, чтобы оценить эффективность работы оператора с этими визуальными интерфейсами [1]. Однако оценке защищённости взаимодействия оператора с интерфейсами посвящено очень малое количество работ.

Для повышения защищённости работы оператора с человеко-компьютерными интерфейсами приложений информационной безопасности разработана система оценки защищённости интерфейсов человеко-компьютерного взаимодействия на основе виртуальной реальности и сенсорных экранов. Оценка защищённости интерфейса состоит из двух частей: (1) оценка каждой имеющейся уязвимости и (2) оценка суммарного влияния всех имеющихся уязвимостей на систему.

Оценка защищённости человеко-компьютерного интерфейса

Оценка защищённости интерфейса заключается в: (1) оценке каждой отдельной уязвимости системы и (2) суммарной оценке уязвимости всей системы.

1. Оценка каждой имеющейся уязвимости. Традиционно для базовой оценки критичности уязвимости используются следующие параметры: (1) вектор атаки, (2) сложность атаки, (3) требуемые привилегии, (4) взаимодействие пользователя, (5) ущерб конфиденциальности, (6) ущерб целостности, (7) ущерб доступности. Однако в случае человеко-компьютерного взаимодействия, вектор атаки всегда будет физический, по этой причине он не задействуется при оценке уязвимости интерфейсов. Также был добавлен параметр «ущерб оператору», так как возможны атаки интерфейс, провоцирующие временное ухудшение физического состояния оператора [2, 3]. При расчёте распределение уровня влияния уязвимости на систему в соответствии с полученными результатами следующее [4]:

1) низкий уровень – от 1 до 3 баллов включительно;
2) средний уровень – от 4 до 6 баллов включительно;
3) высокий уровень – от 7 до 8 баллов включительно;
4) критический уровень – от 9 до 10 баллов включительно.

2. Оценка суммарного влияния всех имеющихся уязвимостей на систему проводится по следующему принципу. Каждому элементу интерфейса присваивается значение уровня уязвимости: высокий, средний, низкий, защищённый. Если хотя бы один элемент обладает значением «критический», то уровень уязвимости всей системы считается критическим. Если хотя бы один элемент обладает значением «высокий», то уровень уязвимости всей системы считается высоким. Если хотя бы один элемент обладает значением «средний», то уровень уязвимости всей системы считается средним. Если больше одного элемента обладают значением «средний», то уровень уязвимости всей системы считается высоким. Если хотя бы один элемент обладает значением «низкий», в то время как остальные защищены, то уровень уязвимости всей системы считается низким. Если больше одного элемента обладают значением «низкий», то уровень уязвимости всей системы считается средним.

Интерфейс системы оценки защищённости

Пример интерфейса для оценки влияния уязвимости на систему приведен на рис. 1. Данный интерфейс представляет собой панель с кнопками для выбора значений параметров уязвимости. При нажатии на кнопку «Рассчитать» программный алгоритм вычисляет уровень критичности конкретной уязвимости.

На рисунке представлен результат расчёта для набора входных параметров: (1) Конфиденциальность – Нет ущерба; (2) Целостность – Высокий;

(3) Доступность – Высокий; (4) Урон оператору – Низкий; (5) Сложность применения – Высокая; (6) Требуемые привилегии – Высокие; (7) Взаимодействие – Нет (Аудио). Значение возможного ущерба равно 6.2 и входит в диапазон значений для среднего уровня критичности уязвимости.

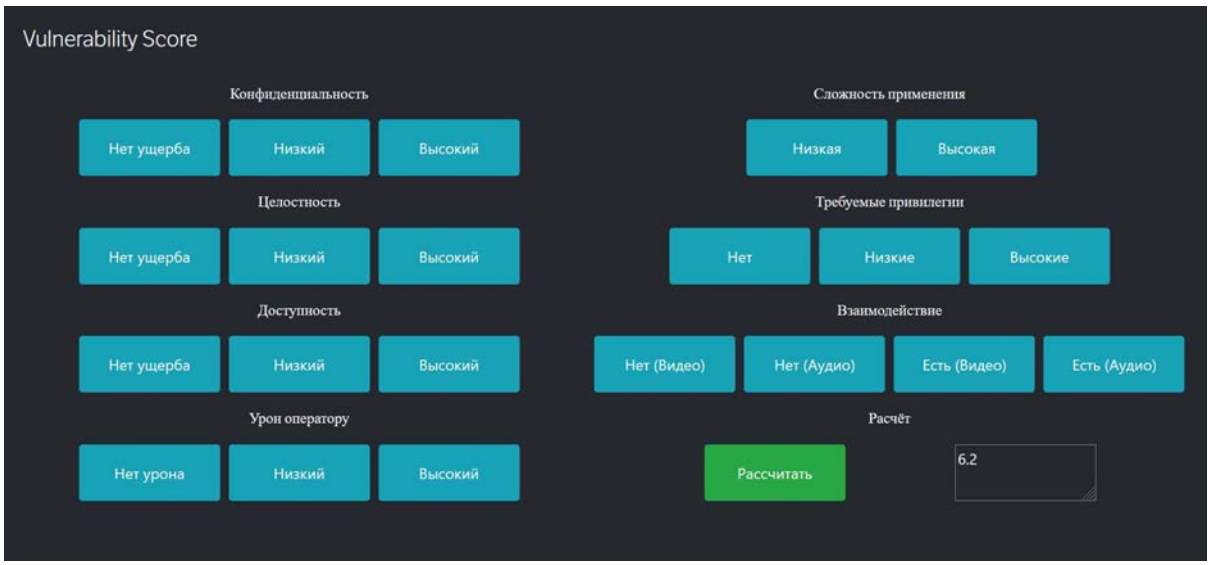


Рис. 1. Интерфейс для оценки возможного ущерба от уязвимости

Пример интерфейса для оценки суммарного влияния всех имеющихся уязвимостей на систему приведен на рис. 2.

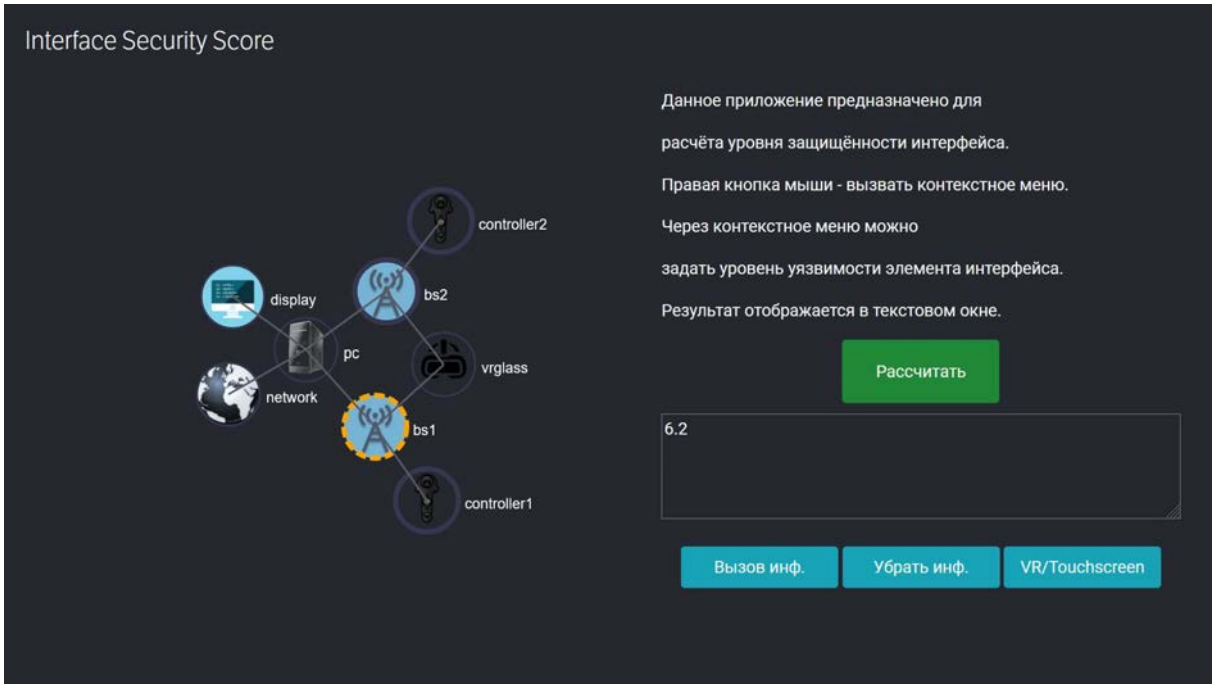


Рис. 2. Внешний вид графического интерфейса системы оценки защищённости интерфейса виртуальной реальности

Интерфейс содержит графовую модель оцениваемого интерфейса (на рисунке представлена модель интерфейса на основе виртуальной реальности) и панель управления для расчёта уровня защищённости интерфейса. При нажатии на кнопку «Рассчитать» программный алгоритм вычисляет уровень защищённости системы. С помощью кнопок «Вызов инф.» и «Убрать инф.» можно вызвать или убрать дополнительную информацию об элементах оцениваемого интерфейса. Кнопка «VR/Touchscreen» позволяет переключаться между типами человеко-компьютерных интерфейсов: виртуальная реальность и сенсорные экраны.

Выводы

В данной работе представлена система оценки защищённости интерфейсов человеко-компьютерного взаимодействия, реализованных на основе виртуальной реальности и сенсорных экранов. Данная система оценки позволит оценивать интерфейсы информационной и компьютерной безопасности, что позволит повысить защищённость взаимодействия оператора с приложениями информационной безопасности при разработки таких приложений.

Работа выполнена при финансовой поддержке РФФИ (проект 20-37-90130 Аспиранты).

Список используемых источников

1. Котенко И. В. и др. Визуальная аналитика для информационной безопасности: оценка эффективности и анализ методов визуализации // Вопросы кибербезопасности. 2021. №. 6 (46). С. 36–46.

2. Sproul J., Ledger S., MacCallum J. A review of digital media guidelines for students with visual light sensitivity // International Journal of Disability, Development and Education. 2021. Т. 68. №. 2. С. 222–239.

3. South L., Saffo D., Borkin M. A. Detecting and Defending Against Seizure-Inducing GIFs in Social Media // Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems. 2021. С. 1–17.

4. Dodiya B., Singh U. K., Gupta V. Trend Analysis of the CVE Classes Across CVSS Metrics // International Journal of Computer Applications. 2021. Т. 975. С. 8887.

Статья представлена научным руководителем,
кандидатом технических наук, доцентом А. А. Чечулиным.

УДК 004.51
ГРНТИ 81.93.29

КОНЦЕПТУАЛЬНАЯ МОДЕЛЬ ИНТЕРФЕЙСА ВЗАИМОДЕЙСТВИЯ «СИСТЕМА – ОПЕРАТОР», ОСНОВАННОГО НА ТЕХНОЛОГИЯХ ВИЗУАЛИЗАЦИИ, УЧИТЫВАЮЩИХ КОГНИТИВНЫЙ АППАРАТ ЧЕЛОВЕКА

К. Н. Жернова, К. Е. Израилов,
М. В. Коломеец, Д. С. Левшун, А. А. Чечулин

Санкт-Петербургский Федеральный исследовательский центр Российской академии наук"

Для того чтобы определить возможные способы взаимодействия системы беспилотной транспортной среды и оператора, требуется разработать концептуальную модель данного взаимодействия. В докладе представлена концептуальная модель интерфейса взаимодействия «система – оператор», основанного на технологиях визуализации. Данная концептуальная модель учитывает уязвимости когнитивного аппарата человека, которые могут помешать правильно воспринимать информацию, предоставляемую системой оператору. Концептуальная модель показывает способы передачи визуальной информации от системы к оператору, а также зависимость качества восприятия информации оператором от способа визуализации данных.

человеко-машинное взаимодействие, информационная безопасность, пользовательские интерфейсы, визуализация данных, машинное зрение.

Введение

Оператор может взаимодействовать с интерфейсами беспилотной транспортной среды различными способами. Однако для повышения качества интерфейса необходимо определить эти способы взаимодействия и выбрать наиболее эффективные. Качество взаимодействия оператора с системой зависит от правильного подбора моделей визуализации для отображения данных системы.

Для определения способов взаимодействия оператора с интерфейсами беспилотной транспортной среды была разработана концептуальная модель взаимодействия оператора с системой. Данная концептуальная модель описывает взаимодействие оператора с интерфейсом беспилотной транспортной среды, который состоит из двух основных компонентов: (1) визуализация и (2) управление. Также модель учитывает когнитивный аппарат

оператора, который также включает в себя две составляющие: (1) восприятие данных оператором и (2) обработку оператором этих данных для последующего принятия решений.

Описание концептуальной модели

В целях описания взаимодействия системы беспилотной транспортной среды с оператором была разработана концептуальная модель взаимодействия интерфейса и оператора. Данная концептуальная модель приведена на рисунке.

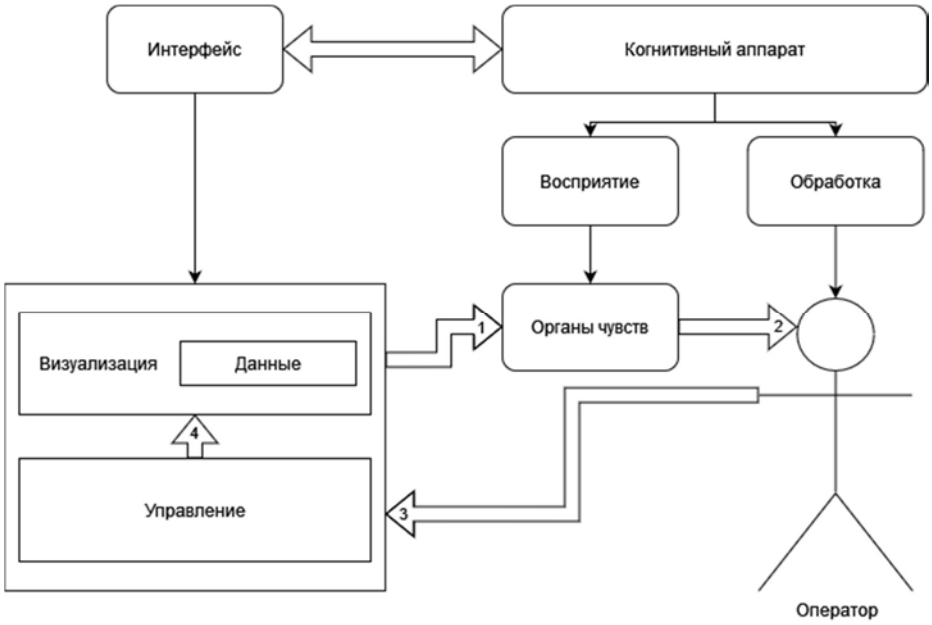


Рисунок. Схема концептуальной модели взаимодействия внутри интерфейса «система-оператор»

Данная концептуальная модель включает в себя четыре потока взаимодействия оператора с системой, которые представляют собой замкнутую петлю.

1. Визуализация → органы чувств человека. Данные, отображаемые на визуализации, воспринимаются оператором через зрительный канал восприятия.

2. Органы чувств человека → мозг человека. На данном этапе происходит обработка и трактовка оператором полученных данных.

3. Оператор → управление визуализацией. После обработки данных оператор принимает решение и взаимодействует с визуализацией с целью управления данными визуализации.

4. Управление визуализацией → визуализация. Модель визуализации отображает все внесённые изменения.

Как видно из описания модели, данная концептуальная модель учитывает когнитивный аппарат человека, который включает в себя восприятие

данных, отображаемых на визуализации, и обработку этих данных человеком. Таким образом, происходит обмен данными между интерфейсом системы и когнитивным аппаратом человека.

Визуализация данных в концептуальной модели

Для концептуальной модели были рассмотрены различные модели визуализации [1]. С их помощью могут отображаться количественные показатели (для отображения количества чего-либо) и категориальные показатели (отображается принадлежность к какой-либо группе, связи между элементами группы и т. д.). Для визуализации количественных показателей необходимо применять графики с высокой точностью восприятия пользователем. Для отображения категориальных показателей можно использовать графики, допускающие погрешности.

На основе исследований [2, 3] был сделан вывод о целесообразности применения тех или иных моделей визуализации для отображения каждой группы показателей (количественные или категориальные). Таким образом, было получено три группы моделей визуализации.

1. В случае необходимости отображения количественных показателей следует применять тепловые карты, простейшие графики, матрицы, параллельные координаты, графы, хордовые диаграммы, карты, так как они обладают достаточно высокой точностью.

2. Для визуализации категориальных показателей следует подбирать облака слов, простейшие графики, графики рассеивания, параллельные координаты, карты деревьев, графы, карты вороного, хордовые диаграммы.

3. В случаях, когда важны показатели как количественные, так и категориальные, можно выбирать простейшие графики, параллельные координаты, графы, хордовые диаграммы.

Выводы

В данной работе описана разработанная концептуальная модель взаимодействия оператора с визуальным интерфейсом беспилотной транспортной среды. Данная концептуальная модель учитывает когнитивный аппарат человека, посредством которого оператор воспринимает и обрабатывает полученную информацию, а также принимает решения на основе этих данных. Были также рассмотрены различные модели визуализации, возможность применения которых зависит не только от поставленной задачи, но и от эффективности восприятия оператором этих моделей визуализации. Таким образом, предложенная модель позволит повысить качество интерфейса путём подбора визуализаций, учитывающих восприятие оператора.

Работа выполнена при финансовой поддержке РФФИ (проект 19-29-06099 мк).

Список используемых источников

1. Котенко И. В., Коломеец М. В., Жернова К. Н., Чечулин А. А. Визуальная аналитика для информационной безопасности: оценка эффективности и анализ методов визуализации // Вопросы кибербезопасности. 2021. № 6 (46). С. 36–46.

2. Cleveland W. S., McGill R. Graphical perception: Theory, experimentation, and application to the development of graphical methods //Journal of the American statistical association. 1984. Vol. 79. №. 387. pp. 531–554.

3. Heer J., Bostock M., Ogievetsky V. A tour through the visualization zoo //Communications of the ACM. 2010. Vol. 53. №. 6. pp. 59–67.

УДК 004.51
ГРНТИ 81.93.29

УЯЗВИМОСТИ ВИЗУАЛЬНЫХ ИНТЕРФЕЙСОВ «СИСТЕМА – ОПЕРАТОР» В БЕСПИЛОТНОЙ ТРАНСПОРТНОЙ СРЕДЕ

К. Н. Жернова, М. В. Коломеец

Санкт-Петербургский Федеральный исследовательский центр Российской академии наук

Несмотря на то, что транспортная среда умного города является беспилотной, а значит, отчасти автономной, окончательные решения по части информационной и компьютерной безопасности принимает человек. Оператор должен вовремя реагировать на возникающие события безопасности и угрозы. Однако восприятие оператора само по себе обладает рядом уязвимостей, от которых оператора требуется защитить. В данном докладе представлено краткое описание интерфейса «система – оператор» беспилотной транспортной среды, описаны схемы взаимодействия системы с оператором со стороны системы, также доклад даёт описание основным уязвимостям интерфейса и атакам, в которых могут быть задействованы эти уязвимости.

человеко-машинное взаимодействие, информационная безопасность, пользовательские интерфейсы, визуализация данных, машинное зрение.

Введение

В настоящее время исследователи открывают всё большее количество уязвимостей, угрожающих работе оператора с данными компьютерных сетей, в том числе сети инфраструктуры беспилотной транспортной среды «умного города». Однако, взаимодействие оператора с интерфейсами беспилотной транспортной среды само по себе может находиться под угрозой.

Для повышения защищённости взаимодействия оператора с интерфейсами беспилотной транспортной среды требуется повышать уровень осведомленности операторов и разработчиков данных интерфейсов об уязвимостях, характерных для визуальных интерфейсов. С этой целью в данной работе рассматриваются три основных группы уязвимостей визуальных интерфейсов и приводятся примеры атак, использующих эти уязвимости.

Интерфейс «система – оператор» беспилотной транспортной среды

Взаимодействие оператора с компьютерной системой беспилотной транспортной среды представляет собой кольцо обмена данными между оператором и системой. Схема взаимодействия представлена на рисунке.

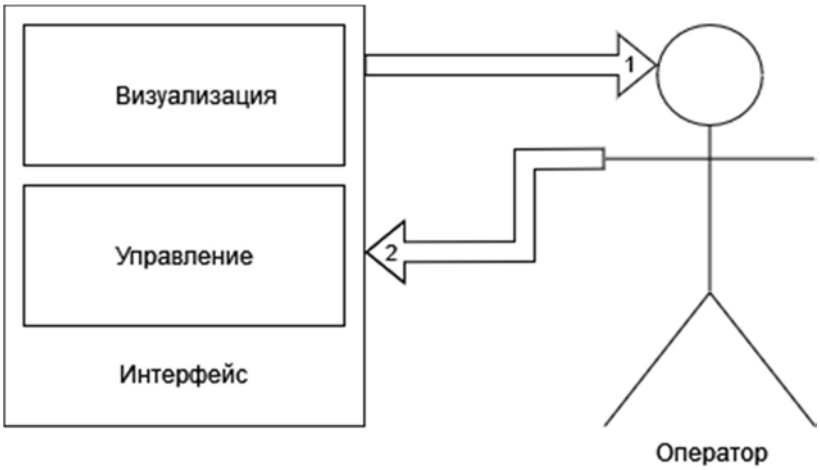


Рисунок. Схема взаимодействия оператора и системы беспилотной транспортной среды

Кольцо взаимодействия оператора и системы составляют два потока данных: (1) поток данных от интерфейса к оператору и (2) поток данных от оператора к интерфейсу системы. Со стороны системы, интерфейс передаёт данные оператору посредством визуализации обрабатываемых данных. Оператор передаёт данные системе посредством компонента управления интерфейсом.

Уязвимости интерфейсов беспилотной транспортной среды

Поскольку кольцо взаимодействия состоит из трёх основных компонентов (интерфейс, оператор и процесс взаимодействия между ними), уязвимости беспилотной транспортной среды также разделяются на три группы, представленные ниже.

(1) Уязвимости системы. Данная группа включает в себя уязвимости, которым может быть подвержена компьютерная система беспилотной транспортной среды. В эту группу могут входить уязвимости сети, с помощью которых злоумышленник может атаковать компьютерную систему [1].

(2) Уязвимости оператора. В данную группу входят особенности человеческого организма, которыми может воспользоваться злоумышленник для того, чтобы вызвать у оператора усталость, раздражение, временное ухудшение физического состояния и т.п. с целью, чтобы оператор допускал ошибки при взаимодействии с интерфейсом. Примерами атак, задействующих данную группу уязвимости, могут служить изменение частоты излучения дисплея, которое может повлиять на самочувствие людей с повышенной чувствительностью к свету [2] и появление ярких раздражающих изображений на экране [3].

(3) Уязвимости взаимодействия системы и оператора. Данный тип уязвимостей может понизить эффективность процесса взаимодействия оператора с системой. Поскольку данная работа сфокусирована на визуальных интерфейсах беспилотной транспортной среды, то под взаимодействием оператора и системы понимается взаимодействие оператора с визуализацией данных системы. Таким образом, в данную группу входят уязвимости при восприятии оператором данных визуализации, а также уязвимости, связанные с управлением визуализацией. Например, с помощью подбора соответствующей визуализации злоумышленник может спровоцировать ошибку восприятия, при которой данные могут быть неверно интерпретированы [4]. Данная ошибка восприятия может быть вызвана тем, что графические примитивы, использующиеся при построении визуализации, неправильно нормализованы [5].

Выводы

В данной работе описаны основные типы уязвимостей визуальных интерфейсов взаимодействия между оператором и системой беспилотной транспортной среды, а также приведены примеры некоторых возможных атак, эксплуатирующих данные типы уязвимостей. Приведённая классификация позволит повысить уровень защищённости визуальных интерфейсов беспилотной транспортной среды посредством повышения осведомленности оператора и разработчиков о возможных уязвимостях данного типа интерфейсов.

Работа выполнена при финансовой поддержке РФФИ (проект 19-29-06099 мк).

Список используемых источников

1. Kolomeets M., Zhernova K., Chechulin A. Unmanned transport environment threats // Proceedings of 15th International Conference on Electromechanics and Robotics" Zavalishin's Readings". Springer, Singapore, 2021. pp. 395–408.

2. Sproul J., Ledger S., MacCallum J. A review of digital media guidelines for students with visual light sensitivity // International Journal of Disability, Development and Education. 2021. V. 68. N. 2. pp. 222–239.

3. South L., Saffo D., Borkin M. A. Detecting and Defending Against Seizure-Inducing GIFs in Social Media // Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems. 2021. pp. 1–17.

4. Angelini M., May T., Santucci G., Schulz HJ. On Quality Indicators for Progressive Visual Analytics // EuroVA@ EuroVis. 2019. pp. 25–29.

5. Котенко И. В. и др. Визуальная аналитика для информационной безопасности: области применения, задачи и модели визуализации // Вопросы кибербезопасности. 2021. №. 4 (44). С. 2–15.

Статья представлена научным руководителем,
кандидатом технических наук, доцентом Чечулиным А. А.

УДК 004.51
ГРНТИ 81.93.29

МЕТОДЫ ОЦЕНКИ КАЧЕСТВА ЧЕЛОВЕКО-КОМПЬЮТЕРНЫХ ИНТЕРФЕЙСОВ ДЛЯ ПРИЛОЖЕНИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ОСНОВЕ СЕНСОРНЫХ ЭКРАНОВ

К. Н. Жернова, А. А. Чечулин

Санкт-Петербургский Федеральный исследовательский центр Российской академии наук

Для того чтобы оператор мог своевременно реагировать на события сетевой безопасности и принимать адекватные решения, нужна эффективная модель компьютерной сети, совмещённая с технологиями сенсорных экранов. Чтобы оценить эффективность такой модели, нужно измерить её качество. Основными параметрами модели, по которым можно судить о том, насколько успешна разработка модели, являются качество, эффективность и результативность. Данная работа посвящена оценке эффективности работы оператора с моделью компьютерной сети с использованием интерфейсов на основе сенсорного экрана. В докладе кратко рассматриваются способы оценки качества и эффективности модели, подходящие для оценки разработанной модели компьютерной сети.

человеко-машинное взаимодействие, информационная безопасность, пользовательские интерфейсы, сенсорные экраны, оценка качества.

Введение

Существует множество методов оценки человеко-компьютерных интерфейсов с целью определения их эффективности. Данные методы вклю-

чают в себя как количественную оценку определённых показателей качества, так и субъективную оценку пользователями удобства использования интерфейсов [1].

Для повышения качества взаимодействия оператора с приложениями сетевой безопасности предложены методы оценки человеко-компьютерных интерфейсов на основе сенсорных экранов. Предлагаются три метода оценки качества интерфейса: (1) оценка скорости выполнения заданий испытуемыми; (2) оценка точности выполнения заданий испытуемыми; (3) оценка количества жестов, реализованных в приложении безопасности.

Модель человеко-компьютерного интерфейса на основе сенсорных экранов

Пример интерфейса для сетевой безопасности приведен на рисунке.

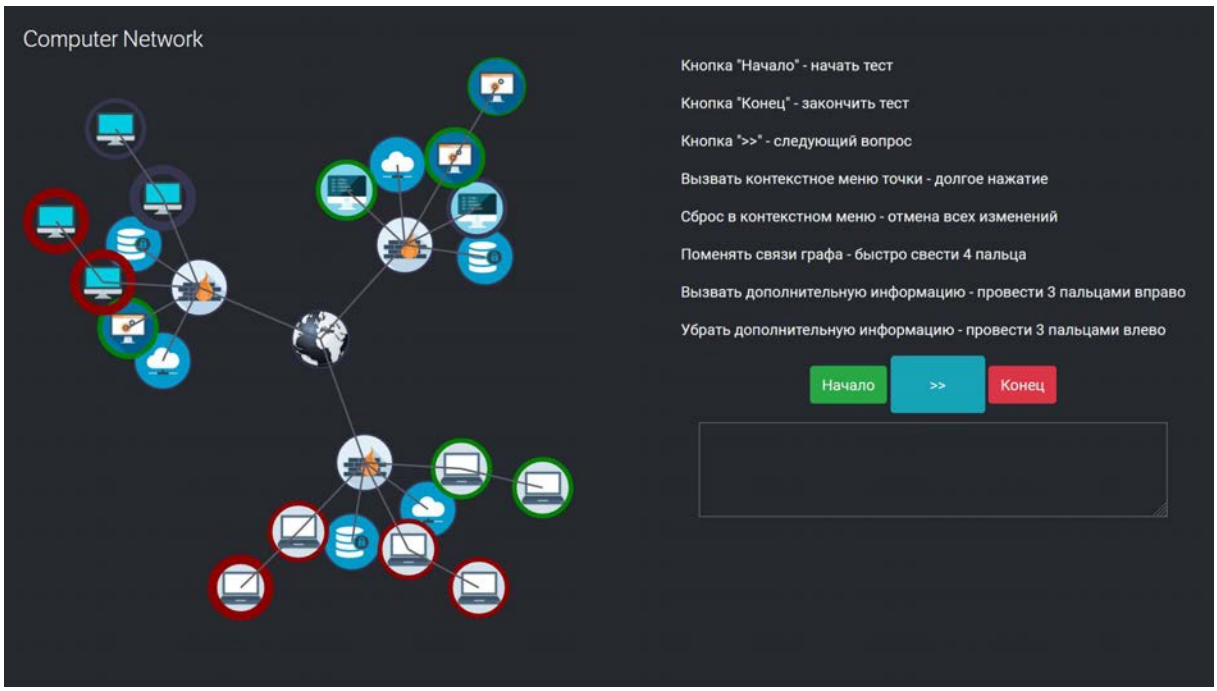


Рисунок. Визуальная модель компьютерной сети

На рис. представлена модель централизованной компьютерной сети. Модель представляет собой централизованный граф, вершинами которого являются отображения подключенных устройств, представленные в виде узнаваемых символов-изображений, центром этого графа является отображение глобальной сети Интернет. Как видно на рисунке, данная компьютерная сеть состоит из трёх подсетей, сообщающихся между собой через сеть Интернет. Доступно помещение заражённого устройства в карантин с помощью контекстного меню. Для этого нужно сначала выбрать устройство с помощью долгого нажатия, а затем выбрать пункт «Поместить в карантин

хост». Также можно поменять связи с физических на логические, если свести/развести четыре пальца на экране, и вызвать/убрать дополнительную информацию о хостах сети, если провести пальцами влево/вправо по экрану.

Методы оценки качества сенсорного интерфейса

Для оценки качества предлагается экспериментально измерять следующие количественные параметры [2, 3]: (1) скорость; (2) точность; (3) количество используемых жестов на сенсорном экране.

Скорость измеряется как среднее время, затрачиваемое испытуемыми на выполнение тестового задания. Предлагается два способа оценки скорости взаимодействия с интерфейсом:

(1) задать допустимый порог значений и сравнивать с этим порогом;

(2) сравнивать показатели модели, использующей сенсорный интерфейс, и модели, использующей кнопочный интерфейс.

В первом случае устанавливается допустимый порог значений для следующих параметров распределения по времени: (1) максимум распределения «Upper fence», (2) верхний квантиль «Q3» и (3) среднее значение «Mean». Параметры распределения по времени, полученные при решении задач, поставленных перед испытуемыми, сравниваются с заданными ранее допустимыми порогами этих значений. Во втором случае модели сравниваются между собой также в соответствии с параметрами распределения по времени.

Под *точностью* понимается средний процент ошибок, допущенных испытуемыми при выполнении задания. Таким образом, в качестве параметра точности выступает процентное соотношение общего числа выполнений тестового задания к числу ошибок, допущенных во время задания пользователями.

Количество используемых жестов должно быть достаточно большим, чтобы реализовать управление всеми функциями приложения. Однако эти жесты должны быть простыми для запоминания. Для этого предлагается делать зеркальными жесты, привязанные к противоположным функциям приложения. Например:

(1) провести пальцами вправо по экрану – показать дополнительную информацию;

(2) провести пальцами влево по экрану – убрать дополнительную информацию.

Выводы

В данной работе рассмотрены методы оценки человеко-компьютерных интерфейсов приложений безопасности на основе сенсорных экранов.

Предложенные методы оценки позволят оценить эффективность взаимодействия с интерфейсами, использующимися для работы с приложениями информационной безопасности.

Работа выполнена при финансовой поддержке РФФИ (проект 20-37-90130 Аспиранты).

Список используемых источников

1. Котенко И. В. и др. Визуальная аналитика для информационной безопасности: оценка эффективности и анализ методов визуализации // Вопросы кибербезопасности. 2021. №. 6 (46). С. 36–46.

2. Elmqvist N., Yi J. S. Patterns for visualization evaluation //Information Visualization. 2015. Vol. 14. No. 3. –pp. 250–269.

3. Arendt D. L., Burtner R., Best D. M., Bos N. D., Gersh J. R., Piatko C. D., Paul C. L. Ocelot: user-centered design of a decision support visualization for network quarantine // 2015 IEEE Symposium on Visualization for Cyber Security (VizSec). IEEE, 2015. pp. 1–8.

УДК 004.273
ГРНТИ 50.41.01

ЭГОИСТИЧНЫЕ РАСПРЕДЕЛИТЕЛЬНЫЕ АЛГОРИТМЫ КАК АЛГОРИТМЫ УПРАВЛЕНИЯ НАГРУЗКОЙ В РСХД

А. А. Зарубин, Н. М. Редругина, А. А. Швидкий

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В данной статье представлен подход к моделированию и расчету нагрузки в распределенной системе хранения данных. Используемый метод показывает, как можно усовершенствовать работу реальной системы за счет использования эгоистичного распределительного алгоритма контроля потоков требований. Это помогает решить проблему расчета сложных в исполнении и трудоемких в аналитическом расчете моделей.

система хранения данных, распределенная СХД, эгоистичные распределительные алгоритмы, аналитическое моделирование, система массового обслуживания.

Аналитический расчет нагрузки в распределенной системе хранения данных (РСХД) подразумевает моделирование сетей массового обслуживания с реализацией обратных связей. На рис. 1 показана обобщенная схема

сети массового обслуживания работы РСХД с репликацией данных на другие узлы системы. Обратная связь с блоком генерации запросов позволяет контролировать выполнение последующих операций записи. Данные модели являются сложными в построении, трудоемкими для расчета и часто имеют решения лишь в частных случаях. Что приводит к поиску альтернативных путей решения данных задач. [1]

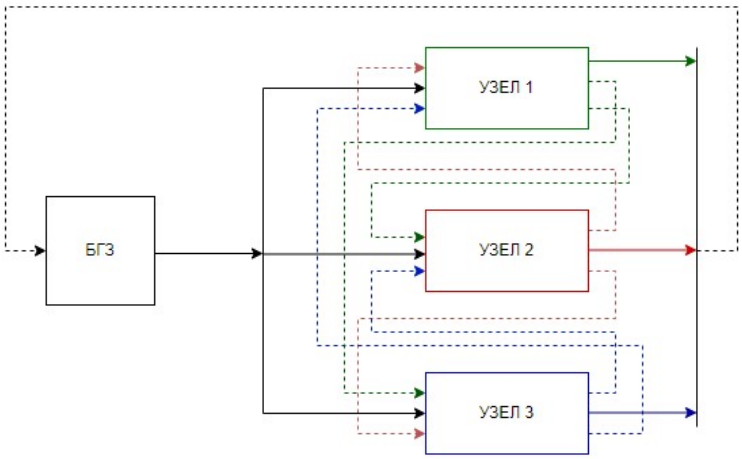


Рис. 1. Обобщенная схема системы РСХД

В данной статье описывается подход к разработке модели и расчета характеристик системы с использованием эгоистичных распределительных алгоритмов для распределенной системы хранения данных с учетом репликации записи. Для реализации РСХД был выбран синхронный подход к репликации данных, показанный на рис. 2, так как с его помощью гарантируется отказоустойчивость, однако жертвуется качество восприятия так как на стороне пользователя загруженность очередей заметно больше, чем в других подходах [3].

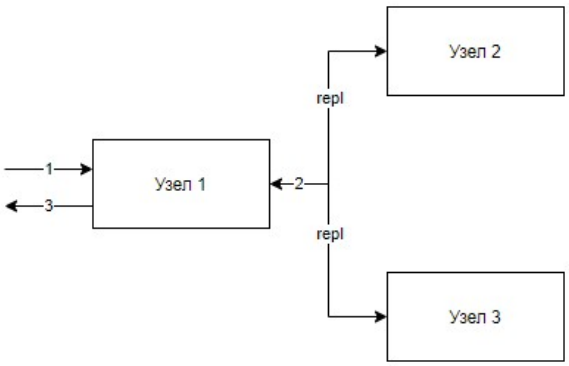


Рис. 2. Синхронный подход к репликации данных

Для реализации аналитического моделирования систему со сложной структурой было решено преобразовать в систему с упрощенной архитектурой. В случае рассматриваемой системы три узла с взаимной передачей реплицируемых данных для записи были преобразованы в сеть из двух последовательных СМО, которые было принято интерпретировать следующим образом: узел записи оригинала требования (СМО 1) и узел самой долгой записи реплики (СМО 2).

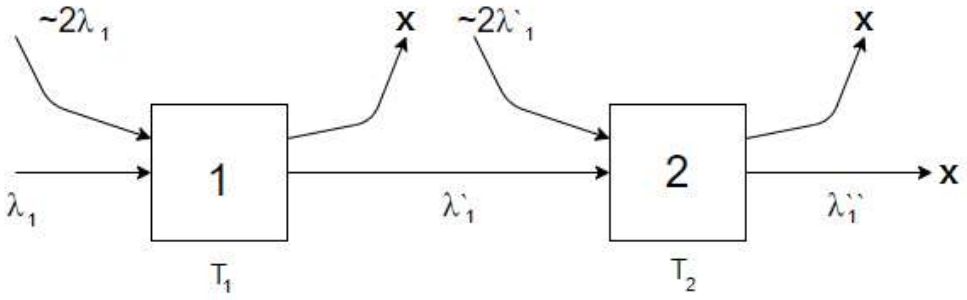


Рис. 3. Упрощенная модель системы с репликацией

Согласно схеме (рис. 3), может быть сделан вывод о времени нахождения требования в данной системе (1):

$$\hat{T} = T_1 + T_2 , \quad (1)$$

Были определены два пути решения задачи учета обратной связи со стороной, генерирующей входные запросы:

– первое решение подразумевает моделирование системы в том виде, в котором она представлена. Осуществляется путем нахождения модели телетрафика, которая включает в себя обратную связь, и разработки такой модели. Как уже упоминалось ранее, данные модели сложные в исполнении и трудоемкие в аналитическом расчете;

– второе решение заключается в моделировании поведения, при котором поток требований, поступающий в систему, зависит от того насколько данная система справляется с обслуживанием входящих требований.

В теории массового обслуживания есть класс математических моделей, которые не имеют явной обратной связи, однако они позволяют моделировать её возможности. К одной из таких моделей относится эгоистичные распределительные алгоритмы [2], которые, с одной стороны, не могут абсолютно точно смоделировать поведение данной системы, но выполняют основную задачу. При этом такие модели с малой трудоемкостью моделируют наличие в системе обратной связи со стороной генерирующей входной поток требований.

Данная модель построена по следующему принципу – все требования в имеющейся вычислительной системе делаться на две группы:

– требования, находящиеся в блоке очереди и ожидающие обслуживания, – в данном случае, это требования, находящиеся на стороне клиента;

– требования, которые находятся в блоке обслуживания, коллективно использующие обслуживающие приборы.

Блок обслуживания в случае рассматриваемой системы включает в себя два узла: узел первой записи и узел записи последней реплики.

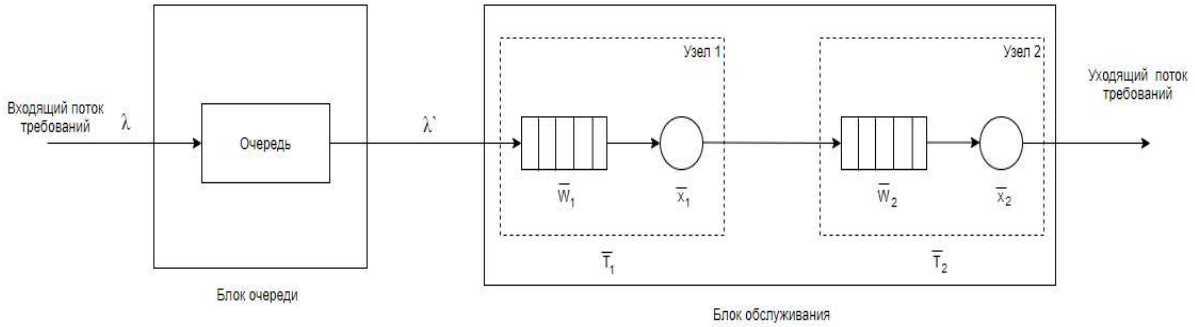


Рис. 4. Работа системы с эгоистическим распределительным алгоритмом для двух узлов

Условием перехода из блока очереди в блок обслуживания является приоритет требования, достигающий величины, равной приоритету требований в блоке обслуживания. При рассмотрении случая, когда $0 \leq \beta \leq \alpha$, где α – скорость приоритета в блоке очереди, β – скорость приоритета в блоке обслуживания, верно, утверждение, что требование, поступившее в блок очереди, должно догнать по приоритету требования находящиеся в блоке обслуживания. Как только условие выполниться, это требование попадет в блок обслуживания и может быть обслужено.

После получения результатов аналитического моделирования получен график зависимости среднего времени нахождения требования в системе от входящей нагрузки при разной скорости роста приоритета требований, а также график по результатам имитационного моделирования.

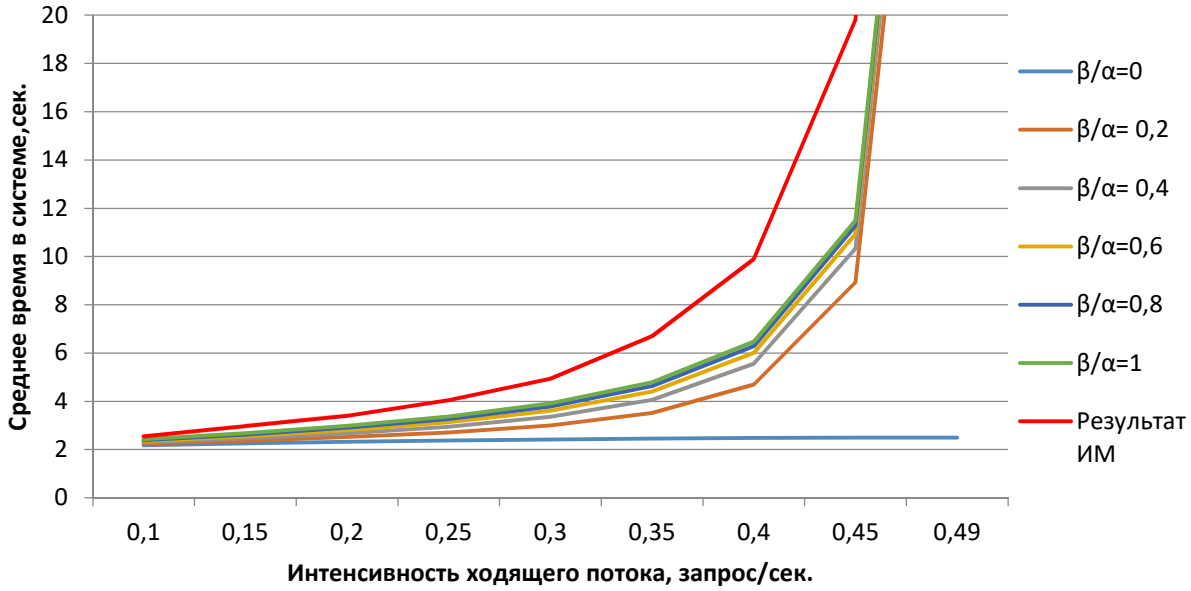


Рис. 5. Зависимость среднего времени нахождения требования в системе от входящей нагрузки

Из графика видно, что выбранный алгоритм не может абсолютно точно повторить поведение данной системы, но выполняет основную задачу в рамках наблюдения за поведением системы.

Выводы

Реализация системы как подхода с эгоистическими распределительными алгоритмами позволяет получить лучшие значения временных характеристик в ходе моделирования системы чем предложенная обратная связь после записи всех доступных реплик данных пришедших от клиента на запись.

Список используемых источников

1. Иверсен Вилли Б. Разработка телетрафика и планирование сетей / пер. с англ. под ред. А. Н. Берлина. изд. Москва: Нац. Открытый Ун-т "ИНТУИТ": БИНОМ. Лаб. знаний, 2011. 526 с.

2. Клейнрок Л. Вычислительные системы с очередями / пер. с англ. под ред. Б.С. Цыбакова изд. Москва: Мир, 1979. 600 с.

3. Кирносов В. Ю., Куржангулов Н. М. Сравнительный анализ механизмов репликаций данных в различных СУБД // Фундаментальные и прикладные исследования в современном мире. 2017. 18-1. С. 84–91.

УДК 004.273
ГРНТИ 50.41.01

АНАЛИЗ ХАРАКТЕРИСТИК ОТКРЫТЫХ СИСТЕМ ХРАНЕНИЯ ДАННЫХ

А. А. Зарубин, А. А. Савельева, А. А. Швидкий

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье рассмотрены наиболее популярные открытые системы хранения данных, а также разработаны критерии для их сравнительной оценки. Данные системы в настоящий момент представляют функциональные возможности и производительность на уровне коммерческих систем, а также имеют продуманный подход к построению таких систем на базе общедоступного аппаратного обеспечения. Данный подход уже доказал свою надёжность и эффективность, а также привёл к появлению целого класса систем хранения данных – программно-определяемых систем хранения данных.

система хранения данных, программно-определяемая СХД, распределенная СХД.

Открытые системы хранения данных основаны на открытых компонентах ОС Linux (*OpenMediaVault*, QuadSTOR) и ОС Unix (*FreeNAS*). Сами по себе они являются установленной открытой операционной системой, с набором системных утилит, для обеспечения доступа к данным. Например, такими пакетами могут быть lio для iscsi, mdraid для внутренней организации дисков, SMB и NFS сервер для файлового доступа. Большинство из этих пакетов являются модулями ядра.

Открытые системы можно разделить на два типа:

– программно-определяемые СХД,

– распределённые программно-определяемые СХД.

Так как все открытые системы покрывают максимально возможный диапазон требований к оборудованию, архитектурно они рассчитаны на использование общедоступных аппаратных платформ[3].

Среди программно-определяемых открытых СХД можно выделить:

1. Legacy СХД, основанные на стандартных компонентах ОС linux. Такие компоненты идут встроенными в большинстве дистрибутивов операционных систем(ОС CentOS Linux, ОС Redhat Linux, ОС Debian Linux, ОС Ubuntu Linux, ОС FreeBSD), и всё их развёртывание заключается в правильном конфигурировании данных элементов.

2. OpenMediaVault является программным NAS, и предоставляет графический интерфейс для управления дисками, группами дисков, способов подключения клиентов и управление правами доступа клиентов. Обладает следующими функциями [1]:

– запуск на платформе готового программного комплекса,

– основан на Debian Linux OS,

– управление через вэб-интерфейс,

– управление томами,

– поддержка информации о состоянии дисков – S.M.A.R.T.,

– объединение каналов связи,

– предоставление общего доступа к файлам (*File sharing*),

– расширяема плагинами архитектура.

3. FreeNAS является программной СХД, основанной на ОС FreeBSD (семейство Unix). Является одной из самых популярных систем для построения классической программно-определяемой СХД. Так как основана на базе FreeBSD, использует в качестве подсистемы управления дисками – ZFS. ZFS (*Zettabyte File System*) – с одной стороны это файловая система, а с другой стороны это универсальны менеджер дисковых томов и устройств, с большим количеством дополнительных функций (управление избыточностью, создание мгновенных снимков, обеспечение дедупликации). Среди возможностей freeNAS – следующие [2]:

– файловый, блочный и объектный доступ,

– вэб-интерфейс,

– защита данных, путём обеспечения избыточности,
– создание мгновенных снимков,
– репликация данных в другую локацию,
– шифрование данных,
– расширяемая плагинами архитектура.

4. QuadSTOR является открытым проектом, предназначенным для установки на ОС Linux, и обладающем минимальным набором возможностей для построения высокопроизводительных программно-определяемых СХД, со встроенными функциями повышения эффективности хранения данных. Среди основных особенностей можно выделить:

– тонкое выделение дисков (выделение необходимого пространства по требования),
– работа по протоколам FC, iSCSI NFS и CIFS (со встроенным FC target),
– дедупликация данных при поступлении на СХД,
– построение кластера высокой доступности,
– синхронное зеркалирование на блочном уровне,
– поддержка API ускорение работы VMware,
– работа с кластерами Windows Server.

Все эти проекты позволяют организовать СХД с базовым набором функций, отвечающих минимальному набору требований к СХД.

Так же существует несколько проектов открытых распределенных программно-определяемых СХД, среди которых MinIO, Linstore и Ceph.

MinIO [4] – проект распределенной программно-определяемой СХД, предполагающей объектный доступ к информации. Данный проект является открытой разработкой, предназначенной исключительно для работы в облачной инфраструктуре.

Linstor [5] – проект, обладающий самой высокой производительностью из всех открытых проектов, а так же опережающий по производительности многие коммерческие проекты.

Ceph [6] – проект объектной СХД, реализующей, поверх объектов, хранилища необходимых типов – блочного и файлового. Благодаря такой структуре имеет встроенную поддержку всех протоколов доступа к данным, реализуемую собственными компонентами, без необходимости в использовании внешних шлюзов.

Распределённые программно-определяемые СХД имеют преимущества перед программно-определяемыми как в возможности масштабирования (рис.), так и в возможности повышения производительности.

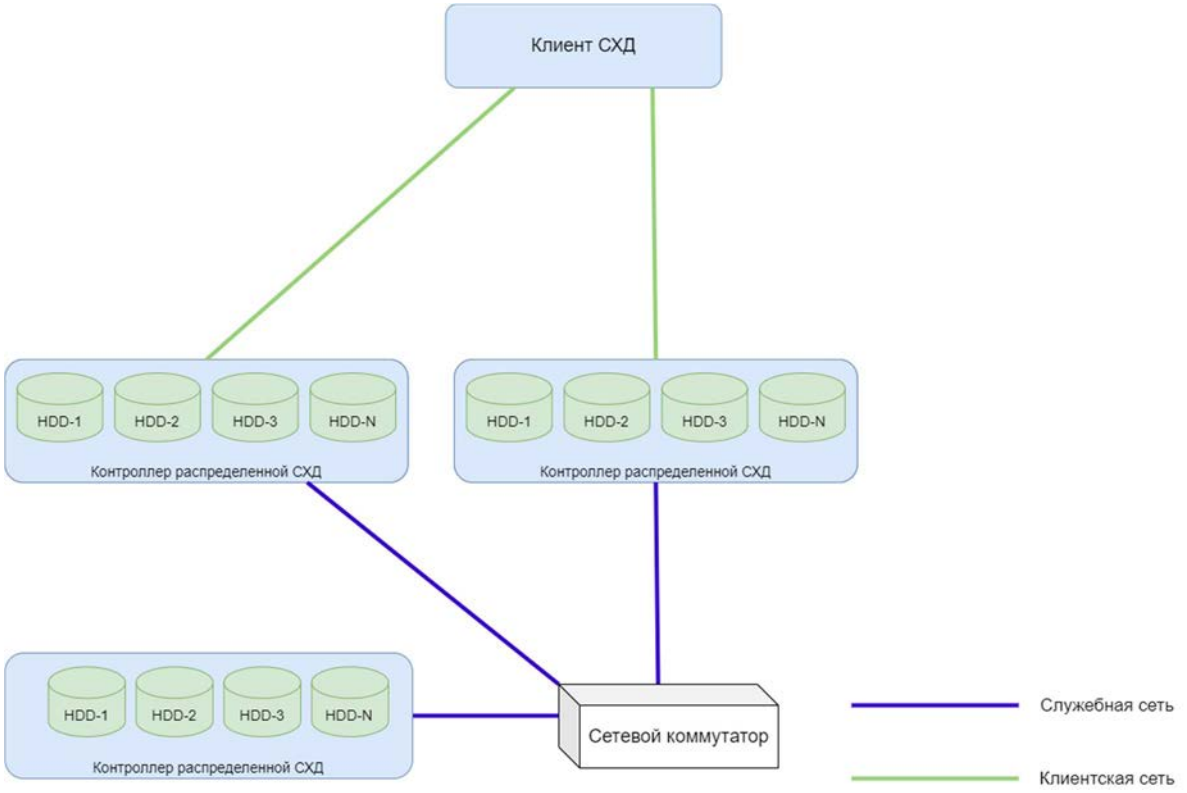


Рисунок. Схема построения распределенной СХД

Тот факт, что распределённая программно-определяемая СХД может быть определена несколькими классическими, связанными логическими протоколами для объединения систем, говорит о том, что распределенные программно-определяемые СХД обладают всеми возможностями программно-определяема СХД, но при этом имеют расширенную функциональность:

– возможность управления созданием копий данных и их количеством;

– заложенная в архитектуру возможность разнесения данных по различным локациям;

– возможность горизонтального масштабирования, путем добавления дополнительных узлов хранения.

Всё это делает распределенные программно-определяемые СХД наиболее подходящим кандидатом для дальнейшего исследования. Исходя из результата анализа открытых программно-определяемых СХД, можно сделать вывод о функциональности программно-определяемых СХД (табл.).

ТАБЛИЦА. Сравнение функциональности программно-определяемых СХД

Критерий	MinIO	Ceph	Linstore
Относительная Производительность	низкая	низкая	высокая
Максимальное количество узлов (теоретическое)	32 [9]	не ограничено	16 [10]

Критерий	MinIO	Ceph	Linstore
Максимальное количество узлов(достигнутое)	32 [9]	225	16 [10]
Обеспечение объектного доступа	да	да	нет
Обеспечение блочного доступа	нет	да	да
Обеспечение файлового доступа	нет	да	да
Репликация для обеспечения избыточности	нет	да	да
Коды коррекции для обеспечения избыточности	да	нет	нет
Катастрофоустойчивость	да	да	нет
Георепликация	нет	да	нет
Разделение доменов хранения	нет	да	нет
Встроенные механизмы кэширования	нет	да	да
Наличие собственного протокола блочного доступа	нет	да	да
Встроенные механизмы шифрования данных	нет	нет	да
Интеграция с системами виртуализации	нет	да	да
Относительная сложность развёртывания	низкая	очень высокая	средняя
Относительная простота документации	средняя	высокая	низкая
Наличие механизмов поиска ошибок	да	да	нет

Исходя из проведённой оценки систем хранения данных, можно сделать вывод о необходимость проводить исследования на открытых системах хранения данных, так как закрытые не обладают необходимой гибкостью в настройке, и перестройке рабочих параметров системы хранения данных, а закрытый или ограниченный доступ к диагностической информации делает невозможность её анализ с целью повышения производительности СХД.

Так же можно сделать вывод о том, что распределённые программно-определяемые СХД имеют преимущество перед классическими СХД, так как обладают широкими возможностью к масштабированию как производительности, так и доступного объёма для хранения информации. При этом имеются все возможности нивелировать влияние масштабирования на безопасность и защищённость данных от потери.

Ещё одним преимуществом открытых СХД является возможность их развёртывания на оборудовании любого типа, что позволит как использовать имеющееся оборудование, так и выбирать наиболее доступное из представленных на рынке.

Список используемых источников

1. Openmediavault. 2020. URL: https://www.openmediavault.org/ (дата обращения: 25.03.2021).

2. FreeNAS. Features. 2020. URL: https://www.freenas.org/about/features/ (дата обращения: 25.03.2021).

3. Зарубин А. А., Елагин В. С., Савельева А. А., Швидкий А. А. Подходы к моделированию нагрузки на распределенную систему хранения данных // Системы синхронизации, формирования и обработки сигналов. 2018. Т. 9, № 3. С. 90–95

4. Intel. Implementation Guide for MinIO. Storage-as-a-Service. 2020. URL: https://min.io/resources/docs/CPG-MinIO-implementation-guide.pdf (дата обращения: 25.03.2021).

5. LINBIT HA-Solutions Gmbh. Block Storage Management for Containers. 2020. URL: https://linbit.com/linstor/ (дата обращения: 25.03.2021).

6. Ceph docs. 2020. URL: https://docs.Ceph.com/en/latest/rados/operations/pools/ (дата обращения: 25.03.2021).

УДК 004.056.53
ГРНТИ 49.33.35

РАЗРАБОТКА МОДУЛЯ ANSIBLE ДЛЯ ОБНАРУЖЕНИЯ НЕЛЕГИТИМНЫХ БЕСПРОВОДНЫХ ТОЧЕК ДОСТУПА В КОРПОРАТИВНОЙ СЕТИ

Е. А. Зебзеев, М. М. Ковцур, Т. В. Петрова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Нехватка квалифицированных специалистов по безопасности и доступность средств автоматизации в инструментах безопасности привели к росту использования автоматизированных процессов, которые «самостоятельно» решают задачи, основанные на предопределенных правилах и шаблонах, поэтому автоматизация в настоящее время является одним из важнейших трендов для системы безопасности. С помощью автоматизации сетевых задач и функций, а также с помощью повторяющихся процессов с автоматическим контролем и управлением, повышается доступность сетевых служб. В докладе представлено описание модуля Ansible для обнаружения нелегитимных беспроводных точек доступа в корпоративной сети. Рассмотрена структура модуля обнаружения нелегитимного устройства.

автоматизация, Ansible, безопасность, нелегитимная точка доступа.

В настоящее время очень часто происходят различного рода атаки на беспроводные корпоративные сети [1–3], и одной из таких атак является намеренное подключение нелегитимной беспроводной точки доступа с целью получения корпоративных данных компании или же с целью взлома сети [4]. С этим можно бороться по-разному: системный администратор может вручную постоянно осуществлять мониторинг [5] сети на появление в ней нелегитимных беспроводных точек доступа и отключать их, а можно все эти действия выполнять с помощью различных инструментов автоматизации.

В последнее время автоматизация приобрела очень большую популярность. Существует несколько весьма известных инструментов автоматизации, таких, как Puppet, Chef, SaltStack и Ansible. На основе рассмотренных преимуществ [6] данных инструментов и статистики запросов по ключевым словам на популярном поисковом ресурсе google.com за последние несколько лет (рис. 1), были сделаны выводы, что Ansible – наиболее популярная система автоматизации. Ansible – это система управления конфигурациями, которая позволяет автоматизировать и упростить настройку, обслуживание и развертывание серверов, служб, программного обеспечения и т. д.

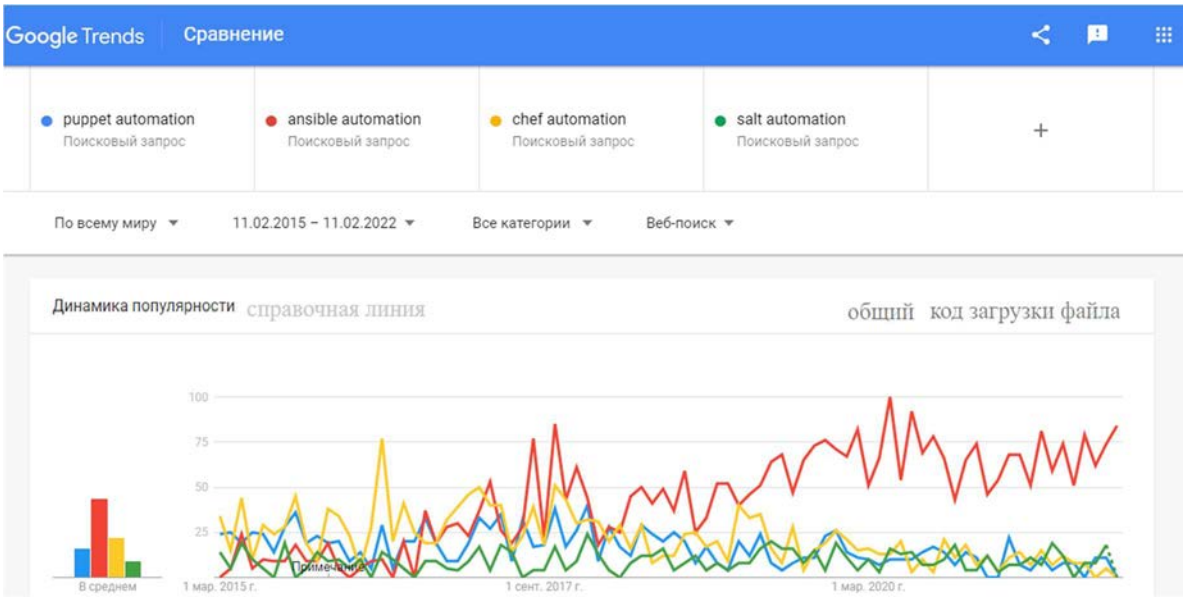


Рис. 1. Статистика запросов по ключевым словам
на популярном поисковом ресурсе google.com за последние 7 лет

На рис. 2 представлена концепция работы модуля обнаружения нелегитимных точек доступа. Модуль реализуется на компьютере с операционной системой Ubuntu [7], на котором установлены инструмент автоматизации Ansible и база данных MySQL. Также в данной концепции имеется коммутатор, с которым взаимодействует компьютер посредством Ansible по протоколам управления SNMP и SSH, и имеется нелегитимная точка доступа, которая подключается к одному из портов коммутатора. Нелегитимные устройства в сети могут отслеживаться какими-либо вышестоящими внешними системами, например, сенсорами или системой обнаружения вторжения, которые видят MAC-адреса беспроводных устройств и вносят эти адреса в SQL-таблицу как нелегитимное устройство.

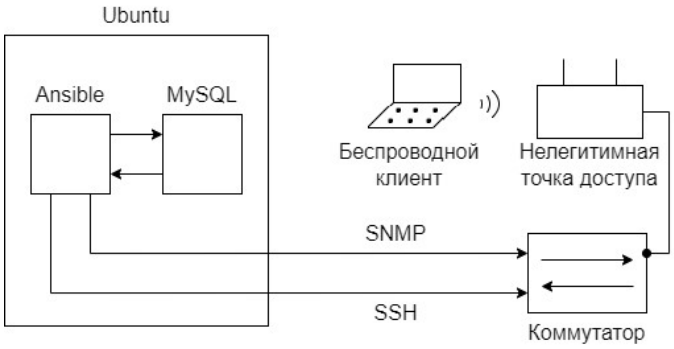


Рис. 2. Концепция работы модуля обнаружения нелегитимных точек доступа

На рис. 3 представлена схема эксперимента. В неё включены две виртуальные машины (ВМ): Ubuntu и EVE-NG, которые развернуты в VMWare Workstation. EVE-NG – эмулированная виртуальная среда, позволяющая создать полноценную виртуальную лабораторию с сетевым оборудованием. В ней был развернут коммутатор Cisco и к нему подсоединен компьютер, который на данный момент заменяет нелегитимную точку доступа.

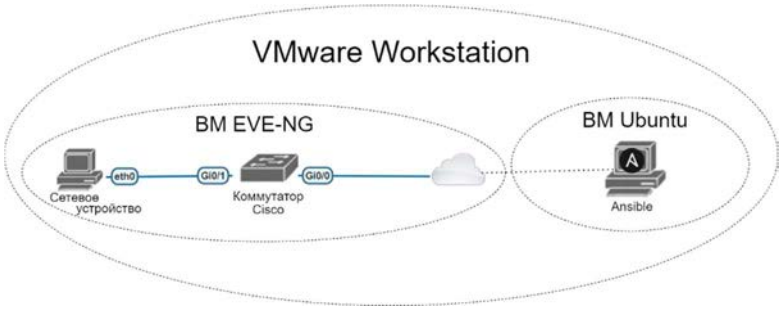


Рис. 3.Схема эксперимента

Концепция разрабатываемого модуля представлена на рис. 4. Данный модуль состоит из двух компонентов: инструмента автоматизации Ansible и второго компонента – базы данных MySQL. Ansible состоит из двух файлов – playbook’а и файла инвентаризации. База данных MySQL содержит в себе две таблицы «verification» и «alert».

Файл инвентаризации – это файл, описывающий устройства, к которым Ansible будет подключаться. Playbook – это описание состояния ресурсов системы, в котором она должна находиться в конкретный момент времени, включая установленные пакеты, запущенные службы, созданные файлы и многое другое. Вместо того, чтобы индивидуально использовать

команды для удалённой настройки компьютеров из командной строки, можно настраивать целые сложные среды, передавая скрипт одной или нескольким системам.

Рис. 4. Концепция разрабатываемого модуля

На рис. 5 представлена блок-схема работы playbook’a. Алгоритм заключается в следующем: сначала происходит обращение к коммутатору посредством протокола SNMP и достаются значения MAC-адреса, индекса порта и название порта, указанные в табл. 1 коммутации на коммутаторе, далее из SQL-таблицы “verification” достается значение MAC-адреса устройства, которому присвоен флаг “R” (rogue – нелегитимное устройство). Затем происходит сравнение MAC-адреса, полученного с коммутатора, и MAC-адреса из SQL-таблицы “verification”. Если они идентичны, то блокируется порт коммутатора, к которому подключено устройство с данным MAC-адресом, затем данное событие записывается в SQL-таблицу “alert”.

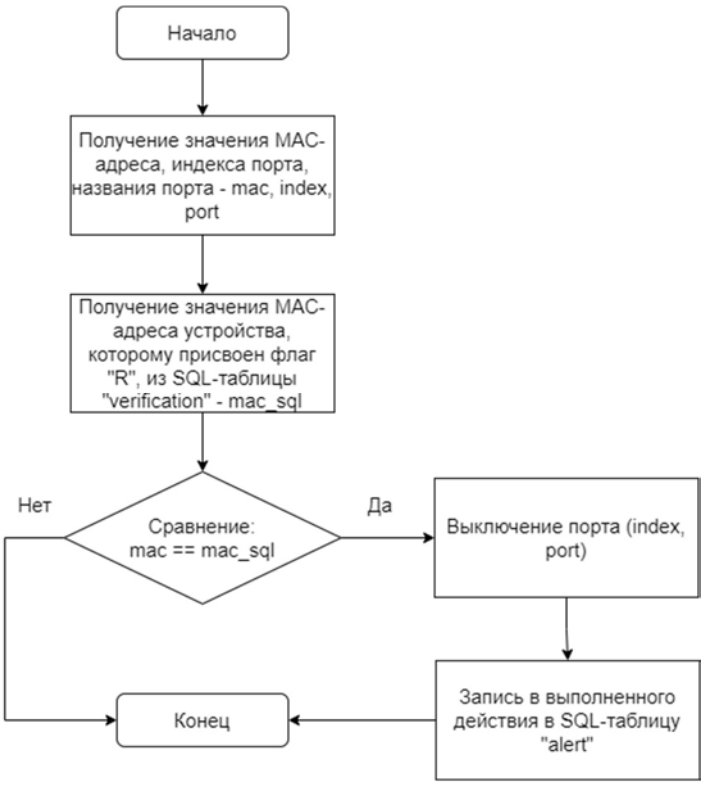


Рис. 5. Блок-схема playbook’a

В таблице представлено имя устройства, его IP-адрес и MAC-адрес, а также флаг “V” – verified, которым отмечается проверенное устройство, и флаг “R” – rogue, которым отмечается нелегитимное устройство. В ту же очередь в табл. 2 представлено имя коммутатора, на котором происходило действие, индекс порта, который был отключен, время, когда это произошло, и само действие.

ТАБЛИЦА 1. Пример заполнения SQL-таблицы “verification”

name	ipadd	macadd	flag
ubuntu	192.168.176.128	00:2c:29:dc:5b:c2	V
unknown	-	00:50:79:66:68:04	R

ТАБЛИЦА 2. Пример заполнения SQL-таблицы “ alert”

name	port_index	time	action
cisco	1	2022-02-04 16-37-11	shutdown
cisco	2	2022-02-13 11-54-03	shutdown

Также был проведен эксперимент на физическом оборудовании. Схема эксперимента представлена на рис. 6. Она содержит в себе точку доступа Asus, коммутатор Cisco Catalyst 2960 и ВМ Ubuntu.

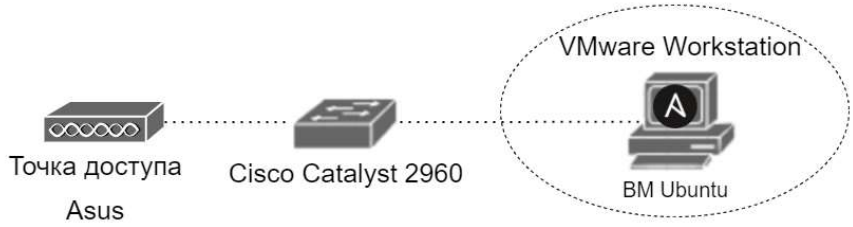


Рис. 6. Схема эксперимента

Результатом данной работы является разработанная структура модуля Ansible, который автоматически обнаруживает беспроводное нелегитимное устройство в корпоративной сети с помощью таблицы коммутации и протокола SNMP, а также осуществляет блокировку порта, к которому было подключено нелегитимное устройство, и запись данного действия в SQL-таблицу. Данное решение позволяет автоматически блокировать и отключать нелегитимную точку доступа, которая подключена к коммутатору, что позволяет уменьшить вероятность взлома корпоративной сети. Также данные действия были подтверждены экспериментально на физическом оборудовании.

Список используемых источников

1. Красов А. В., Петрив Р. Б., Сахаров Д. В., Сторожук Н. Л., Ушаков И. А. Масштабируемое Honeypot-решение для обеспечения безопасности в корпоративных сетях // Труды учебных заведений связи. 2019. Т. 5. № 3. С. 86–97.

2. Миняев А. А., Третьяков И. В. Автоматизированная система контроля сетевого доступа в инфокоммуникационной среде // Международная конференция по мягким вычислениям и измерениям. 2009. Т. 1. С. 215–217.

3. Ковцур М. М., Герлинг Е. Ю., Коновалова В. В., Киструга А. Ю. Исследование способов удаленного перехвата трафика в корпоративных сетях // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2021. № 4. С. 68–75.

4. Александрова Е. С., Ковцур М. М. Разработка модели нарушителя в беспроводных сетях стандарта IEEE 802.11 // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VI Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2017. Т. 2. С. 24–28.

5. Ковцур М. М., Коновалова В. В., Мисливский Б. С., Михайлова А. В., Акилов М. В. Разработка методики удаленного мониторинга трафика в корпоративных сетях // Заметки ученого. 2021. № 6-1. С. 27–31.

6. Красов А.В., Косов Н.А., Холоденко В.Ю. Исследование методов провижининга безопасной сети на мультивендорном оборудовании с использованием средств автоматизированной конфигурации // Colloquium-journal. 2019. № 13-2 (37). С. 243-247.

7. Штеренберг С. И. Исследование и анализ особенностей форматов исполнимых файлов под Linux для скрытого вложения информации // Информационные технологии и телекоммуникации. 2014. Т. 2. № 1. С. 38–48.

УДК 004.056
ГРНТИ 49.33.35

РАЗРАБОТКА АРХИТЕКТУРЫ СТЕНДА ДЛЯ ТЕСТИРОВАНИЯ ЭФФЕКТИВНОСТИ МОДУЛЯ ОБНАРУЖЕНИЯ МНОГОШАГОВЫХ АТАК

И. Ю. Зеличенок, И. В. Котенко

Санкт-Петербургский Федеральный исследовательский центр Российской академии наук

В работе описывается процесс проектирования архитектуры стенда для проверки эффективности предполагаемого модуля обнаружения аномалий, проведен анализ решений, используемых на сегодняшний день. Основной особенностью данного стенда является моделирование разнородного трафика на разных узлах системы, который предположительно будет сниматься разными компонентами модуля обнаружения аномалий с применением методов машинного обучения и технологий обработки больших данных для выявления многошаговых атак и создания гипер-предупреждения, содержащего подробное описание атаки.

защита информации, кибератаки, многошаговые атаки, обнаружение атак.

С развитием информационных технологий атаки на сети стали более комплексными и сложными, из-за чего при большом потоке данных выявить их вручную становится невозможным [1, 2]. Для анализа большого потока данных целесообразно использовать разработки, сочетающие в себе методы машинного обучения для глубокого анализа данных и технологии обработки больших данных. Однако, методы машинного обучения крайне чувствительны к качеству данных, поэтому главной задачей при разработке таких технологий является получение целостного и достоверного набора данных.

Сложными или многошаговыми атаками можно назвать те, в которых отдельное событие может быть частью сценария атаки, даже если оно кажется безобидным, или события, относящиеся к одному и тому же сценарию атаки, имеют общую черту - они представляют собой действия, ведущие к одной цели, но это не обязательно явно выражено в событиях [3]. Многошаговые атаки не могут быть описаны менее чем двумя событиями.

Для получения данных, необходимых для анализа многошаговых атак, активность системы, с которой данные были получены, должна отслеживаться на наибольшем количестве уровней сети.

Цель исследования заключалась в анализе существующих подходов и методик для получения данных для экспериментов и предоставлении первичного прототипа стенда, а главной задачей – анализ существующих публикаций по релевантной теме и создание прототипа стенда на основе выявленных в публикациях тенденций.

После анализа релевантных работ, было выявлено два основных направления получения данных для экспериментов. Исследователи либо использовали готовые наборы данных, либо создавали их самостоятельно.

Наиболее распространенными наборами данных, используемыми в научной среде, являются DARPA, KDD 1999, DEFCON, CICIDS, и другие (рис. 1). Большая часть исследователей предпочитает создавать наборы данных самостоятельно.

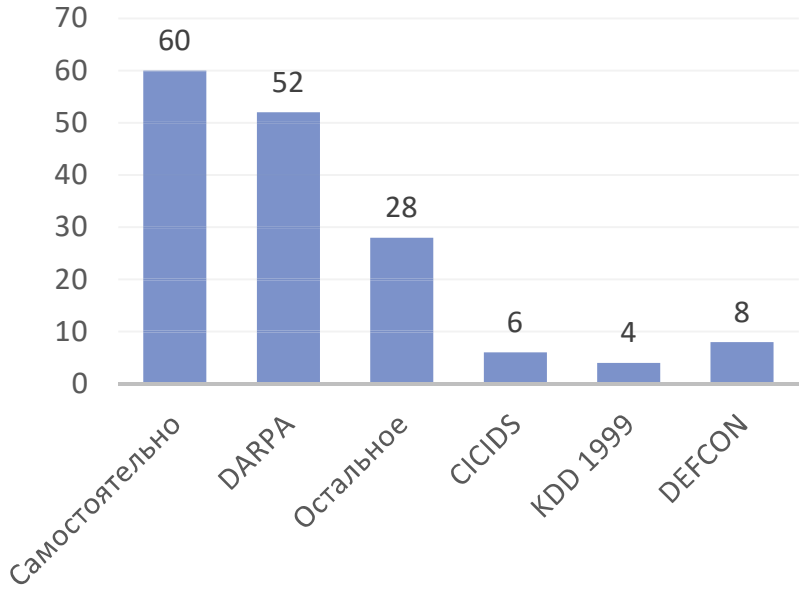


Рис. 1. Источники экспериментальных данных в публикациях

Самыми распространенными в исследованиях публичными наборами данных [4] являются данные серии DARPA, собранные американскими военными, которые применяются для анализа и тестирования методов выявления многошаговых атак. К данной серии относятся наборы данных

DARPA 1999, DARPA 2000 и DARPA CGP (CGC). Данные наборы содержат предупреждения систем обнаружения вторжений (IDS), собранные с использованием сетевого трафика и журналов аудита, собранных в сети моделирования. IDS обрабатывали эти данные в пакетном режиме и пытались идентифицировать сеансы атаки в процессе нормальной работы. В отличие от DARPA 1999, DARPA 2000 включает в себя многошаговые атаки LLDoS 1.0 и LLDoS 2.0. Первая начинается с фазы зондирования, потом идет этап проникновения и заканчивается установкой средства для запуска DDoS. Вторая же является усложненным вариантом первой. DARPA CGP – это данные, полученные из проекта Grand Challenge Problem. Он задает примеры атак в виде предупреждений из источников на разных уровнях: систем управления сетью, межсетевого экрана, сетевой IDS и IDS на основе хоста.

KDD 1999 является упрощенной выборкой из комбинации наборов данных DARPA для соревнований «Захват флага» (*Capture the Flag*, CTF), в котором одна команда пытается защитить набор сервисов, а другая получить к ним несанкционированный доступ. Данные DEFCON также получены в результате проведения ежегодного CTF в Лос-Анджелесе.

Данные KDD и DARPA используются в научной среде начиная с 2000-х годов. Однако, за 20 лет информационные технологии заметно эволюционировали, а атаки на них стали более сложными. Обучение моделей машинного обучения на атаках, проведенных по сценарию «зондирование – проникновение – DdoS» может быть недостаточным.

CICIDS и остальные данные, созданные институтами или частными компаниями, слишком мало изучены.

Для достижения наибольшего качества и достоверности наборов данных было принято решение моделировать трафик самостоятельно.

В процессе исследования релевантных публикаций, начиная с 2018 года [5–10], было выявлено два основных подхода к проектированию стендов для генерации данных.

При первом подходе исследователи сразу создают сложную структуру сети и проектируют IDS, основываясь на архитектуре всей сети в целом. Данный подход эффективен, когда заранее известно, для какой сети будет использоваться спроектированная IDS, определена ее типовая нагрузка и состав.

При втором подходе IDS создается для типового элемента сети, а затем стенд расширяется, добавляются новые виртуальные машины и компоненты-сборщики. При этом подходе отрабатываются методы расширения и адаптации IDS к другим нетиповым сетям, когда заранее неизвестно, какие узлы и процессы будет отслеживать система.

Исходя из проведенного исследования, были выявлены основные требования к получаемым данным с предполагаемой системы:

– полный трафик – моделирование пользователей, наличие разных машин в сети-жертве и реальные атаки из сети-атаки;

– помеченный набор данных – должна быть разметка с типами атак;

– полное взаимодействие – все компоненты сети должны взаимодействовать и моделировать реальное поведение рабочей сети;

– разнообразие атак - в набор данных должны быть включены разнообразные атаки на разных узлах системы;

– неоднородность – захват данных со всех узлов машин-жертв во время проведения атак.

Для стенда, который должен обеспечивать описанные ранее критерии, можно выдвинуть следующие требования:

– простая повторяемость экспериментов – стенд должен содержать в себе инструментарий для простой реализации экспериментов, например, скрипты или дополнительное ПО;

– гибкая настройка всех элементов стенда;

– возможность собирать данные на всех уровнях стенда для выявления многошаговых атак;

– разнообразие активностей, создаваемых стендом;

– масштабируемость – возможность увеличить объем данных или число виртуальных машин без потери производительности;

– большой поток данных, генерируемый стендом.

Исходя из проанализированных источников и выдвинутых требований к данным и стенду, была выбрана архитектура, продемонстрированная на рис. 2.

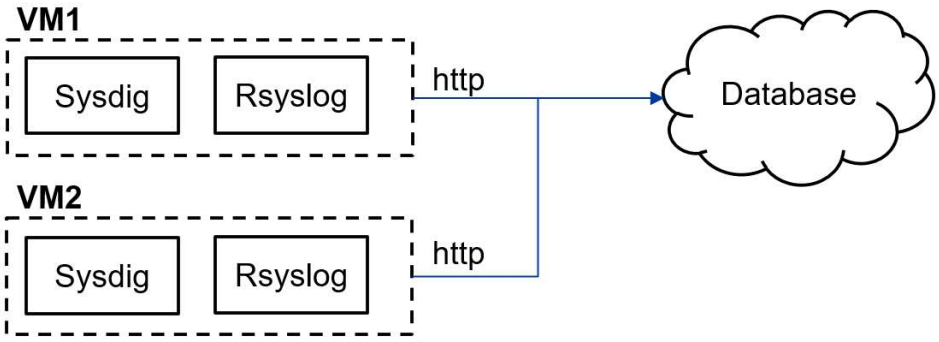


Рис. 2. Архитектура стенда

Предлагаемый стенд для проведения экспериментов состоит из следующих компонентов:

- Sysdig - компонент, используемый для сбора системных логов.
- Rsyslog - используется для логгирования сетевой активности.
- Database – база данных.

Для имитации активности был использован скрипт, разворачивающий и имитирующий работу двух серверов, веб-сервисов и краулера [10].

Краулер (рис. 3) сканирует Интернет в поиске информации на заданную тему и переносит полученную информацию в Elasticsearch. Сайт, который находится на сервере nginx, загружает информацию из Elasticsearch. Kibana хостит JEFF monitor, а тот, в свою очередь, отслеживает прогресс краулера.

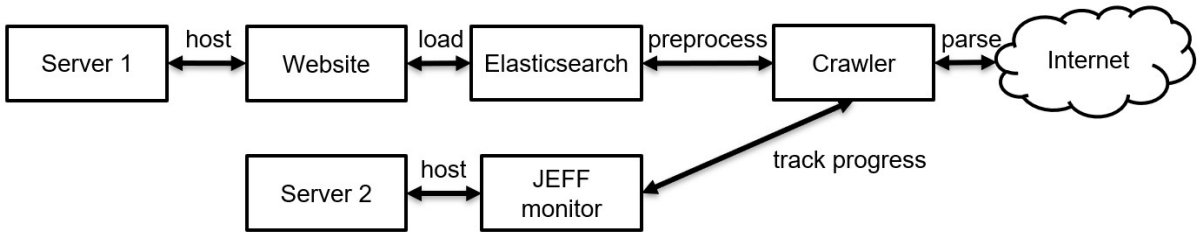


Рис. 3. Схема моделируемой нагрузки на стенд

Данная архитектура обладает рядом преимуществ, например, стенд легко масштабируется за счет добавления новых виртуальных машин и/или компонентов сбора данных. За счет распределенной инфраструктуры производительность ухудшается не так сильно, как если бы компоненты и коррелятор были вместе. Имеется возможность получить данные на разных узлах за счет гибкой настройки компонентов-сборщиков и их комбинации для выявления многошаговых атак.

Недостатками данной архитектуры является наличие эффекта «узкого горла» во время передачи больших объемов данных по http-протоколу в базу данных [8].

В результате исследования был проведен анализ тенденций в создании трафика для систем обнаружения вторжений. На основе исследования была предложена архитектура стенда, имитирующего нормальную нагрузку и создающего более 6 тысяч записей в секунду. В рамках будущих работ планируется провести собственный обзор существующих алгоритмов и подходов к анализу и корреляций событий информационной безопасности.

Работа выполнена при частичной финансовой поддержке РНФ (проект № 21-71-20078).

Список используемых источников

1. Kotenko I., Stepashkin M. Analyzing Vulnerabilities and Measuring Security Level at Design and Exploitation Stages of Computer Network Life Cycle // Lecture Notes in Computer Science. 2005. Vol. 3685. pp. 311–324.

2. Kotenko I., Konovalov A., Shorov A. Agent-based simulation of cooperative defence against botnets // Concurrency and Computation: Practice and Experience, Vol. 24, Issue 6, 2012. P. 573-588.

3. Hu H. et al. Security metric methods for network multistep attacks using AMC and big data correlation analysis // Security and Communication Networks. 2018. Vol. 2018.

4. Julio Navarro, Aline Deruyver, Pierre Parrend, A systematic survey on multi-step attack detection // Computers & Security. 2018. Vol. 76. pp. 214–249.

5. Ying Lin, Zhengzhang Chen, Cheng Cao, Lu-An Tang, Kai Zhang, Wei Cheng, and Zhichun Li. Collaborative Alert Ranking for Anomaly Detection // Proceedings of the 27th ACM International Conference on Information and Knowledge Management (CIKM '18). Association for Computing Machinery. 2018. New York. pp.1 987–1995.

6. Zhao D. et al. Bidirectional rnn-based few-shot training for detecting multi-stage attack // arXiv preprint arXiv:1905.03454. 2019.

7. Mahdavi E., Fanian A., Amini F. A real-time alert correlation method based on codebooks for intrusion detection systems // Computers & Security. 2020. Vol. 89. 101661.

8. Landauer M., Skopik F., Wurzenberger M., Hotwagner W., Rauber A. A Framework for Cyber Threat Intelligence Extraction from Raw Log Data // 2019 IEEE International Conference on Big Data (Big Data), Los Angeles, CA, USA. 2019. pp. 3200–3209.

9. Десницкий В. А., Чечулин А. А., Котенко И. В., Левшун Д. С., Коломеец М. В. Комбинированная методика проектирования защищенных встроенных устройств на примере системы охраны периметра // Труды СПИИРАН. 2016. № 5 (48). С. 5–31.

10. Di Mauro M., Di Sarno C. Improving SIEM capabilities through an enhanced probe for encrypted Skype traffic detection // Journal of information security and applications. 2018. Vol. 38. pp. 85–95.

УДК 004.031.2
ГРНТИ 49.33.29

ИЗМЕНЕНИЕ ПАРАДИГМЫ ИЛИ ПРИНЦИПОВ ИСПЫТАНИЙ СЕТЕВОГО ОБОРУДОВАНИЯ ПРИ ПЕРЕХОДЕ К ГЕТЕРОГЕННЫМ СЕТЯМ 5G

А. В. Зимин, Ю. П. Ревенко

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Важность испытаний сетевого оборудования с переходом к сетям 5го поколения только растет. Если для сетей TDM и даже NGN были достаточно устоявшиеся правила совместной работы сетей и оборудования, то переход к гетерогенным сетям, тренд к самоорганизации и виртуализации, а также лавинообразный рост услуг и технологий, повышает требования к проверке оборудования на готовность стать полноценным и надежным участником сети пятого поколения. При таких вводных приходится основываться и рассматривать новые модели и алгоритмы или комбинации уже существующих моделей, необходимо максимально учитывать суммарный образ сети, в некотором смысле сдвинуться от испытания каждого одного конкретного «черного ящика», в сторону тестирования в комплексном информационном поле.

5G, NGN, пост-NGN, Network Under Test, гетерогенные сети.

Современные тенденции развития технологий уже такие, что, когда мы говорим об изменении ситуации на сети, о сроках эксплуатации какого-либо сетевого оборудования, речь идет уже далеко не о десятилетиях, это диапазон в несколько лет, а зачастую и меньше.

При этом подходы или методы испытаний в телекоммуникациях из серий контрольных вызовов и наборов сценариев на протокол-тестере, также претерпели ряд изменений и превратились в комплексы чрезвычайно сложных системно-сетевых процедур, ориентированных на функциональные (корректная маршрутизация, СОРМ, пограничные контроллеры сессий и т. п.), параметрические (задержки, потери и т. п.), сервисные (QoS, QoE и т.п.) и разные наборы требований [1]. Так в Рекомендации Q.3900 тестирования NGN рассматривается уже, прежде всего как тестирование функциональности на модельных сетях. И основными функциями, требующими обязательного тестирования, являются: Transport stratum functions; Transport functions; Transport control functions; Transport user profile functions; Service stratum functions; Service control functions; Application/Service support functions; Service user profile functions; End-user functions; Management Functions [2].

Для тестирования каждой из этих функций уже необходимо более предметно разбирать их внутреннюю функциональность, необходимо также определить их назначение и степень ответственности.

В свою очередь технические средства NGN могут реализовывать в своем составе сразу несколько функций, что уже значительно усложняет процедуру тестирования и испытания сетевого оборудования. С каждым новым поколением сети сложность, архитектура и взаимодействие сетевых элементов стремительно изменяется, что накладывает новые требования к самой сети и возможному качеству обслуживание.

Так, переход к сетям 5G, которые уже ориентированы на виртуализацию сетевых функций, не говоря уже о концепции NFV, с соответствующим изменением структуры сети, добавлением новых сетевых элементов, появлением новых протоколов, предъявляет уже свои, как правило, повышенные требования к качеству обслуживания, задержкам и потерям пакетов, надежности сети [3].

Гетерогенные сети 5G призваны решить большее число проблем, возникающих в мобильных сетях. Вполне естественно, что с развитием сети, с каждым новым поколением появляется все большее число новых технологий и новых сетевых элементов.

Сети пятого поколения уже в обязательном порядке предполагают наличие разнородного трафика (H2H, D2D, M2M), помимо традиционных услуг NGN. Например, технология Network Slicing предполагает на основе общего сетевого ресурса, физической среды, обеспечивать существование

множества виртуальных, логически разделенных сетей для внедрения различных услуг, для которых в свою очередь зачастую требуются разные технологии, каждая со своими показателями качества обслуживания.

Таким образом сымитировать, предусмотреть и оценить многообразие возможных к возникновению на реальной сети ситуаций становится уже не тривиальной задачей. Что будет и какими будут сети всего лишь через несколько лет? Предсказать или прогнозировать такое развитие чрезвычайно сложно. При этом с переходом к гетерогенным сетям, существующие методы и модели тестирования по отношению к 3G несильно изменились [4]. На сегодняшний день существует довольно большое число различных видов испытаний, которые можно классифицировать по тому или иному признаку, это могут быть испытания, например, по виду, т.е. сертификационные или инспекционные, приемосдаточные или аттестационные; по различным видам внешних воздействий, такие как механические или климатические. Конечно, нельзя не обратить внимание на испытания характеристик оборудования – это и функциональные и испытания на надежность, безопасность и многие другие.

При этом разделяется два подхода «белого» и «черного ящика».

В первом случае ориентируемся на внутреннюю структуру программной реализации, испытываемого объекта, с целью исследовать программный код и выявить максимальное число возможных ветвления по всем путям исполнения программы.

Во втором случае внутренняя структура и реализация нам не известна и не интересна, основной идеей или целью такого подхода есть задача определения того, что тестируемая система корректно взаимодействует с другими функциональными элементами сети и соответствует предъявляемым к ней требованиям с точки зрения спецификаций и функционального поведения [5].

Сейчас мы, в основном и опираясь на наши нормативно-правовые акты, проводим испытания программного обеспечения (ПО) и программно-аппаратных комплексов (ПАК) через модель «черный ящик». Несмотря на то, что это уже далеко не новая идея, она по-прежнему позволяет применять формально описанные модели для того, чтобы сделать процедуру исследований и испытаний более экономичной, понятной и прозрачной. Такой подход также может обеспечить ряд преимуществ еще на стадии разработки ПО и ПАК, отразить планируемое поведение системы в некотором конкретном окружении и конечно позволяет избавиться от многих проблем еще на ранней стадии разработки ПАК.

Но при всем этом многообразии видов и типов испытаний различного сетевого оборудования, мы можем заметить очевидные закономерности, и сказать о том, что так или иначе эти все испытания сводятся к испытаниям

на соответствие показателей, критериев, параметров, требований и норм изложенных в различных документах, таких как рекомендации ITU-T, IETF, IEEE, 3GPP, TMF и тп, или в наших отечественных нормативно-правовых документах, с построением или применением модельных сетей, что чрезвычайно важно, особенно при тестировании новых протоколов.

Применение модельных сетей также рекомендуется в Q.3900. Этой рекомендацией предусмотрено, что процесс тестирования включает два основных уровня: локальное тестирование средств NGN-EUT и тестирование комплексных решений NGN и реализуемых с их помощью услуг – NUT (*Network Under Test*) [6]. Локальное тестирование технических средств NGN, в свою очередь включает в себя:

Уровень 1.1 – Тестирование функциональных возможностей,

Уровень 1.2 – Тестирование под нагрузкой,

Уровень 1.3 – Тестирование на соответствие.

На уровне Тестирования NUT осуществляется:

Уровень 2.1 – Тестирование функциональных возможностей, реализованных в NUT (тестирование функциональных возможностей NUT,

Уровень 2.2 – Тестирование межсетевого взаимодействия,

Уровень 2.3 – Тестирование услуг в NUT,

Уровень 2.4 – Сквозное тестирование,

Уровень 2.5 – Тестирование качества обслуживания,

Уровень 2.6 – Тестирование мобильности и роуминга в NUT.

Подводя небольшой промежуточный итог: испытания проводились, да и сейчас осуществляются преимущественно в лабораторных условиях, даже в случае эмуляции различных тестовых ситуаций на сети, это все равно можно считать «лабораторными» условиями и модельными сетями.

Очевидно, что в современном мире такой подход уже не закрывает многих проблем, существующих на сети. Уже недостаточно провести испытания одного «черного ящика», во многих случаях необходимо смотреть на совместимость совершенно разнопланового, в частности, гетерогенного сетевого оборудования.

Конечно, вполне очевидное решение при таких вводных – это основываться на построении новых или комбинации уже существующих моделей, математических моделей и соответствующих прогнозах, виртуализации.

Оценить возможность применения к нашей задаче новых моделей и методов, таких как цифровые двойники, подходы к прогнозированию на базе нейронных сетей и теории хаоса.

Для таких моделей и прогнозов будет необходимо максимально учитывать суммарный образ сети, в некотором смысле сдвинуться от испытания каждого одного конкретного «черного ящика», в сторону тестирования в комплексном информационном поле.

Дополнением, а где-то может и альтернативой мы также рассматриваем подход, описанный в статье «Декомпозиция в испытаниях сетевых элементов NGN/пост-NGN» [7]. Речь идет о парадигме *рекурсивной декомпозиции* сетевой архитектуры на уровни, а потом на системы того же уровня, далее на подсистемы меньшего размера. Декомпозиция выполняется до тех пор, пока все подсистемы не окажутся отдельными программно-аппаратными или только программными сетевыми элементами, подпадающими под действие тех стандартов или иных нормативно-правовых актов.

Список используемых источников

1. Кучерявый А. Е., Гольдштейн Б. С. Сети связи пост-NGN. СПб.: БХВ-Петербург, 2013. 160 с.

2. Рекомендация Q.3900: Методы тестирования и архитектура модели сети для тестирования технических средств СПП применительно к сетям электросвязи общего пользования // МСЭ-Т, 09.2006.

3. Nam Hee Lee, Sung Deok Cha. Generating test sequences from a set of MSCs // Computer Networks. 2003. 42. pp. 405–417.

4. Гольдштейн Б. С., Крюков Ю. А., Хегай И. П., Шляпоберский В. Э. Интерфейсы СОРМ. Справочник по телекоммуникационным протоколам. Книга 7. СПб.: БХВ-Петербург, 2006. 160 с.

5. Luo, G. Bochmann, A. Petrenko, Test selection based on communication nondeterministic finite-state machines using a generalized Wp-method, IEEE Transactions on Software Engineering. 20 (1994). pp. 149–162.

6. Lee, D., Yannakakis, M. Principles and methods of testing finite state machines-a survey // Proceedings of the IEEE 84 (8) (19e6). pp. 1090–1123.

7. Зимин А. В, Ревенко Ю. П. Декомпозиция в испытаниях сетевых элементов NGN/пост-NGN // Актуальные проблемы инфотелекоммуникаций в науке и образовании. XI Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2022. Т. 1. (*В данном сб. статей*).

Статья представлена профессором кафедры ИКС СПбГУТ,
доктором технических наук, профессором Б. С. Гольдштейном.

УДК 621.397
ГРНТИ 49.33.29

ДЕКОМПОЗИЦИЯ В ИСПЫТАНИЯХ СЕТЕВЫХ ЭЛЕМЕНТОВ NGN/ПОСТ-NGN

А. В. Зимин, Ю. П. Ревенко

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Предложенный в статье подход к проведению испытаний, в том числе и сертификационных, сетевого оборудования базируется старом принципе divide et impera (разделяй и властвуй, лат.). В контексте данной статьи речь идет о парадигме рекурсивной декомпозиции сетевой архитектуры на уровни, а потом на системы того же уровня, а потом на подсистемы меньшего размера, причем декомпозиция выполняется до тех пор, пока все подсистемы не окажутся отдельными программно-аппаратными или только программными сетевыми элементами, подпадающими под действие тех или иных стандартов, рекомендаций или нормативно-правовых актов российской системы сертификации в области «Связь» [1].

Для унифицированных интерфейсов и стандартных протоколов взаимодействия этих сетевых элементов как раз необходим второй компонент предлагаемого подхода, это формализованное абстрактное описание функций, интерфейсов и протоколов элементарных сетевых элементов. Данный принцип дополняется объединением результатов декомпозиции в некоторые объединенные конечные автоматы поведения (ОКАП) для каждого сетевого элемента, позволяющим тестировать каждый такой сетевой элемент в отдельности.

MSC, ОКАП, КАП, NGN/IMS, декомпозиция.

Формализация тестирования сетевой архитектуры пост-NGN

Ниже предлагается подход к тестовым испытаниям с использованием сценариев на языке диаграмм последовательностей сообщений Message Sequence Charts (MSC), предусматривающий построение семантически эквивалентных конечных автоматов. Тестовые сценарии выражаются в виде последовательности сообщений, которыми должны обмениваться различные сетевые элементы.

Определяются условия активации сценария и назначения состояний для генерации только допустимых состояний и переходов. Тестовые последовательности состоят из последовательностей внешних входных событий, поскольку взаимодействие задач определяется внешними входными событиями и текущим состоянием системы. Как следствие, для генерации исполняемых тестовых случаев нам требуется описание глобального поведения

системы в виде набора MSC, каждый из которых выполняет тот или иной частичный сценарий из общего описания поведения глобальной системы и генерации тестовых последовательностей из GFSM (*Global Finite State Machine*). Ниже несколько слов о MSC.

Сценарии на языке MSC

В рамках рассматриваемой в статье методологии формализованные описания активно задействует спецификации в виде карт последовательностей сообщений MSC. При этом выполняется также и обратная задача перевода из абстрактных форм в MSC, что особо важно при испытаниях сетевых элементов NGN/IMS [2].

В контексте данной статьи важно подчеркнуть, что каждый компонент системы, участвующий в коммуникации, называется экземпляром и выполняется во времени строго последовательно вдоль временной оси. Все события вдоль каждой временной оси экземпляра полностью упорядочены, а сами события – это нечто либо отправляющее или принимающее сообщение, либо условие.

Математическая модель

Предлагаемую в статье абстракцию можно представить как некоторое формализованное обобщение функций, свойств и интерфейсов объектов, позволяющее воспринимать однотипные сетевые элементы разных производителей как если бы они были абсолютно идентичны. Для этого предлагается отделить существенные атрибуты от несущественных и формализовать описание этих существенных атрибутов [3].

Итак, события составляют конструкции типов «сообщение» (message), «условие» (condition) и «действие» (action), являющиеся элементами множеств E^m , E^c and E^A соответственно. «Ссылки» (reference) и другие подобные конструкции входят в множество E^l. Весь набор типов объектов, событий и меток представлен в множествах P, E and ∑, соответственно.

Структура набора спецификаций тестовых (сертификационных) испытаний *MSCs* описывается пятеркой (1)

$$\mathrm{MSCs} = (\mathrm{S}, s_0, \sum^R, n_r, \mathrm{Sr}), \quad (1)$$

где S – конечное множество сценариев, причем $s_0 \in S$ является сценарием верхнего уровня, $\sum^R$ – множество имен, n_r: $S \rightarrow \sum^R$ – отображение сценариев в этикетки, а $S_r = \{(s_1,s_2)|s_1,s_2 \in S\}$ – отношения между сценариями.

Каждый *сценарий MSC* описывается шестеркой (2)

$$\mathrm{Sp} = (\mathrm{Ps}, \mathrm{Es}, \sum \mathrm{s}, \mathrm{ps}, \mathrm{ls}, \langle \mathrm{s}), \quad (2)$$

где $\mathrm{Ps} \subseteq \mathrm{P}$ – конечное множество экземпляров (instances), $\mathrm{Es} \subseteq \mathrm{E}$ – конечное множество событий (events), $\sum \mathrm{s} \subseteq \sum \mathrm{s}$ – конечное множество этикеток (labels),: $\mathrm{Es} \to 2^{Ps}$– функция отображения каждого события в один или несколько экземпляров, $\mathrm{ls} : (\mathrm{Ps} \cup \mathrm{Es}) \to \sum \mathrm{s}$– функция присвоения этикетки каждому экземпляру и событию, $\langle \mathrm{s}: \cup \langle \mathrm{Ps} \cup \{(\mathrm{ms}, \mathrm{f}(\mathrm{ms}))|\mathrm{ms} \in E_s^M\}$ – отношение порядка между событиями, где $\langle p_s = \{(\mathrm{e1}, \mathrm{e2})|\mathrm{e1}, \mathrm{e2} \in \mathrm{E_s}\}$ описывает отношение порядка между экземплярами, а f ставит в соответствие получаемое событие отправляемому событию.

Спецификация автоматов поведения сетевых элементов

Конечная цель абстракций предыдущего раздела заключается в представлении основных MSC взаимодействия сетевых элементов в сети NGN/IMS в виде конечных автоматов поведения (КАПов), отображающих наиболее значимые тестовые сценарии процесса сертификационных испытаний этих сетевых элементов [4].

Конечный автомат поведения MSC определяется пятеркой (3)

$$\mathrm{КАП} = (\mathrm{Q}, \sum \mathrm{кап}, \delta, \mathrm{q0}, \mathrm{F}), \quad (3),$$

где Q – это конечны й набор состояний, определяемых в терминах индикаторов местоположения объекта, $\sum_{\mathrm{КАП}}=\mathrm{E_s}$ – это конечное множество событий, $\delta \subseteq \mathrm{Q} \times \sum_{\mathrm{КАП}} \sum \mathrm{кап} \times \mathrm{Q}$ – это множество переходов, $q_0 \in \mathrm{Q}$ является начальным состоянием, а $\mathrm{F} \in \mathrm{Q}$ – конечное состояние.

Обобщенный конечный автомат поведения (ОКАП), составленный из совокупности поведенческих автоматов того или иного сетевого элемента, прост в том, что все возможные пути и результирующие состояния идентифицируются рекурсивно. Мы используем переменные состояния и их значения таким образом, что переходы создаются только при изменении значений переменных состояния. Поэтому состояние в ОКАП определяется как набор значений переменных состояния системы. Аналогично, переход представляет собой упорядоченную последовательность сообщений, которыми необходимо обмениваться. Следует отметить, что при неупорядоченном и потенциально параллельном обмене сообщениями создаются множественные переходы.

Дадим последнее в этой статье формальное определение.

Обобщенный конечный автомат поведения ОКАП определяется четверкой (4)

$$\mathrm{ОКАП} = (\mathrm{Sокап}, \mathrm{Sокап0}, \sum \mathrm{окап}, \mathrm{Токап}), \quad (4)$$

где $S_{ОКАП}$ является конечным набором (множеством) состояний, $S_{ОКАП0} \in S_{ОКАП0}$ является начальным состоянием, $\sum_{ОКАП} = \langle E_1; E_2; \dots \rangle, E_i \in E^M$ это набор меток, и $T_{ОКАП} \subset S_{ОКАП} \times \sum_{ОКАП} \times S_{GОКАП}$ является конечным множеством переходов.

Пусть Z – область всех значений данных, тогда состояние ОКАП – это функция от множества переменных к множеству значений данных, $\delta : V \rightarrow Z$. Обозначим множество всех возможных состояний *States*, *States*: $2^{V \rightarrow Z}$, тогда набор состояний ОКАП является подмножеством *States*, где $S_{ОКАП} \subseteq States$. Чтобы убедиться, что число состояний ОКАП остается конечным, Z должен быть конечным по размеру. Поэтому в конструкциях "action (действия)" разрешается только присвоение явных значений данных.

Оставив за рамками данной статьи более глубокий анализ поведения MSC с помощью КАПов поясним основную их роль для процесса испытаний сетевых элементов. Она связана как раз с упоминавшийся выше временной осью, отношением порядка между экземплярами и соответствием получаемых событий отправляемым событиям. Так в качестве примера определим и назначим для MSC (рис. 1) неотрицательные и монотонно возрастающие индикаторы местоположения для каждого события, появляющегося в MSC. Например, на рис. 1 bMSC B1 находится в своем исходном местоположении [0,0,0,0] для каждого экземпляра. Если происходит событие i1, то система входит в местоположение [1,0,0,0].

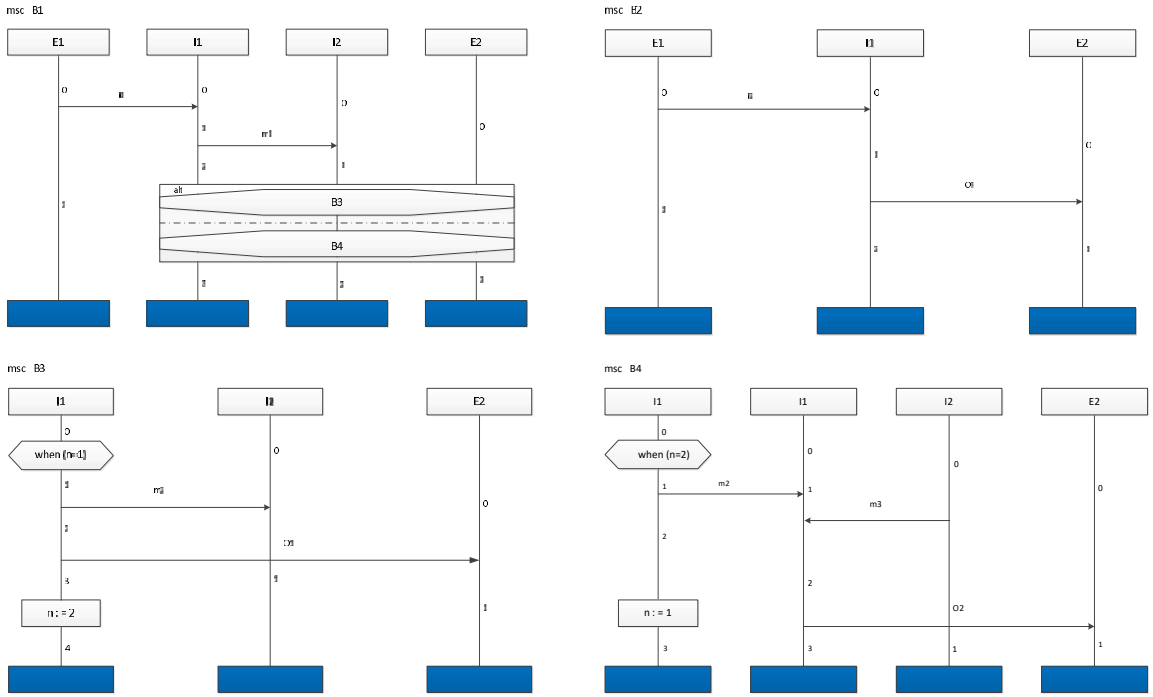


Рис. 1. bMSC B1, B2, B3, B4

Кроме того, в дополнение к обмену сообщениями, встроенное выражение "alt" в MSC B1 указывает, что после обмена двумя сообщениями выборочно должно быть выполнено либо MSC B3, либо MSC B4.

Фактически речь идет о назначении неотрицательных и монотонно возрастающих индикаторов расположения для каждого события, появляющегося в сценарии. Проиллюстрируем это примером на рис. 2.

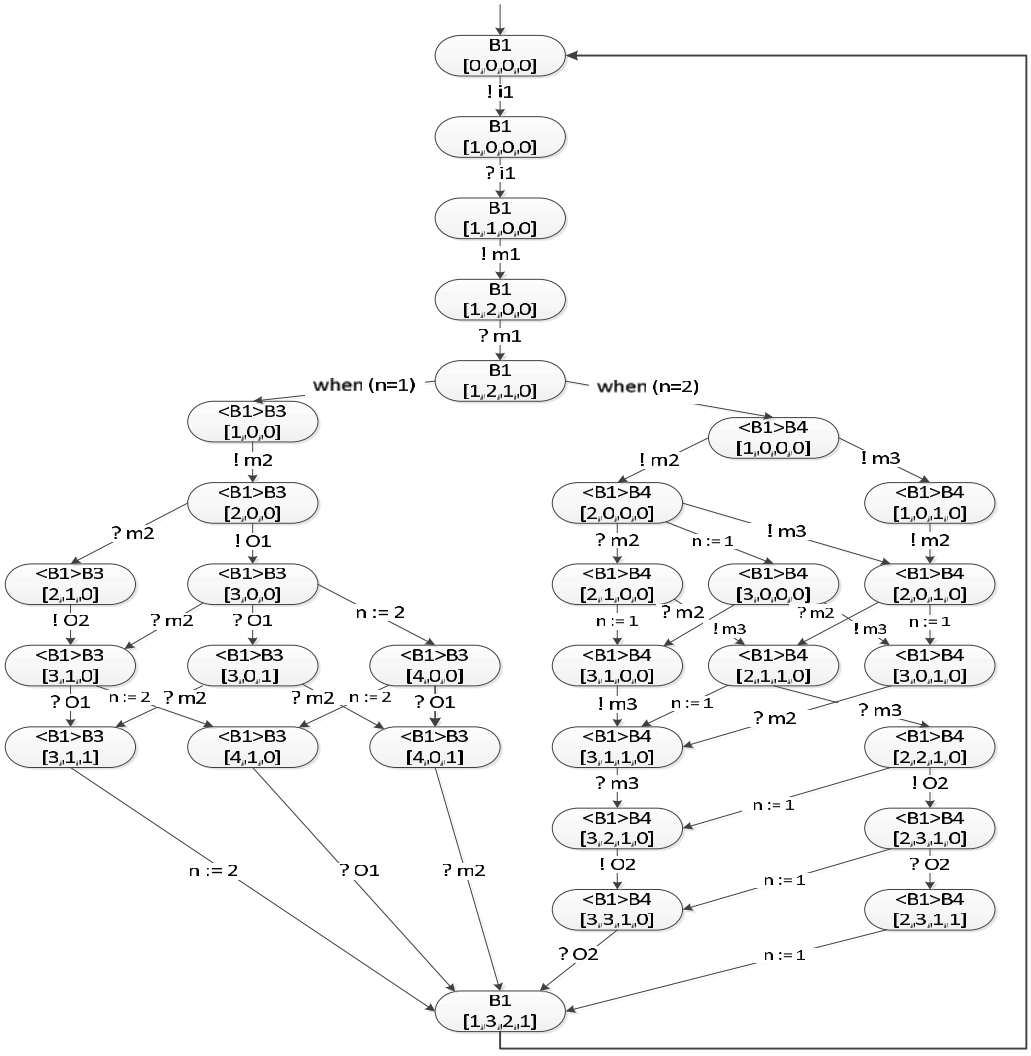


Рис. 2. Конечный автомат MSC B1

Пусть B1 находится в своем исходном местоположении [0,0,0,0] для каждого экземпляра. Если происходит событие i1, то система входит в местоположение [1,0,0,0]. Кроме того, КАП обрабатывает и различные встроенные (in-line) выражения. Но главное в нем синхронные условия конкатенации и активации: экземпляр I3 из MSC B4 не может отправить сообщение m3 до того, как будет оценено условие активации *when* ($n = 2$). Именно так КАП синхронизирует информацию о пути. Например, система переходит в состояние '(B1)B3[1,0,0]', когда значение 'n' равно 1.

Генерация тестовых последовательностей

На базе введенных выше КАПов и ОКАП последовательность испытаний можно легко получить, построив для набора событий путь, покрывающий диаграмму переходов. В предлагаемой модели КАПов проверочная последовательность необязательна, поскольку каждое состояние кодируется с учетом значения переменных состояния целевого ОКАП.

Поэтому достаточными являются два критерия покрытия. Первый требует, чтобы каждое состояние в ОКАП посещалось по крайней мере один раз, а второй – чтобы каждый переход посещался хотя бы один раз. Вместе они охватывают все комбинации условий активации экземпляров MSC.

Заключение

Предложенный в статье подход апробирован в процессе тестирования и сертификационных испытаний ряда сетевых элементов NGN/IMS, выполнявшихся в испытательном центре СПбГУТ, и доказал свою эффективность.

Вместе с тем было обнаружено уязвимое звено в предложенном подходе. Несмотря на простоту предложенного метода, в некоторых ситуациях он перестает быть практичным из-за проблемы лавинообразного роста числа состояний (всплеска состояний) при объединении ряда MSC в ОКАП. Решением этой проблемы является дополнение предложенной модели элементами, базирующимися на сетях Петри и позволяющих упростить кодирование событий при больших разбросах значений переменных состояния. Последнее является предметом дальнейшей работы.

Список используемых источников

1. Кучерявый А. Е., Гольдштейн Б. С. Сети связи пост-NGN. СПб: БХВ-Петербург, 2013. 160 с.

2. Nam Hee Lee, Sung Deok Cha. Generating test sequences from a set of MSCs // Computer Networks. 2003. 42. pp. 405–417.

3. Luo, G. Bochmann, A. Petrenko, Test selection based on communication nondeterministic finite-state machines using a generalized Wp-method // IEEE Transactions on Software Engineering. 20 (1994). pp. 149–162.

4. Lee, D., Yannakakis, M. Principles and methods of testing finite state machines-a survey // Proceedings of the IEEE 84 (8) (19e6). pp. 1090–1123.

Статья представлена профессором кафедры ИКС СПбГУТ, доктором технических наук, профессором Б. С. Гольдштейном.

УДК 621.391.52
ГРНТИ 49.41.01

АНАЛИЗ МЕТОДОВ СЕТЕВОЙ СТЕГАНОГРАФИИ С ИСПОЛЬЗОВАНИЕМ SCTP-ПРОТОКОЛА

Б. Г. Ибрагимов[1], **К. М. Тахирова**[2]

[1]Азербайджанский Технический Университет

[2]Военная академия Вооруженных сил Республики Азербайджан

В данной работе рассмотрены важные для практического использования вопросы сокрытия информации смешанного типа в текстовых документах, вопросы сетевой стеганографии, методы и алгоритмы скрытия данных. Частично, в статье исследован метод стеганографической защиты информации, позволяющий повысить устойчивость к информационным атакам в системах телекоммуникации. Проанализированы методы сетевой стеганографии для скрытия данных с использованием механизмов SCTP–протокола (Транспортный протокол с контролем пакетов), передаваемого по каналам связи.

сетевая стеганография, скрытый канал, SCTP, пропускная способность, полезный и служебный пакет, стоимость стеганографии, скрытия данных.

В настоящее время глобальное распространение и постоянное совершенствование телекоммуникационных систем на базе архитектурных концепции NGN (*Next Generation Network*) и FN (*Future Network*) с использованием транспортных протоколов сопровождается ростом их пропускной способности, интеграцией мультимедийных услуг и приложений [1, 2].

На основе исследования установлено [3–5], что методы сетевой стеганографии можно разделить на три большие группы, среди которых важное место занимают методы сетевой стеганографии. Сущность метода заключается в изменении данных в полях заголовков сетевых протоколов и в полях полезной нагрузки пакетов. Эти методы базируются на методах изменения данных в полях заголовков протокола и механизма, где они основаны на модификации полей заголовков IP (*Internet Protocol*), TCP (*Transmission Control Protocol*) и SCTP пакетов [6–8].

Следует отметить, что сетевая стеганография для скрытия данных, которые передаются по каналам связи с использованием методов изменения данных в полях заголовков протокола, состоит из двух полезных $L_{\text{nn}}(\lambda_i)$ и служебных $L_{\text{cn}}(\lambda_i)$ пакетов:

$$L_n(\lambda_i) = L_{\text{nn}}(\lambda_i) + L_{\text{cn}}(\lambda_i) + L_{ck}(\lambda_i), \qquad i = \overline{1,n}\ , \tag{1}$$

где $L_n(\lambda_i)$ общая длина передаваемого пакета, которая состоит из длины полезного $L_{nn}(\lambda_i)$ и служебного пакетов $L_{cn}(\lambda_i)$, а также длины скрытия передаваемого пакета $L_{ck}(\lambda_i)$ с интенсивностью входящего потока пакетов λ_i информации смешанного типа $i=\overline{1,n}$.

В мультисервисной телекоммуникационной сети связи имеется передающая сторона А (Алиса) и принимающая сторона В (Боб). В их распоряжении имеется множество каналов связи, которые описываются следующим образом:

$$N_k(b_i,t)=\sum_{i=1}^{n}[N_{nk}(b_i,t)+N_{ck}(b_i,t)]+N_{\text{ш}}(t),\quad i=\overline{1,n}\ , \qquad (2)$$

где $N_{nk}(b_i,t)$ – скрытые сетевые информационные каналы связи, с помощью которых передаются полезный пакет трафика, $N_{nk}(b_i,t)=U[b_i,t,\lambda_i]$; $N_{ck}(b_i,t)$ – скрытые сетевые информационные каналы связи, с помощью которых передаются служебный пакет трафика (сигнальное поле, шум, дезинформация, ключи, синхронное поле и др.); $N_{\text{ш}}(t)$ – источники шумов.

Скрытый канал может существовать в любом открытом канале, в котором существует некоторая избыточность. Скрываемые информации смешанного типа называются стеганограммой. Они располагаются в определенном физическом носителе. В сетевой стеганографии роль носителя выполняют передаваемые по сети телекоммуникации пакеты [8].

Учитывая вышеизложенные методы сетевой стеганографии, интересным представляется также направление с использованием механизмов SCTP – протокола [1, 8].

В данном случае, протокол SCTP-стенография использует новые характерные особенности данного протокола, такие как мультипоточность и использование множественных интерфейсов (Multi-Homing).

Методы изменения содержимого протокола SCTP-пакетов основаны на факте, что каждый SCTP-пакет состоит из частей и каждая из этих частей может содержать переменные параметры. Вне зависимости от реализации статистический анализ адресов сетевых карт, используемых для пересланных блоков, может помочь в обнаружении скрытых связей. Устранение возможности применения данного метода стеганографии может быть достигнуто путем изменения адреса отправителя и получателя в случайно выбранном пакете, который содержится в повторно высылаемом блоке [1, 6, 7].

Модификация пакетов с использованием гибридного метода может быть представлена на примере системы HICCUPS (*Hidden Communication*

System for CorrUPted Networks), которая использует несовершенства передачи данных в сетевом окружении, такие как помехи и шум в среде канала связи, а также обычную подверженность данных к искажению [1].

В данном случае анализируемая система является стенаграфической системой с распределением пропускной способности в общественной сетевой среде или в канале связи. Данная система для беспроводных сотовых сетей более восприимчива к искажению данных, чем проводные, поэтому использование помех и шума в канале связи во время работы системы выглядит очень заманчиво [1, 2, 9].

Для прослушки всех кадров с передаваемыми данными в среде телекоммуникации и возможность отправки поврежденных кадров с неправильно откорректированными кодовыми значениями – две важные сетевые особенности, необходимые для реализации HICCUPS.

В частности, беспроводные мобильные сети используют воздушное соединение с переменной частотой ошибок в битах $P_{BER}(\lambda_i)$ (BER), что создает возможность вводить искусственно поврежденные кадры. Этот метод обладает низкой полосой пропускания $\Delta F_k \to \min$, громоздкой реализацией, низкой стенографической стоимостью и высокой сложностью обнаружения. Тем не менее, анализ кадров с неверной контрольной суммой может привести к обнаружению использования данного метода.

Учитывая выше перечисленные методы, основные характеристики сетевой стеганографии при передаче и приеме потоков пакетов с интенсивностью λ_i определяются следующими параметрами:

● Пропускная способность скрытого канала связи, $C_{nc}^{ck}(\lambda_i, t)$, $i = \overline{1,n}$, эта есть объем секретных данных $I_{cd}(\lambda_i, t)$, который может быть отправлен в единицу времени T_c и равно

$$C_{nc}^{ck}(\lambda_i, t) = F[N_k, I_{cd}(\lambda_i, t), T_c], \quad i = \overline{1,n}, \tag{3}$$

Здесь T_c – длительность сообщения, содержащие скрытые и полезные информации.

● Вероятность обнаружения всех частей сообщения пакетов трафика, которые существуют во всех (полезных и служебных) каналах связи $\mathrm{P}_{\text{во}}^{kc}(\lambda_i)$ определяется следующей функциональной зависимостью

$$\mathrm{P}_{\text{во}}^{kc}(\lambda_i) = E[\rho(\lambda_i),\, L_{nk}(\lambda_i)], \quad i = \overline{1,n}, \tag{4}$$

Здесь $L_{nk}(\lambda_i)$ – длина пакета контейнера, которая несет секретные данные; $\rho(\lambda_i)$ – средняя загрузка канала передачи сообщений с учетом скорости обслуживания скрытого канала связи μ_i выражается как:

$$\rho(\lambda_i) = \frac{\lambda_i}{N_k \cdot \mu_i} \le 1, \quad i = \overline{1,n} \tag{5}$$

● Экономическая эффективность стеганографической стоимости системы $C_{\text{эс}}^{\text{сс}}(\lambda_i)$, $i = \overline{1,n}$.

С учетом формулы (3), (4) и (5) получим функциональную зависимость, определяющую качество функционирования системы стеганографии при передаче и приеме потоков пакетов на базе методов модификации сетевой стеганографии:

$$Q_{\text{КФ}}^{\text{СС}}(\lambda_i) = W[C_{nc}^{ck}(\lambda_i, t), \text{P}_{\text{во}}^{kc}(\lambda_i), C_{\text{эс}}^{\text{сс}}(\lambda_i)], \quad i = \overline{1,n}\ , \tag{6}$$

Выражение (6) характеризует эффективность функционирования, используемое методы сетевой стеганографии с учетом показателей метода сокрытия информации в текстовых документах при использовании механизмов SCTP–протокола. Кроме того, данная зависимость определяет основные параметры методов сетевой стеганографии, которые позволяют осуществлять сравнение с помощью показателей методов сетевой стеганографии, как пропускной способности стеганографии, сложности обнаружения так и стоимости стеганографии.

Учитывая важность создания и исследования новых методов сетевой стеганографии для скрытия данных, передаваемых по каналам связи необходимо проанализировать методы SCTP-стеганографии с учетом показателей выражения (6), которым в докладе будем уделять большое внимание.

Таким образом, в докладе также будем рассматривать сравнительные анализы методов сокрытия информации смешанного типа в текстовых документах по их основным характеристикам и реализации, с помощью которых можно сделать вывод о прямой зависимости основных характеристик друг от друга.

Список используемых источников

1. Рябко Б. Я., Фионов А. Н. Основы современной криптографии и стеганографии. 2-е изд. М.: Горячая линия – Телеком, 2020. 232 с.

2. Шелухин О. И., Рыбаков С. Ю., Магомедова Д. И. Скрытие информации в аудиосигналах с использованием детерминированного хаоса // Наукоемкие технологии в космических исследованиях Земли. 2021. Т. 13. № 1. С. 80–91.

3. Ибрагимов Б. Г., Тахирова К. М. Анализ показателей информационной безопасности на базе технологии сетевой стеганографии // Актуальные проблемы инфотелекоммуникаций в науке и образовании. X Юбилейная Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2021. Т. 1. С. 411–416.

4. Конахович Г. Ф., Пузыренко А. Ю. Компьютерная стеганография. Теория и практика. К.: МК-Пресс, 2006. 288 с.

5. Ибрагимов Б. Г., Тахирова К. М. Некоторые вопросы защиты информации в системе телекоммуникации с использованием цифровой стеганографии // Материалы Международной НТК «Инновационные технологии в телекоммуникации». АзТУ (4-6 декабр), Баку, 2019. С. 30–32.

6. Грибунин В. Г., Оков И. Н., Трунцев И. В. Цифровая стеганография. М.: Солон-Пресс, 2009. 272 с.

7. Коржик В. И., Флаксман Д. А. Система цифровых водяных знаков с возможностью их извлечения из бумажных копий цифровых документов // Труды учебных заведений связи. 2019. Т. 5. No 3. С. 75–85.

8. İbrahimov B.G., Tahirova K. M. Analysis some aspects steganography methods in integrated service digital networks // The Second Karabakh War as a new generation warfare Republic of Azerbaijan. The War College of the Armed Forces (October 21–22), Baku. 2021. pp. 97–99.

9. Аграновский А. В., Балакин А. В., Грибунин В. Г., Сапожников С. А. Стеганография, цифровые водяные знаки и стегоанализ : монография. М.: Вузовская книга, 2009. 220 с.

УДК 004.7
ГРНТИ 49.33.29

АНАЛИЗ ПРИМЕНЕНИЯ ТЕХНОЛОГИЙ TIME SENSITIVE NETWORK В СЕТЯХ СВЯЗИ ПЯТОГО ПОКОЛЕНИЯ

И. О. Игнатова, Р. В. Киричек

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Технология Time Sensitive Network (TSN) становиться стандартом для конвергентных сетей Промышленности 4.0 благодаря своей способности поддерживать детерминированные требования к задержке. Однако она не может обеспечить необходимую гибкость для поддержки мобильных промышленных приложений, необходимых для заводов будущего. Этого можно добиться за счет интеграции TSN с сетью 5G/IMT-2020, поскольку она была разработаны для поддержки сверхнадежной связи с малой задержкой. Это вызвало значительный интерес к интеграции сетей 5G/IMT-2020 и TSN, и были определены первые рамки для такой интеграции. Однако работа находится на ранней стадии, и решения для эффективной интеграции двух сетей, чтобы 5G/IMT-2020 мог поддерживать уровни QoS TSN, еще предстоит разработать. В данной статье представлен обзор технологий TSN и 5G/IMT-2020, а также концепт их совместной работы.

TSN, IEEE, 5G/IMT-2020, IIoT.

Введение

Будущие умные фабрики будут обеспечивать как беспроводную, так и проводную связь между всей производственной линией, чтобы обмениваться данными и принимать решения автономно. Для достижения этой парадигмы ключевое значение будет иметь высоконадежная и детерминированная связь. Чувствительная ко времени сеть (TSN), основанная на технологии Ethernet, разрабатывается для обеспечения детерминированной, сверхнадежной связи в реальном времени. Однако TSN не может гарантировать гибкость, необходимую предприятиям будущего для поддержки мобильности в некоторых промышленных приложениях. Беспроводные технологии могут исправить этот недостаток, и интеграция TSN с беспроводными технологиями будет иметь ключевое значение. Сети 5-го поколения (5G/IMT-2020) считаются одним из лучших вариантов для поддержки парадигмы Индустрии 4.0, поскольку они были разработаны для обеспечения сверхнадежной связи с малой задержкой (URLLC).

Технология Time Sensitive Network (TSN)

В наше время сложно представить производство, на котором не используется оцифровка всех данных с аналоговых датчиков и передача их в систему управления. Такой подход получил название Индустрия 4.0 или Промышленный Интернет вещей (IIoT). [1]

Time-Sensitive Networking (TSN) – это набор расширений технологии Ethernet, созданием которого занимается рабочая группа IEEE 802.1Q. TSN представляет собой набор стандартов, которые в основном касаются улучшения сетевого взаимодействия на канальном уровне модели OSI.

Сеть TSN состоит из конечных устройств, которые являются источниками и получателями потоков TSN, а также мостов, которые являются коммутаторами Ethernet, их функция – передавать и получать кадры Ethernet потока TSN по расписанию.

Стандарт TSN IEEE 802.1Qcc [2] определяет три модели управления сетью: полностью распределенную модель, централизованную модель сети и распределенных пользователей и полностью централизованную модель. Здесь мы уделим внимание централизованной модели, поскольку именно она позволяет наиболее эффективно использовать сетевые ресурсы.

В этой модели мосты TSN передают свои сетевые возможности и информацию об активной топологии узлу CNC (централизованная сетевая конфигурация). Конечные станции отправляют свои требования к потоку TSN узлу CUC (централизованной конфигурации пользователя), который пересылает эту информацию в CNC (CUC может адаптировать эти требования к потоку TSN для конечной станции перед их пересылкой в CNC); тогда

ЧПУ имеет полное представление о сети TSN и может определить конфигурацию каждого моста (например, планирование) для выполнения требований потока TSN. ЧПУ может отправить определенную информацию о конфигурации TSN на CUC, который может отправить информацию о конфигурации на конечные станции.

TSN использует планировщик Time Aware Shaper (TAS) в IEEE 802.1Qbv для гарантии передачи детерминированного трафика с высоким приоритетом в ограниченное время. С этой целью трафик Ethernet делится на разные классы (может быть до 8 классов трафика, а также Best Efforts (BE) – класс трафика по умолчанию). Для каждого моста и выходного порта планировщик TAS устанавливает временной интервал, в течение которого каждый класс трафика имеет доступ к каналу, чтобы удовлетворялись временные требования к высокоприоритетному трафику. Когда данные поступают на мост TSN, они перенаправляются на соответствующий выходной порт. Данные классифицируются по разным очередям в зависимости от класса трафика. Для поддержки планирования TAS все узлы в сети синхронизируются с использованием одного главного и нескольких подчиненных часов, как определено в стандарте IEEE 802.1AS [3].

Беспроводная сеть 5G/IMT-2020

Система 5G/IMT-2020 (5G/IMT-2020S) состоит из двух основных сетевых компонентов: сети радиодоступа (RAN) и базовой сети (CN). RAN включает в себя UE (пользовательское оборудование) и gNB (узел B нового поколения). 5G/IMT-2020 CN отличается высокой гибкостью и состоит из ряда независимых сетевых функций для плоскости пользователя (UP) и плоскости управления (CP) [4].

UP передает сетевой пользовательский трафик, а CP передает сигнальный и управляющий трафик. UPF (функция плоскости пользователя) обрабатывает восходящий путь между gNB и внешней сетью передачи данных (например, сетью TSN). В плоскости управления SMF (функция управления сеансом) взаимодействует с пользовательской плоскостью для установления или изменения сеансов PDU (блок данных протокола), которые определяют услуги подключения между UE и сетью передачи данных. PCF (функция управления политикой) предоставляет правила политики для SMF. AF (функция приложения) взаимодействует с PCF для управления политикой и может влиять на маршрутизацию трафика в UP. Схема сети представлена на рис. 1.

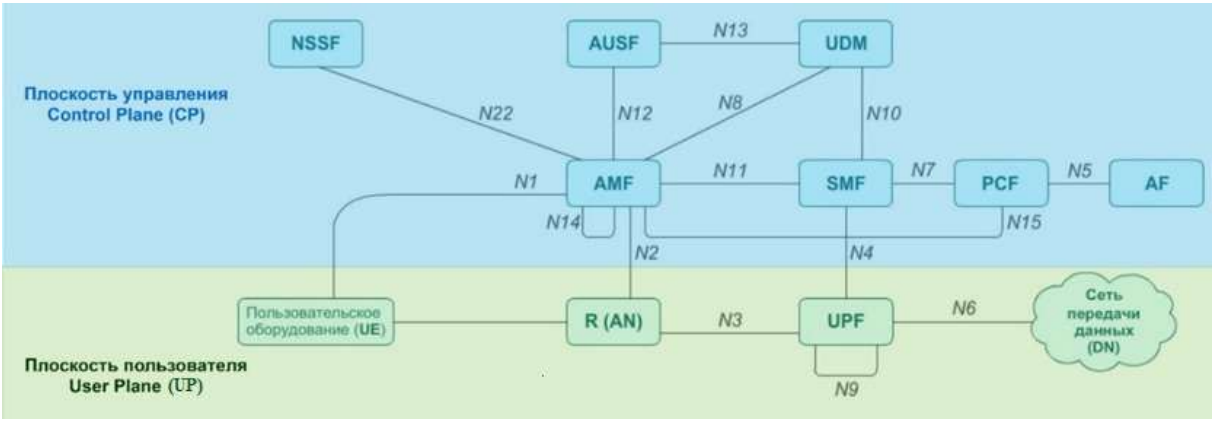


Рис. 1. Компоненты сети 5G/IMT-2020

Для поддержки связи с малой задержкой 5G/IMT-2020 сокращает время обработки в UE и gNB, определяет более гибкие структуры кадров и использование более коротких интервалов передачи на основе различных нумерологий. Эти нумерологии представляют интервал между поднесущими и приводят к временным интервалам от 1 до 0,0625 мс. Возможна передача только с использованием части слота, называемого минислотом. Другим ключевым аспектом сокращения задержки является определение планирования, когда gNB предварительно выделяет ресурсы для UE. Когда UE хочет передать, ему не нужно запрашивать ресурсы у gNB (пропуская задержку, связанную с этим процессом), и оно может передавать данные немедленно.

Интеграция TSN и 5G/IMT-2020

Адаптированная интеграция TSN в 5G/IMT-2020 была определена как наиболее жизнеспособное решение для достижения производительности, необходимой для промышленных приложений. Основная идея состоит в том, чтобы создать модель черного ящика, в которой система 5G/IMT-2020 выглядит как мост TSN с внешней сетью TSN, но внутри использует собственную структуру для передачи кадров TSN. Схема такого решения представлена на рис. 2.

Поскольку TSN является стандартом Ethernet, система 5G/IMT-2020 должна иметь возможность передавать кадры Ethernet. Вместо использования IP-адресов для определения источника и назначения трафика в сети 3GPP в этом типе сеанса PDU используются MAC-адреса. Конечные точки этого сеанса поддерживают наборы фильтров пакетов, которые могут считывать кадры Ethernet, включая их теги VLAN, и определять необходимую информацию, такую как маршрутизация и тип трафика. Чтобы различать классы трафика, 5G/IMT-2020 использует свою внутреннюю структуру QoS. Эти потоки можно отличить по их соответствующему идентификатору потока QoS 5G/IMT-2020 (5QI).

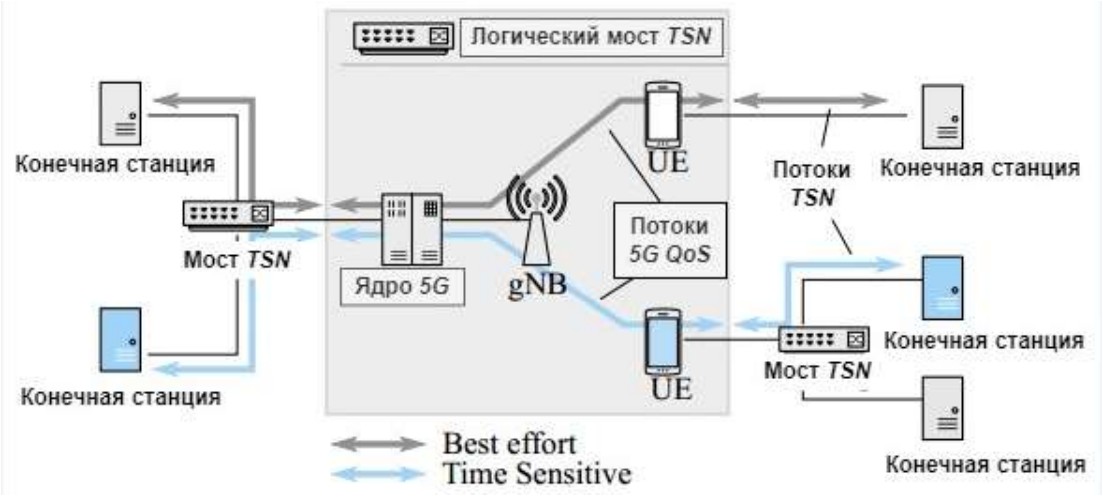


Рис. 2. Логический мост TSN 5G/IMT-2020

Поддержка трафика Ethernet, гарантированная сквозная производительность и синхронизация времени обеспечивают необходимые средства для своевременной доставки трафика TSN через 5G/IMT-2020. Еще одним важным аспектом является настройка моста TSN. Для этого сеть 5G/IMT-2020 должна предоставлять интерфейс конфигурации, который может, с одной стороны, раскрывать ее возможности и текущее использование, а с другой – считывать и применять конфигурации TSN. Эта концепция изображена на рисунке 3, где транслятор TSN направляет запросы конфигурации TSN в необходимые сетевые функции 3GPP для установления и настройки соответствующих сквозных потоков QoS 5G/IMT-2020.

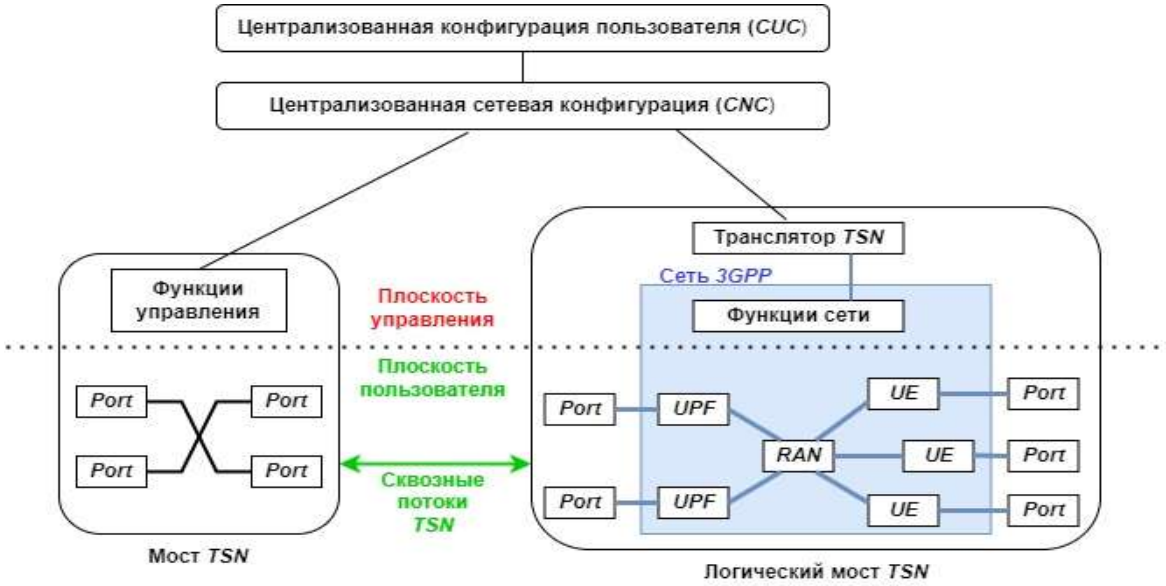


Рис. 3. Модель централизованной конфигурации интегрированной сети

При наличии этих функций система 5G/IMT-2020 способна поддерживать основные задачи транспортировки и настройки TSN. Другие стандарты

TSN могут быть рассмотрены для дальнейшего усовершенствования беспроводной реализации. Например, IEEE 802.1CB, обеспечивающий репликацию и устранение кадров, может повысить надежность за счет сквозного расширения избыточности в сети TSN. Однако надежность 5G/IMT-2020 сильно зависит от состояния беспроводного канала и требует дальнейшего изучения, чтобы можно было эффективно использовать его [5].

Вывод

Результаты показали, что поддержки функций TSN только в 5G/IMT-2020 недостаточно для обеспечения необходимой производительности, требуемой TSN. В зависимости от конфигурации приложения и времени между поступлениями кадров, принадлежащих к разным потокам, предоставляемые сервисные гарантии по надежности и задержке сильно различаются. Чтобы добиться возможной интеграции TSN в 5G/IMT-2020, необходимо применение сквозного для эффективного назначения ресурсов на общих проводных и беспроводных каналах для соответствующих потоков. Для будущего внедрения систем 5G/IMT-2020 с поддержкой TSN в заводской среде, необходимо дальнейшее исследование, настройка и планирование для полной интеграции 5G/IMT-2020 и TSN.

Список используемых источников

1. Москаленко Т. А., Киричек Р. В., Бородин А. С. Архитектуры промышленного интернета вещей // Информационные технологии и телекоммуникации. 2017. Т. 5. № 4. С. 49–56.

2. IEEE, IEEE 802.1Q: Standard for Local and Metropolitan Area Networks--Bridges and Bridged Networks. 2018.

3. IEEE, IEEE 802.1AS: Standard for Local and metropolitan area networks--Time and Synchronization for Time-Sensitive Applications in Bridged Local Area Networks. 2011.

4. 3GPP; Technical Specification Group Services and System Aspects; System architecture for the 5G/IMT-2020 System (5G/IMT-2020S) Stage 2 (Release 16) 3GPP TS 23.501 V16.4.0, March, 2020.

5. Analysis of Multi-user Scheduling in a TSN-enabled 5G/IMT-2020 System for Industrial Applications, David Ginthör, Johannes von Hoyningen-Huene, Ren´e Guillaume, Hans D. Schotten, Robert Bosch GmbH, IEEE International Conference on Industrial Internet (ICII), 2019.

УДК 004.418
ГРНТИ 28.17.33

ОБЛАЧНЫЕ ТЕХНОЛОГИИ, НА ПРИМЕРЕ FLIGHT SIMULATOR, ИГРЫ И ФОТОРЕАЛИЗМ

А. А. Ильин, А. Д. Михайлин, А. А. Поручиков, А. А. Шишкин

Военная орденов Жукова и Ленина Краснознаменная академия связи
имени Маршала Советского Союза С. М. Буденного

Данная статья посвящена обзору применений облачных технологий на примере симулятора Microsoft Flight Simulator, необходимый бюджет для реализации небольших проектов с применением облачных технологий, реализация облачных вычислений на примере создание 3D сцены на основе фотографий. Рассматривается влияние использования в играх, примеры реализации, а, так же анализ дальнейшего развития облачных технологий в различных сферах.

облачные технологии, геоданные, графика.

Вышел первый за многие годы симулятор *Microsoft Flight Simulator* далее (*MFS*) [1], которую смело можно называть технологической революцией, которая заключается в том, что она первая в мире показала на что способны облачные технологи [2] в нем максимально детализировано изображена целая планета 3 000 терабайт одних только геоданных. Поэтому каждый новичок, который оказывается в игре и сразу отправляется посмотреть на свой город, и пытается там отыскать свою улицу и дом. И что характерно находят. Но многих достопримечательностей в игре нету. Например, красной площади там нету, только тень от храма Василия Блаженного, но найти хрущевку в самой глухой провинции шанс почти 100 %. Не всегда всё будет соответствовать реальности, но свой дом в симуляторе вполне себе реально найти.

Все дело в системе автоматической генерации карт, уникальные объекты она не понимает поэтому статуя родины матери, здесь превращается в небоскреб, а римский Колизей становиться жуткой круглой тюрьмой без окон. Зато обычные многоэтажные здания система воспроизводит просто отлично, какой бы формы они не были.

Был случай, когда частники выкупили частный самолет и превратили его в отель там система решила, что это обычный дом и сделала в форме самолета. И та же история произошла с экспонатами в авиа музей русской авиации в Монино, так же разработчики воплотили в симуляторе множество других мелочей можно отмотать время и полюбоваться на затмение, или

наоборот посмотреть какая сейчас погода на другом конце земли, потому что данные по ветру облачности и осадкам собираются в реальном времени. Например, если вы в новостях прочитали что где-то идет ураган, можете слетать в симуляторе и посмотреть, как он выглядит (рис. 1, 2).

Рис. 1. Супер ураган в симуляторе, вид из кабины пилота

Рис. 2. Супер ураган в симуляторе, вид от 3 лица

В целом в генератор ландшафта в симуляторе работает на высоком уровне [3], люди увлечены тем, что пытаются сделать в симуляторе копии реальных снимков, и порой выходит на удивление похоже на рисунке представлены знаменитое фотообои, которые был использован как стандартный рабочий стол для операционной системы *Windows XP* (рис. 3). И оказалось, что с тех пор там разбили виноградники, так что красивой зеленной травы

увы не осталось. Моей целью показывать такие детальные примеры, для понимания что технологии сами по себе это такие бездушные вещи, но в симуляторе их используют для того, чтобы создавать истории и вызывать эмоции. Давая пользователю цель, давать ему бесконечный просмотр для исследования, именно такие вещи необходимы для любого симулятора, который претендует на симулятор высокого статуса.

В *MFS* нету сюжета это очень сложный и нишевый проект, но благодаря одной крутой технологии он превратился в весьма такой массовый хит, способный увлечь даже людей не увлекающихся пилотированием самолетов. Разработчики этого проекта наглядно показали на своем детище, что процедурная генерация может использоваться не только в инди играх, чтобы сэкономить на создании различных игровых предметов и ландшафтов. По мнению разработчиков, процедурная генерация станет одним из главных двигателей симуляторов в ближайшем будущем.

Рис. 3. Сравнение фотографий рабочего стола для операционной системы *Windows XP* и тоже самое место, реализованное в симуляторе *MFS*.

Сейчас в большинстве симуляторов с открытым миром локации сравнивая с *MFS* являются несоизмерима меньше. Чем лучше становиться графика, тем меньше становиться игровые локации, потому что создание каждого квадратного километра начинает обходиться все дороже и дороже. Есть всего 2 пути вырваться из этой ловушки. Переложить задачу создания на компьютеры, потому что они быстрые или на игроков, потому что их много, часто в симуляторах самими игрокам дается возможность самим воздвигать дома, изменять ландшафт и прочее.

Возникает вопрос, а где хранить созданные миры, *Microsoft* для данного проекта приходится содержать 3 000 терабайт данных, раздавая их всем по первому требованию. Хотя обычный винчестер у пользователя это 0,5–2 терабайта. *Microsoft* может себе позволить содержать такие сервера [4], так как компания не только очень богата, она еще одна из крупнейших компаний на рынке облачных сервисах, с ней могут соперничать только *Google* и *Amazon*, так что серверов у нее в избытке.

А вот как быть простым разработчикам, могут ли они вообще использовать такие технологии и сколько вообще это стоит. Сама *Microsoft* понятное дело этого не рассказывает, но это и не нужно. Потому что еще пару лет

назад русский программист Роман Шувалов выпустил свой проект *Generation streets*. Она делает тоже самое что и *MFS* сгенерировала локацию в целую планету, на которой можно найти собственную улицу или дом. Конечно, разработчику не хватало спутниковых снимков, которые бы обрабатывали искусственным интеллектом, ему не помогало куча художников и модельеров. Но в целом технологии были те же. Ему точно также пришлось запустить сервер что бы игра брала с него данные по ландшафту и строения и это удовольствие обходилось ему в 6 евро в месяц. Хотя и ему не нужно хранить постоянно 3 000 терабайт, но в целом это не какая-то секретная технология доступная лишь *Microsoft*, а вполне обычная вещь, которую могут использовать даже нишевые разработчики.

Но на данный момент студиям проще и выгодней записывать все на жесткие диски игроков, но размеры клиентов уже начали переваливать в отметку в 200 гигабайт. Прямо сейчас та же *Microsoft* начинает предлагать альтернативу [5], в виде оперативной погрузки нужных файлов прямо из интернета. В духе если пользователь давно не пользовался программой, то часть проекта удаляется, а при первом требовании быстро подгружается.

Генерация локаций – это хорошо, экономия места тоже, но что там с улучшением картинки, когда уже обещанная революция нагрянет? И вот тут самое время рассказать про китайский проект *black myth wu kong*, многие видели игровой процесс и задались вопросом это и есть следующее поколения уровня графики в играх? Локации линейны и небольшие модели вполне себе обычные, освещение очень качественное. Лишь малое взаимодействие с окружением уровень интерактивности довольно низкий. Сейчас все стремятся к картинке фотореализма, но возможно наступит время, когда фотореалистичная графика станет самой простой и дешевой, а мультипликационный стиль графики станет самым сложным и дорогим. А все, потому что технологии фотограмметрии развиваются не по дням, а по часам. Хотя фотограмметрия работает только с небольшими объектами и нужно специальное оборудование чтобы все получилось качественно. Однако *Intel* создает инструмент способный делать копии реальной местности всем, у кого есть в руках фотоаппарат. Раньше уже такое попытались сделать, но трехмерные сцены получались просто кошмарного качества со сплошными артефактами. Специалисты *Intel* нашли решение они сперва создают грубую трехмерную сцену, далее происходит заливка цветом, и на основе нейросетей создается качественная *3D* модель, расставляются тени блики и множество мелки деталей (рис. 4).

А затем обрабатывают её с помощью нейронной сети. Разработчики считают, что подобные технологии позволят создавать симуляторы неотличимые от реальности, потому что в них графика будет трехмерном вариантом фотографии. Команда разработчиков уверяет, что когда-нибудь они смогут обучить систему работать даже с подвижными объектами. Просто

себе представьте сейчас отдельно записывают движения, модели и текстуры, но все идет к тому, что все это можно будет делать одновременно. Целиком перенося в симулятор виртуального двойника актера.

Рис. 4. Этапы создания *3D* модели на основе фотографий

Фотореализм постепенно перестает быть недосягаемой вершиной. Уже виден путь к нему, появляются первые инструменты для его достижения, поэтому за перспективы развития графики можно не беспокоиться. И так же виден путь решения проблемы бюджетов автоматизации процесса разработки и машинная генерация контента. В целом индустрия готова к новому скачку, такому же который начался с выхода игры *Doom* в 1993 году и продолжался около 10 лет. Но вот конкретное время, когда состоится этот скачок, пока сложно сказать.

Список используемых источников

1. История Microsoft Flight Simulator. URL: https://itc.ua/articles/microsoft-flight-simulator-nebo-eto-svoboda/ (дата обращения: 01.02.2022).

2. Что такое облачные вычисления? Все, что нужно знать о данной технологии. URL: https://tempting.pro/chto_takoe_oblachnye_vychisleniyaask_vse_chto_nugno_znat_o_dannoi_tehnologii/ (дата обращения: 04.02.2022).

3. Microsoft Flight Simulator. URL: https://www.microsoft.com/ru-kz/p/microsoft-flight-simulator/9nrrjllxm68v (дата обращения: 03.02.2022).

4. Что такое облачные технологии и зачем они нужны // LG. URL: https://sonikelf.ru/oblachnye-texnologii-dlya-zemnyx-polzovatelej/ (дата обращения: 02.02.2022).

5. Microsoft облачный сервис Windows. URL: https://habr.com/ru/news/t/567770/ (дата обращения: 05.02.2022).

Статья представлена
заместителем начальника кафедры боевого применения средств связи ВАС, кандидатом военных наук, доцентом В. Г. Ивановым.

УДК 621.391
ГРНТИ 49.37.33

МОДЕЛИРОВАНИЕ ПРОЦЕССА РАЗМЕЩЕНИЯ НАГРУЗКИ В БЛОКАХ OTN С УЧЁТОМ ПЕРЕДАЧИ ПАКЕТОВ PTP

Е. В. Казакевич, Ф. А. Прошин

Петербургский государственный университет путей сообщения Императора Александра I

Возможность функционирования телекоммуникационной сети при повышении уровня нагрузки, которая поступает от систем пакетной коммутации, представляет собой приоритетное требование для современных производителей. Транспортная сеть предполагает использование универсальных алгоритмов обработки данных, которые могут работать при наличии стабильной синхронизации между сетевыми элементами. Механизм PTP представляет собой наиболее простой способ достижения синхронной работы оборудования сложной сети с множеством различных устройств, что позволяет применить его к OTN. Реализация этого протокола с учётом архитектуры OTN, основанной на принципах кадрового и мультикадрового построения информационных единиц, возможна, как один из вариантов, на уровне полезной нагрузки, например в составе пакетов Ethernet. Данная работа направлена на анализ этапов обработки сообщений PTP указанным методом и построение алгоритма данного процесса. Предлагается имитационная модель цикла корректировки часов ведомого устройства, показывающая, какие процессы могут влиять на точность и насколько велика возникающая асимметрия. Данная модель позволяет выполнять настройку согласно условиям функционирования сети и характеристикам устройств.

OTN, синхронизация, PTP, агентное моделирование, AnyLogic.

Стандарт Precision Time Protocol IEEE 1588v2 (PTP) широко распространён на сетях Ethernet операторского класса. Наличие различных настроек, включая телекоммуникационный профиль [1] обусловливает его использование в качестве основного механизма для обеспечения сетевой синхронизации. Алгоритм предполагает различные варианты работы, учитывающие технические возможности каждого сетевого элемента. Наиболее общая архитектура состоит из ведущих часов, от которых корректируется время на остальных устройствах; граничных, корректирующихся от ведущих и выступающих ведущими для последующих элементов; прозрачных, не поддерживающих обработку PTP, но способных пропускать их с необходимой корректировкой метки времени.

Данная работа представляет анализ процесса корректировки ведомых часов относительно ведущих в простом варианте, то есть при обмене сообщениями в режиме «End-to-End». Считается, что перед началом алгоритма

определены ведущие часы (Master) согласно специальному правилу [2]. Диаграмма процесса приводится на рис. 1, где обозначены используемые типы сообщений.

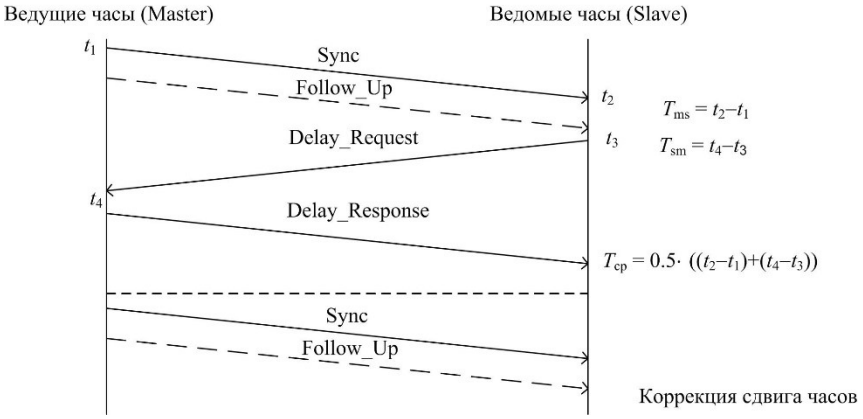


Рис. 1. Процесс корректировки ведомых часов

Сообщения PTP представляют собой кадры стандартной длины с служебными полями, которые передают метки t_1, t_2 t_3, t_4, используемые для определения сдвига часов. Для переноса сообщений между устройствами в сети необходимо использовать протоколы нижнего уровня. Так как OTN предполагает возможность переноса пакетной нагрузки, то сообщения могут передаваться как составляющая кадра Ethernet, но в протоколах высокого уровня. При моделировании определён процесс размещения, как указано на рис. 2. Сообщение PTP размещается в поле пакета UDP, который входит в состав IP-пакета. Далее пакет вставляется в кадр Ethernet. Для переноса по OTN необходимо применить алгоритм GFP [3], выполнив размещение кадра в GFP-F, и далее выполнить его размещение как нагрузку для OPU согласно [4].

Рис. 2. Последовательное размещение сообщения PTP

Такой способ реализации PTP обеспечивает правильную корректировку часов между оконечными узлами, так как чтение сообщения выполняется при выделении нагрузки OPU. Величина сдвига $T_{сдв}$, используемая для подстройки часов ведомого устройства, вычисляется на основе среднего времени прохождения сообщения в каждом направлении. Алгоритм процесса формирования, переноса, обработки сообщений PTP приводится на рис. 3. Данный алгоритм показывает цикл обмена сообщениями с метками, повторный опрос и корректирование ведомых часов.

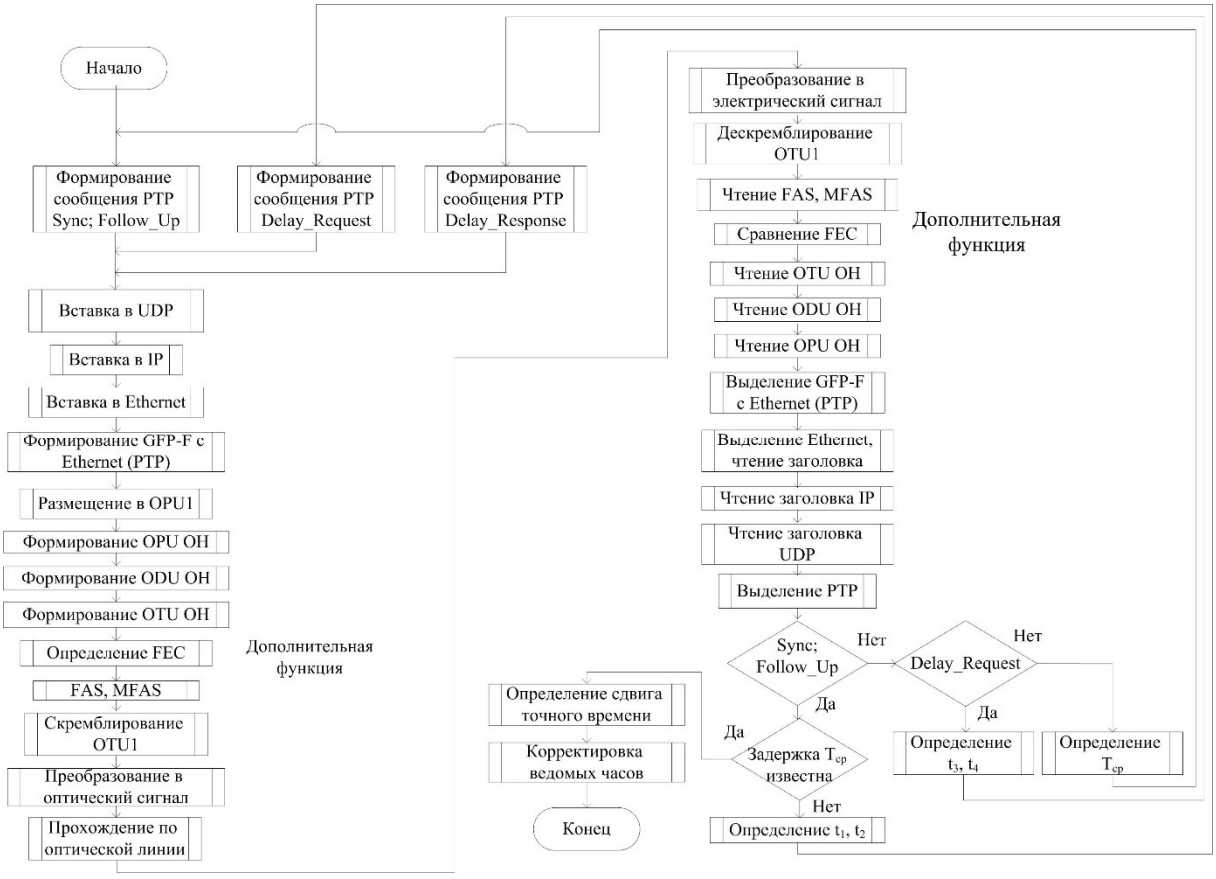


Рис. 3. Алгоритм процесса обмена сообщениями PTP

Построена имитационная модель с помощью среды AnyLogic [5]. Процессам из блок-схемы соответствуют блоки «Delay» с задаваемым временем задержки. На рис. 4 показана полученная модель.

На данной модели отдельно выделены канал обмена от ведущего к ведомому (от *S4* к *S27*) и в обратном направлении (от $S4_{обр}$ к $S27_{обр}$). Процесс прохождения сигнала по оптической линии не учитывается, так как он вносит намного меньшие задержки в общее время обмена. Величины задержек выбраны постоянными в соответствие с условием работы на программном или аппаратном уровнях. Значения для процессов обработки PTP-сообщений на уровне операционной системы (*S1*, *S2*, *S3*, *S27* и для обратного направления) заданы с экспоненциальным распределением.

Моделирование выполнялось для 100 циклов синхронизации, соответствующих показанному на рис. 1. Для каждого цикла определено время T_{ms} и T_{sm}, используемые при вычислении среднего времени прохождения сообщения $T_{ср}$. На рис. 5 показаны распределения времени прохождении при указанных условиях.

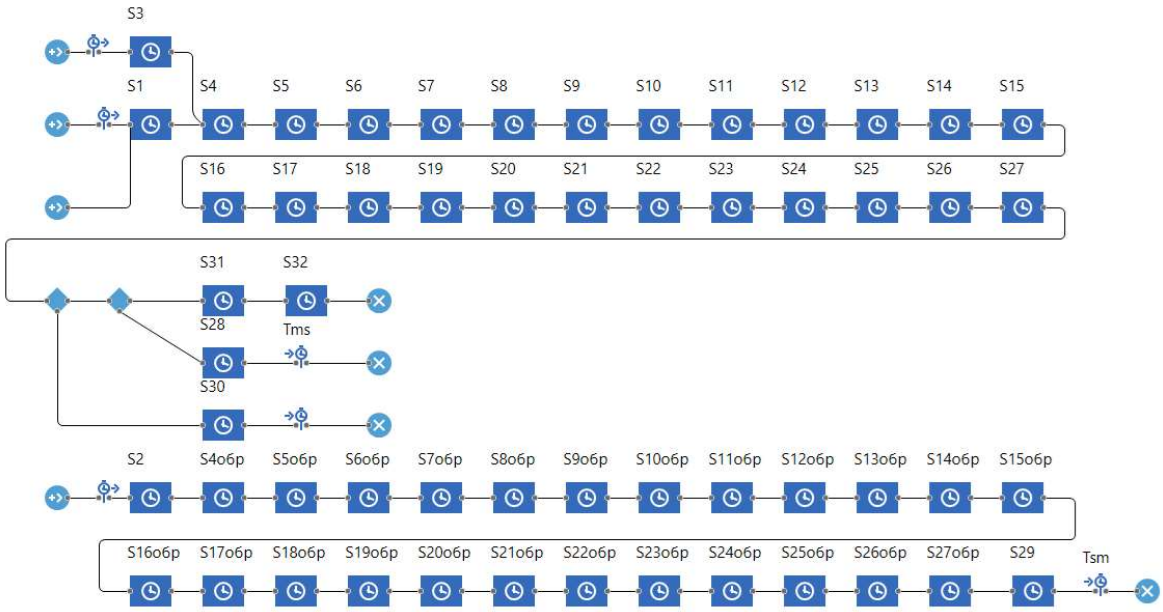


Рис. 4. Имитационная модель процесса корректировки часов

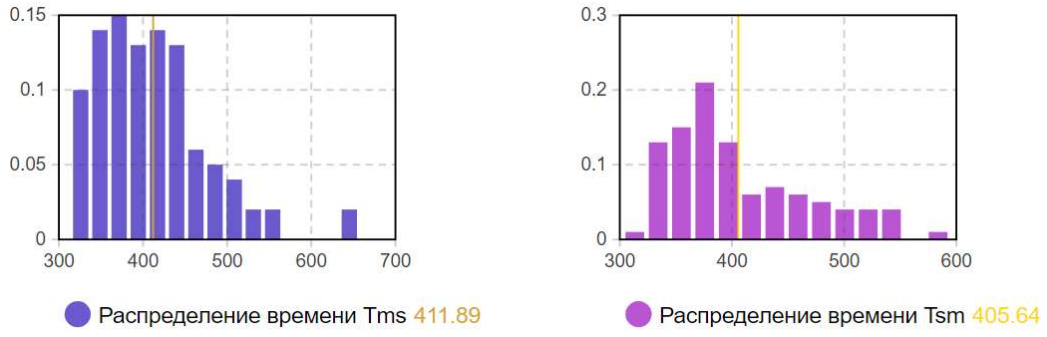


Рис. 5. Результат при переменном времени формирования и обработки PTP

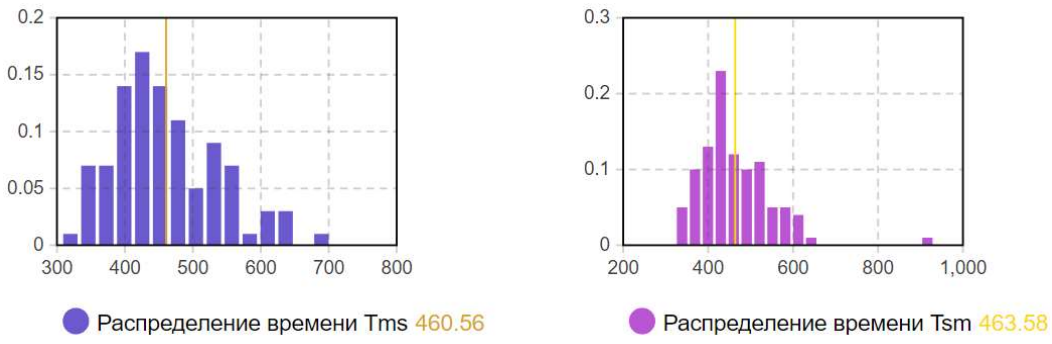


Рис. 6. Результат при экспоненциальной задержке на уровне PTP, UDP

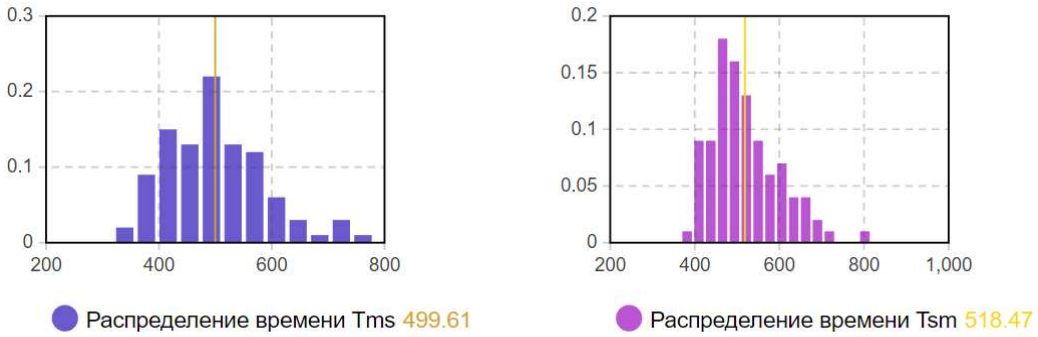


Рис. 7. Результат при экспоненциальной задержке на уровне PTP, UDP, IP

Результаты моделирования показывают, что время доставки сообщений от ведущего устройства к ведомому и обратно отличаются. Представленный метод синхронизации предполагает перенос сообщений в сигналах уровня пользователя, что предполагает обработку информации операционной системой. Как показано на рис. 5, возникают отдельные реализации, при которых задержки значительно превышает среднее значение (T_{ms} – 650 мс, T_{sm} – 590 мс). При учёте переменной задержки на уровне UDP среднее время увеличивается и также наблюдаются единичные реализации с величинами до 900 мс. Согласно рис. 7 обработка на уровне IP добавляет задержку к общему времени, при этом наблюдается большее количество реализаций с превышением среднего значения.

Рассматриваемый метод переноса PTP в полезной нагрузке может быть реализован в OTN, так как стандартные алгоритмы размещения позволяют переносить сообщения PTP. Качество функционирования такого алгоритма определяется вносимыми оборудованием задержками. Основная часть процессов на настоящее время реализуется на основе микросхем (ПЛИС) с фиксированными минимальными задержками. Наличие программной обработки PTP и последовательного размещения имеет большее значение относительно остальных процессов. Таким образом, эффективность данного метода определяется способом реализации этапов обработки на уровне нагрузке. При аппаратной реализации возможно снижение таких задержек до минимального времени и уменьшение общего времени цикла синхронизации. Представленная модель позволяет выполнять исследование при различных условиях и методах реализации. Это обеспечивается корректированием алгоритма и возможностью описания каждого процесса с точки зрения его характера и свойств.

Список используемых источников

1. Precision time protocol telecom profile for frequency synchronization ITU-T G.8265.1/Y.1365.1 (06/2021) / International Telecommunication Union, Geneva : ITU, 2021. 36 p.

2. Synchronization for Next Generation Networks – The PTP Telecom Profile. White Paper, USA : Symmetricom, 2021. 13 p.

3. Generic Framing Procedure ANSI T1X1.5/2000-024R3 (Draft ANSI T1.xxx.yy-200x) / American National Standards Institute : ANSI, 2000, 42 p.

4. Interfaces for the optical transport network ITU-T G.709/Y.1331 (06/2020) / International Telecommunication Union. Geneva : ITU, 2020. 280 p.

5. Куприяшкин А. Г. Основы моделирования систем : учеб. Пособие. Норильск, Норильский индустр. ин-т, 2015. 135 с.

Статья представлена профессором кафедры «Электрическая связь» ПГУПС, доктором технических наук, профессором А. К. Канаевым.

УДК 004.056.53
ГРНТИ 81.96

РАЗРАБОТКА МЕТОДА ВЫЯВЛЕНИЯ АТАК ARP INJECT В БЕСПРОВОДНОЙ СЕТИ СЕМЕЙСТВА IEEE 802.11

Н. И. Казаков, М. М. Ковцур, В. В. Коновалова, А. С. Салита

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье рассматривается метод выявления атаки ARP Inject на беспроводную точку доступа. ARP Inject или по другому ARP-spoofing – это разновидность атак MitM, основанная на манипуляции механизмами протокола ARP. В современном мире использование беспроводной сети с каждым днем становится более популярным и удобным способом передачи данных. К сожалению, такой способ имеет ряд уязвимых мест, одно из которых используется в рассматриваемой атаке, что приводит к нарушению доступности данных, а также нарушению конфиденциальности. Выявление атаки позволит минимизировать риски, связанные с наличием уязвимостей беспроводного канала связи, и уберечь критичные данные. Для того, чтобы выявить атаку, необходимо выстроить модель, описывающую её отличительные особенности, о чем и будет написано в данной статье.

ARP, IEEE 802.11, беспроводная сеть, выявление атак, ARP Inject.

Популярность применения беспроводных сетей для передачи данных растет с каждым днем. Улучшается качество применяемых технологий, с ростом которых повышаются возможности у атакующих беспроводные сети людей. Одной из популярных атак является MITM или другими словами атака «человек посередине». Использование протокола ARP имеет уязвимые места, которые можно применять в атаке типа MITM [1].

В основу выполнения атаки ARP Inject заложено использование протокола разрешения адресов (*Address Resolution Protocol*, ARP). ARP — это протокол, который позволяет сетевым соединениям достигать определенного устройства в сети. ARP связывает адреса интернет-протокола (IP) с адресом управления доступом к среде (MAC) и наоборот. Устройства содержат таблицу сопоставления IP-адресов и MAC-адресов, и используют её для подключения к пунктам назначения в сети. Если хост не знает MAC-адрес для определенного IP-адреса, он отправляет пакет ARP, запрашивая у других соседних устройства в сети соответствующий нужному IP-адресу MAC-адрес [2]. Протокол ARP не предназначен для обеспечения безопасности, поэтому он не проверяет, действительно ли ответ на запрос ARP исходит от авторизованной стороны. Это также позволяет узлам принимать ответы ARP, даже если они никогда не отправляли запрос. Это слабое место в протоколе ARP, которое делает возможным атаки, основанные на подмене ARP запросов [3, 4].

ARP Inject представляет собой атаку «Человек посередине» (MitM), которая позволяет злоумышленникам перехватывать пакеты между сетевыми устройствами. Атака обычно проходит по следующему сценарию:

1. Злоумышленник должен иметь доступ к сети. Он сканирует сеть, чтобы определить IP-адреса как минимум двух устройств: рабочая станция (Client) и маршрутизатор (Router) (рис. 1).

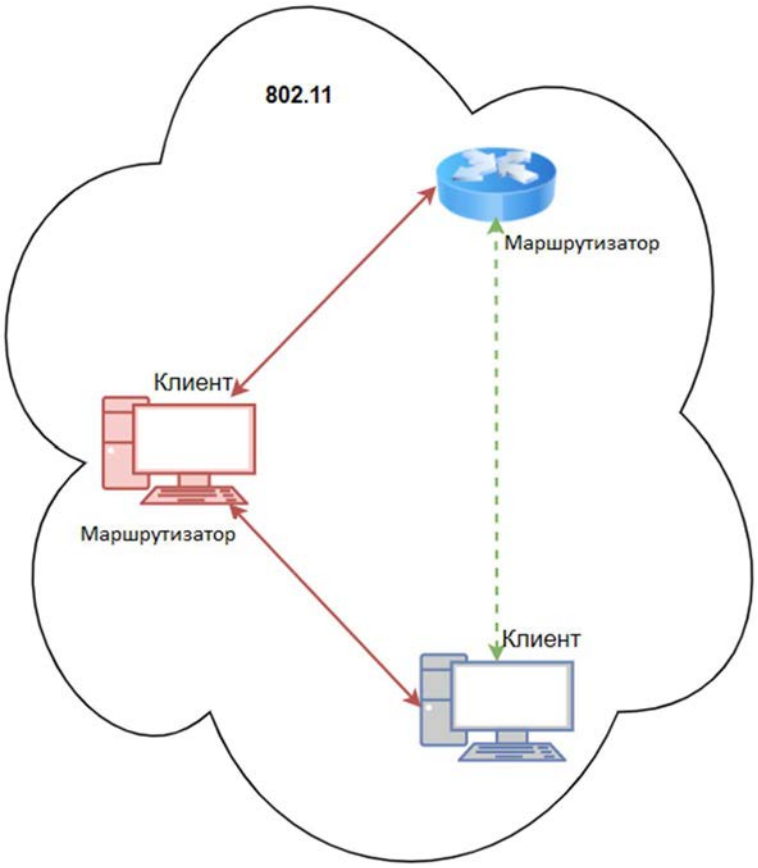


Рис. 1. Взаимодействие компонентов сети при атаке *ARP Inject*

2. Злоумышленник может использует инструмент спуфинга, такой как Arpspoof [5] или Driftnet [6], для отправки поддельных ответов ARP, или самодельный скрипт.

3. Поддельные ответы сообщают, что правильный MAC-адрес для обоих IP-адресов, принадлежащих маршрутизатору и рабочей станции,

является MAC-адресом злоумышленника. Это заставляет маршрутизатор и рабочую станцию отправлять трафик к машине злоумышленника, а не друг к другу (рис. 1).

4. Два устройства обновляют свои записи кэша ARP и с этого момента связываются через злоумышленника, а не напрямую друг с другом.

5. Злоумышленник теперь может прослушивать весь передаваемый трафик и иметь доступ к передаваемым данным.

При этом, злоумышленник может маршрутизировать трафик пользователя реальному шлюзу, и тогда пользователь даже не заметит вмешательства третьего лица в передачу трафика.

Для того, чтобы предотвратить или быстро отреагировать на данную атаку, используются средства обнаружения и предотвращения вторжений. Данные технологии можно применять не только в проводной, но и беспроводной сети.

Средства обнаружения и предотвращения вторжений работают с использованием баз данных, содержащих сигнатуры различных сетевых атак. В данной работе проводилось исследование атаки ARP Inject на беспроводной точке доступа с применением снифферов и утилит для перехвата трафика [7].

С помощью сниффера, сканирующего радиоэфир были получены пакеты (рис. 2), сгенерированные на стороне злоумышленника и направленные таким сущностям, как Клиент и Маршрутизатор. В перехваченных пакетах, направляемых в сторону Клиент и Маршрутизатор, видно, что поля ARP заголовка «Sender IP address» и «Sender MAC address» имеют значения, соответствующие данным злоумышленника.

Полученные благодаря мониторингу сети сведения были преобразованы в сигнатуры для определения атаки ARP Inject [8, 9].

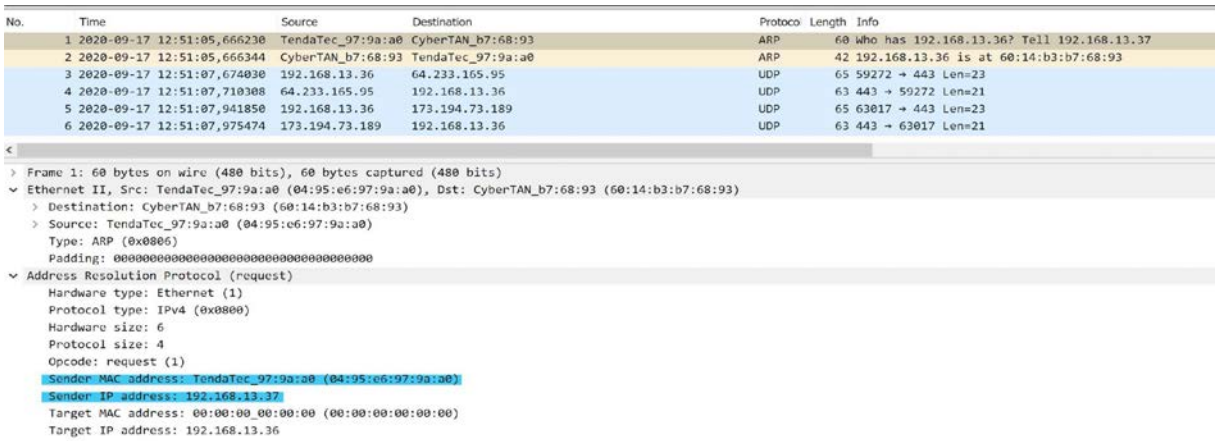


Рис. 2. Пример перехваченных пакетов от злоумышленника

На рис. 2 выделены области, по которым можно определить выполнение атаки ARP Inject. Для того, чтобы её предотвратить, на стороне средств

обнаружения и предотвращения вторжений необходимо вести список MAC-адресов легитимных точек беспроводного доступа, а также MAC и IP-адресов легитимных маршрутизаторов.

Относительно проанализированных данных, используя Python, можно описать сигнатуры для устройства безопасности, принимающего решение о существующей атаке и о её устранении. На рис. 3 представлена часть кода, отвечающая за определение атаки и являющаяся сигнатурой к атаке ARP Inject.

```
"ARP_INJECT": {
    "group": 1,
    "type": "pkt",
    "pkt": [
        {
            "field": "arp.sender_ip",
            "operator": "in",
            "not": false,
            "value": "INSPECTED_AP.gate_ip"
        },
        {
            "field": "arp.sender_mac",
            "operator": "in",
            "not": true,
            "value": ".gate_mac"
        }
    ],
```

Рис. 3. Сигнатура ARP Inject

Первое правило в коде проверяет наличие IP-адреса, указанного в поле «Sender IP address», в списке защищаемых точек доступа и легитимных маршрутизаторов, т. е. соответствие хранимому sender_ip. Второе проверяет равенство sender_mac MAC-адресу шлюза, записанного в поле sender_mac к MAC-адресу, указанного в поле «Sender MAC address». В случае несоответствия, возникает предупреждение и незамедлительное реагирование на данный инцидент информационной безопасности [10, 11].

Обнаружение атак любого вида является важной задачей обеспечения целостности, конфиденциальности и доступности передаваемых данных. Даже такие простые атаки, как ARP Inject, могут стать серьезной проблемой для инфраструктуры компании. Для предотвращения подобных атак создаются всевозможные механизмы, работающие на основе сигнатур. Чтобы предотвратить атаку, для начале необходимо протестировать её на разных

устройствах, затем собрать данные, на основе которых будут написаны сигнатуры, после чего определить в этих данных аномалии и написать сигнатуры, используя выявленные аномалии.

Список используемых источников

1. Красов А. В., Ушаков И. А. Подготовка специалистов в области информационной безопасности в Санкт-Петербургском государственном университете телекоммуникаций им. проф. М. А. Бонч-Бруевича // Инновации. 2013. № 7 (177). С. 92–97.
2. Описание механизмов ARP. URL: https://habr.com/ru/post/80364/
3. Ковцур М. М., Киструга А. Ю., Ворошнин Г. Е. Исследование атак Authentication Failure и ARP Inject и методов их обнаружения в сетях семейства IEEE 802.11 // Информационные технологии и телекоммуникации. 2021. Т. 9. № 1. С. 87-98.
4. Катина Т. В., Ковцур М. М. Алгоритм обнаружения атак на интерфейсе n2 5g сетей // Актуальные проблемы инфотелекоммуникаций в науке и образовании. IX Международной научно-технической и научно-методической конференции : сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2020. С. 569–573.
5. Описание Arpspoof. URL: https://kali.tools/?p=220
6. Описание Driftnet. URL: https://kali.tools/?p=1600
7. Ковцур М. М., Коновалова В. В. Разработка методики удаленного мониторинга трафика в корпоративных сетях // Заметки ученого. 2021. № 6-1. С. 27–31.
8. Ушаков И. А. Обнаружение инсайдеров в корпоративной компьютерной сети на основе технологий анализа больших данных // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2019. № 4. С. 38–43.
9. Balueva A., Desnitsky V., Ushakov I. Approach to Detection of Denial-of-Sleep Attacks in Wireless Sensor Networks on the Base of Machine Learning. // Studies in Computational Intelligence. 2020. V. 868. pp. 350–355.
10. Александрова Е. С., Ковцур М. М. Разработка модели нарушителя в беспроводных сетях стандарта IEEE 802.11 // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VI Международной научно-технической и научно-методической конференции : сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2017. С. 24–28.
11. Василишин Н.С., Ушаков И.А., Котенко И.В. Исследование алгоритмов анализа сетевого трафика с использованием технологий больших данных для обнаружения компьютерных атак // В сб.: Информационные технологии в управлении (ИТУ-2016). Материалы 9-й конференции по проблемам управления. Председатель президиума мультиконференции В. Г. Пешехонов. 2016. С. 670–675.

УДК 004.451
ГРНТИ 81.96

ВЫЯВЛЕНИЕ КЛЮЧЕВЫХ ПАРАМЕТРОВ РУТКИТОВ НА УРОВНЕ ЯДРА ДЛЯ МОДИФИКАЦИИ МОДЕЛИ ОБНАРУЖЕНИЯ

А. И. Катасонов, А. Е. Песин, А. Ю. Цветков

Санкт-Петербургскийгосударственныйуниверситеттелекоммуникацийим. проф. М. А. Бонч-Бруевича

Ключевой частью операционной системы является ядро, и оно играет важную роль в управлении структурами данных, критически важными для корректной работы. Руткиты на уровне ядра являются самым сложным в обнаружении типом вредоносного программного обеспечения, которое может модифицировать ядро запущенной операционной системы в целях скрыть свое присутствие и произвести множество вредоносных действий, таких как сокрытие процессов, модулей, сетевых подключений и множество других. В данной статье представлены характеристические особенности руткитов на уровне ядра и о том, как эти особенности могут быть представлены для обучения моделей в целях обнаружения как изученных, так и ранее неизвестных атак.

компьютерная безопасность, цифровая криминалистика, руткиты на уровне ядра, машинное обучение.

В последние годы руткит на уровне ядра является одним из сложнейших в обнаружении типом вредоносного ПО. Он может эксплуатировать существующие уязвимости в ядре ОС с целью скрыть как свое присутствие, так и свою вредоносную активность. Приложениям пользовательского уровня тяжело обнаружить руткит, поскольку он работает на более высоком уровне привилегий. Скрытная природа руткита делает его самым опасным и изощренным атакующим инструментом злоумышленника. Большинство традиционных систем безопасности сфокусировано на угрозах пользовательского уровня, они не справляются с обнаружением руткитов. [1]

Согласно Хогланду и Батлеру, руткит – набор программ, который остается незамеченным в системе и постоянно воздействует на нее. Для обнаружения руткитов было предложено множество подходов. Руткиты могут нарушать целостность как в статической, так и динамической части ОС. В то время как многие исследования сфокусированы только на целостности динамической части, последние работы посвящены современным руткитам, изменяющим динамические структуры данных.

С увеличением числа киберпреступлений в последние годы, автоматическое обнаружение атак стало важной частью современных систем без-

опасности. Обнаружение на основе обучения является прекрасным подходом для обнаружения как известных, так и еще не известных атак с большой точностью. Цель данной статьи заключается в представлении характеристических особенностей руткитов на уровне ядра и о том, как эти особенности могут быть представлены для обучения модели с целью обнаружения атак [2].

Модули

Руткиты уровня ядра часто загружаются в ядро как LKM. Когда модуль загружается в ядро, создается структура метаданных LDR_DATA_TABLE_ENTRY, необходимая для создания двусвязного списка, на который указывает PsLoadedModuleList. В ОС Windows команда Get-Module-ListAvailable просматривает каталоги для получения списка всех модулей, загруженных в систему. В ОС Linux, команда «lsmod» ищет в каталог для получения списка всех загруженных модулей. Если руткит скрывает модуль из этих каталогов, то пользовательские приложения и служебные инструменты не смогут найти вредоносный модуль. В этом случае мы можем проверить память на наличие двусвязного списка. К сожалению, руткит также может изменить двусвязный список модуля, разорвав связь между соответствующими записями, чтобы скрыть его наличие (рис. 1). В этом случае нам нужно просканировать память, чтобы найти несвязанный модуль [3].

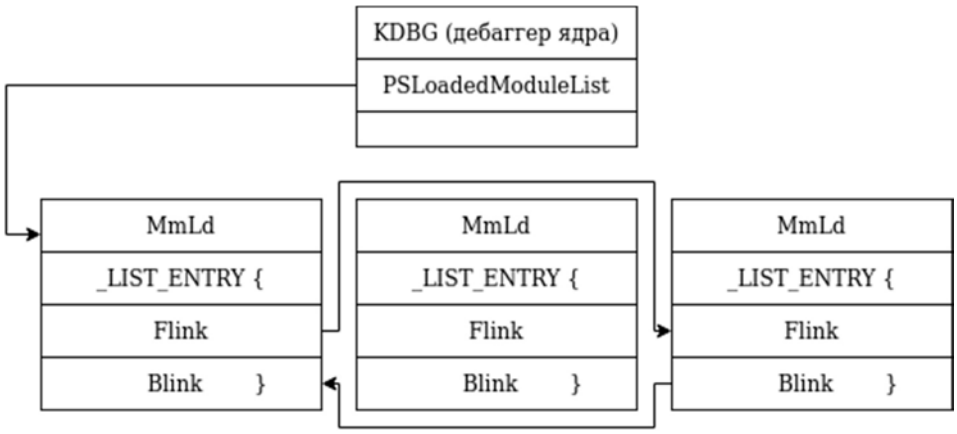


Рис. 1. Сокрытие модуля из двусвязного списка

Все несвязанные и выгруженные модули могут быть обнаружены из энергозависимой памяти при помощи сканирования тегов пула (MmLd), связанных с модулем ядра в физическом адресном пространстве. Если модуля нет в выгруженном списке, это указывает на несвязанный вредоносный модуль, скрытый руткитом. [4]

Процессы

В ОС Windows структура данных EPROCESS связана с каждым процессом, она же создает двусвязный список, на который указывает PsActiveProcessHead (рис. 2). Руткит может скрывать процессы из системных утилит путем перехвата NtQuerySystemInformation. Руткит также может использовать DKOM для разделения данных процесса EPROCESS из структуры двусвязного списка для сокрытия информации о процессе. Поле ActiveProcessLinks в EPROCESS содержит два элемента: Flink указывает на следующую структуру EPROCESS, и Blink к предыдущей структуре EPROCESS. Руткит может изменить структуру, чтобы исключить вредоносный процесс из двусвязного списка. Все данные EPROCESS содержат тег пула «Proc», который доступен для поиска методом сканирования. Неактивные или завершенные процессы могут быть обнаружены, если они находятся в памяти [5].

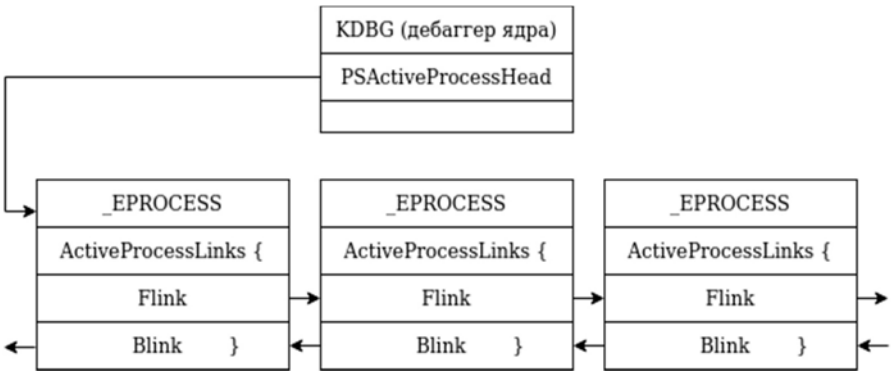


Рис. 2. Двусвязный список структуры данных EPROCESS

Потоки

Поток – это поток выполнения инструкций внутри процесса со структурой ETHREAD. [6] Стартовый адрес потока (thread.StartAddress) указывает на владельца драйвера. Если начальный адрес потока не совпадает с любым модулем ядра в PsLoadedModuleList, это может указать на потерянный поток, оставленный руткитом. Путем обхода списка в энергозависимой памяти все потоки, скрытые от отладчика, могут быть идентифицированы. А сканирование тега пула «Thre» в физической памяти также может обнаружить все скрытые потоки. Путем тщательного изучения информации о потоках можно идентифицировать любые скрытые процессы. В табл. 1 показаны возможные состояния модулей, процессов и потоков.

ТАБЛИЦА 1. Возможные состояния для модулей, процессов и потоков

Особенность / Метка	Разл. 1	Разл. 2	Разл. 3	Разл. 4	Разл. 5	Разл. 6	Потерянный поток
Нормальный	0	0	0	0	0	0	0

Особенность / Метка	Разл. 1	Разл. 2	Разл. 3	Разл. 4	Разл. 5	Разл. 6	Потерянный поток
Вредоносный	0	0	0	0	0	0	1
Вредоносный	0	0	0	0	0	1	1/0
Вредоносный	0	0	0	0	1	1/0	1/0
Вредоносный	0	0	0	1	1/0	1/0	1/0
Вредоносный	0	0	1	1/0	1/0	1/0	1/0
Вредоносный	0	1	1/0	1/0	1/0	1/0	1/0
Вредоносный	1	1/0	1/0	1/0	1/0	1/0	1/0

•Разл. 1 – различие между выводом системной утилиты и результатом сканирования памяти двусвязного списка на наличие загруженных модулей.

•Разл. 2 – различие между результатом сканирования памяти двусвязного списка и результатом сканирования тегов пула «MmLd» для загруженных модулей.

•Разл. 3 – различие между результатом сканирования двусвязного списка и результатом сканирования тегов пула структуры данных DRIVER_OBJECT для загруженных модулей.

•Разл. 4 – различие между выводом системной утилиты и результатом сканирования памяти двусвязного списка на наличие активных процессов.

•Разл. 5 – различие между результатом сканирования памяти двусвязного списка и результатом сканирования тегов пула «Proc» для активных процессов.

•Разл. 6 – различие между выводом отладчика утилиты и результатом сканирования памяти для активных потоков.

Захваты ядра

SSDT является важной целью для руткита, поскольку он содержит указатели подпрограмм системных служб в пространстве ядра. А руткит может перезаписать указатели функций SSDT для указания на вредоносные модули. В ОС Windows таблица SSDT хранит указатели на функции ядра API модулей NT, и теневая таблица SSDT хранит указатели на связанные с графическим интерфейсом функции модуля win32k.sys. Таблица дескрипторов прерываний (IDT) – еще одна важная цель, и руткиты могут изменить записи IDT, чтобы перенаправить поток управления на вредоносный код для выполнения. Проверив память IDT, мы можем найти перехваченную запись [7].

Обратные вызовы и таймеры

Для отслеживания возникновения определенного события в ОС Windows, драйверы должны быть зарегистрированы для процедуры обратного вызова. Функция обратного вызова позволяет драйверу руткита отслеживать активность системы и предпринимать различные вредоносные действия соответственно. Руткит может создать таймер, чтобы получать уведомления об прошествии определенного времени и планировать операции с помощью этого функционала. Мы можем проверить энергозависимую память для обратного вызова объекта и объекта таймера, чтобы найти любые вредоносные или неизвестные модули, указывающие на руткит.

Специальные машинные регистры

Руткиты могут изменять значения машинного регистра для изменения потока управления ядром и заставлять машину регистрировать важную функцию. Поскольку некоторые машинные регистры содержат важные ячейки памяти таблицы ядра, путем изменения значения регистра руткиты могут перенаправить поток управления на адрес памяти вредоносного исполняемого файла. После загрузки системы значения в некоторых машинных регистрах становятся фиксированными и их изменения подозрительны.

Регистр таблицы дескрипторов прерываний

IDT – это структура данных, в которой хранится список прерываний для определения правильной реакции на прерывания и исключения [8]. Используя нагрузки инструкции IDT руткит может изменить базовый адрес IDT и перенаправить все запросы на вредоносный адрес. Обычный сканер безопасности может проверить целостность старого IDT, и руткит останется незамеченным. Таким образом, операция записи в IDTR может быть включена в набор функций модели.

Регистры глобальной и локальной таблицы дескрипторов

Характеристики различных областей памяти определяются в глобальной таблице дескрипторов (GDT) и локальной таблице дескрипторов (LDT). Регистр глобальной таблицы дескрипторов (GDTR) и локальный регистр таблицы дескрипторов (LDTR) хранят значение, указывающее на GDT и LDT соответственно. Руткиты могут изменять значения этих регистров на адрес памяти, по которому существует вредоносный исполняемый файл [9].

Регистр управления Cr0

Общее поведение ЦП и других устройств можно контролировать или изменять регистрами управления, которые могут изменять базовые операции процессора. Для защиты записи используется 16-й бит регистра cr0. Если он установлен, ЦП не сможет записать в раздел постоянной памяти. 16-й бит регистра cr0 может быть изменен руткитом для обхода защиты записи или перехвата SSDT. Некоторые легитимные драйверы ядра, такие как антивирусы или брандмауэры, могут изменить регистр cr0 [10]. Это важную особенность необходимо включить в модель обучения. В табл. 2 показаны возможные состояния перехватчиков ядра, обратных вызовов и таймеров, и специальные машинные регистры.

ТАБЛИЦА 2. Возможные состояния перехватчиков, обратных вызовов, таймеров и регистров

Метка	Перехват SSDT	Перехват IDT	Внутр. перехват	Обратные вызовы	Таймеры	Изменения IDTR	Изменения GDTR	Изменения cr0
Норм.	0	0	0	0	0	0	0	1/0
Вред.	0	0	0	0	0	0	1	1/0
Вред.	0	0	0	0	0	1	1/0	1/0
Вред.	0	0	0	0	1	1/0	1/0	1/0
Вред.	0	0	0	1	1/0	1/0	1/0	1/0
Вред.	0	0	1	1/0	1/0	1/0	1/0	1/0
Вред.	0	1	1/0	1/0	1/0	1/0	1/0	1/0
Вред.	1	1/0	1/0	1/0	1/0	1/0	1/0	1/0

В этой статье подробно описываются характерные особенности руткита на уровне ядра и то, как они могут быть представлены для обучения моделей. Наша модель включает в себя некоторые характерные черты руткитов на уровне ядра, которые появятся в результате непрерывного мониторинга, для обнаружения временных атак. Используя полученные в данном исследовании характеристики можно использовать для обучения моделей в целях обнаружения как изученных, так и ранее неизвестных атак

Список используемых источников

1. Пестов И. Е., Шинкарева П. С., Кошелева С. А., Бурмистров М. Д. Разработка программно-аппаратной системы контроля и управления доступом // Эргодизайн. 2020. № 1 (7). С. 19–24.

2. Построение доверенной вычислительной среды: монография / Красов А. В., Гельфанд А. М., Коржик В. И., Котенко И. В., Петрив Р. Б., Сахаров Д. В., Ушаков И. А., Шариков П. И., Юркин Д. В. СПб.: Индивидуальный предприниматель Петрив Р. Б., 2019. 108 с.

3. Гельфанд А. М., Казанцев А. А., Красов А. В., Орлов Г. А. Исследование распределенного механизма безопасности для устройств интернета вещей с ограниченными ресурсами // Актуальные проблемы инфотелекоммуникаций в науке и образовании. IX Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2020. С. 321–326.

4. Гололобов Н. В., Израилов К. Е. Исследование способа небезопасного вызова API ядра в ОС Windows // Актуальные проблемы инфотелекоммуникаций в науке и образовании. X Юбилейная Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2021. С. 248–252.

5. Волкогонов В. Н., Казанцев А. А., Орлов Г. А., Смирнов Д. Н. Применение физически неклонируемых функций для выполнения аутентификации в среде интернета вещей // Актуальные проблемы инфотелекоммуникаций в науке и образовании. X Юбилейная Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2021. С. 409–414.

6. Ушаков И. А., Котенко И. В. Модель обнаружения внутренних нарушителей на основе использования технологий больших данных // В сб.: Региональная информатика и информационная безопасность. 2017. С. 253-254.

7. Москальчук А. И. Разработка виртуальной пентест-лаборатории для исследования метода оценки уровня защищенности локальной сети // Студенческая весна - 2020. 74-я региональная научно-техническая конференция студентов, аспирантов и молодых ученых : сб. науч. ст. Санкт-Петербург, 2020. С. 33–38.

8. Штеренберг С. И., Москальчук А. И., Коптелова В. А., Виноградова О.М. Разработка методов обеспечения безопасности для создания уязвимых виртуальных машин и изучения методов тестирования на проникновения // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2021. № 1. С. 32-38.

9. Ахметшина М. Э., Манкаев Р. М. А., Ушаков И. А. Аудит информационной безопасности организаций с применением сетевых анализаторов и тестов на проникновение // Актуальные проблемы инфотелекоммуникаций в науке и образовании. X Юбилейная Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2021. С. 50–55.

10. Израилов К. Е., Кузнецов С. А. Применение искусственного интеллекта и методов машинного обучения для поиска уязвимостей исходного кода // Актуальные проблемы инфотелекоммуникаций в науке и образовании. IX Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4-х т. СПб.: СПбГУТ,, 2020. С. 361–366.

Статья представлена заведующим кафедрой ЗСС СПбГУТ, кандидатом технических наук, доцентом А. В. Красовым.

УДК 004.7
ГРНТИ 50.41

ПРОГРАММИРОВАНИЕ КИБЕРФИЗИЧЕСКИХ СИСТЕМ С ИСПОЛЬЗОВАНИЕМ ВИЗУАЛЬНОГО ПРОГРАММИРОВАНИЯ В ПРИЛОЖЕНИИ FLPROG

Р. В. Киричек, А. С. Кривец

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В настоящее время активное развитие получили приложения киберфизических систем. В большинстве случаев разработка тех или иных приложений связана с программированием контроллеров. Незнание языков программирования является ограничивающим фактором при создании проектов, связанных с датчиками, микроконтроллерами, отправкой данных на облачные платформы. Для программирования отладочной платы с открытой аппаратной архитектурой Arduino требуется знание языка С, но процесс его изучения достаточно долговременный. Для решения данного ограничения был создан открытый программный продукт FLProg. Программное Обеспечение представляющее собой графическую среду программирования плат Arduino, ESP32, ESP8266 и Intel Galileo. В FLProg можно создавать всевозможные проекты с подключением огромного количества датчиков, а главное – для этого требуется просто собрать в нужном порядке несколько графических блоков. В результате корректной сборки блоков генерируется программный код, который загружается в микроконтроллер с использованием среды Arduino IDE. В статье освещено приложение FLProg, его функциональные особенности и примеры проектов, реализованных в данном приложении.

визуальное программирование, киберфизические системы, FLProg, Arduino, умный дом.

В настоящее время киберфизические системы активно применяются во всех сферах жизнедеятельности. «Умные» сети электроснабжения, системы управления «умным» транспортом, АСУ (автоматизированные системы управления) в производстве и сельском хозяйстве, а также медицинское оборудование. В связи с появлением огромного количества датчиков с и исполнительных устройств с низкой стоимостью у большинства людей возникает желание автоматизировать процессы в квартире и создать «умным дом», добавив климат-контроль, включение света по команде или даже управление кофеваркой и холодильником. Все эти идеи уже реализуются комплексно, существуют и развиваются такие масштабные решения, которые затрагивают автоматизацию сервисов в городе, создавая более комфортные условия жизнедеятельности горожан [1, 2].

Киберфизический «бум» происходит прямо сейчас и затрагивает каждого из нас. Он близок к каждому, и сегодня всем доступно его развитие. Но существенной проблемой на пути к кибернетизации является то, что

в большинстве случаев разработка тех или иных приложений связана с программированием контроллеров.

Незнание языков программирования является ограничивающим фактором при создании проектов, связанных с датчиками, микроконтроллерами, отправкой данных на облачные платформы. Сегодня, самой популярной и доступной для домашнего программирования является отладочная плата с открытой аппаратной архитектурой – Arduino, а для работы с ней требуется знание языка С, но процесс его изучения достаточно долговременный.

Для решения данного ограничения был создан открытый программный продукт FLProg. Это десктоп-приложение, представляющее собой графическую среду программирования плат Arduino, ESP32, ESP8266 и Intel Galileo [3].

С помощью этого приложения можно запрограммировать контроллер, не зная текстовых языков программирования, а выглядит это как рисование принципиальной или электрической схемы.

Конечно, уже давно существуют графические среды рисования принципиальных или логических схем промышленных контролеров. И такой подход оказался очень удобным для легкого вхождения в разработку систем АСУ инженеров-электриков и электронщиков. Производители оборудования разрабатывают подобные среды для своих датчиков и контролеров, которые имеют высокую стоимость и не используются вне промышленных масштабов [4].

Проект FLProg был вдохновлен вопросом доступности, он позволяет создавать свои проекты на популярных контролерах любому человеку, знакомому с электротехникой и электроникой.

Программа FLProg позволяет создавать прошивки для плат с помощью графических языков FBD и LAD, которые являются стандартом в области программирования промышленных контроллеров [5].

Смысл графического программирования прост: вы выбираете нужные вам логические блоки и соединяете между собой, а программа компилирует проект в полностью готовый код, который загружается в микроконтроллер с использованием среды Arduino IDE. Такой метод работы позволяет не только программировать без знания языка, но и ускорить работу опытным программистам, и даже если готовые блоки не будут соответствовать всем их требованиям, то они могут создать свои, уже оптимизирование под их задачи пользовательские блоки.

При создании программы, авторы старались максимально использовать наработки программистов Siemens, ABB, Schneider Electric в их средах программирования [6]. Авторы расширили классический функционал этих языков, добавив функциональные блоки, отвечающие за работу со внешними устройствами и сервисами, но самое главное – они сделали максимально

удобной работу с самыми популярными платами и контролерами и регулярно добавляют новые, прислушиваясь к требованиям пользователей.

Для удобства пользователей есть возможность получение объемной справки по каждому элементу в библиотеке, что позволяет разобраться с возможностями и принципами подключения элемента, без поиска дополнительной литературы. А в случае непонимания, в справке ко многим элементы есть видео урок.

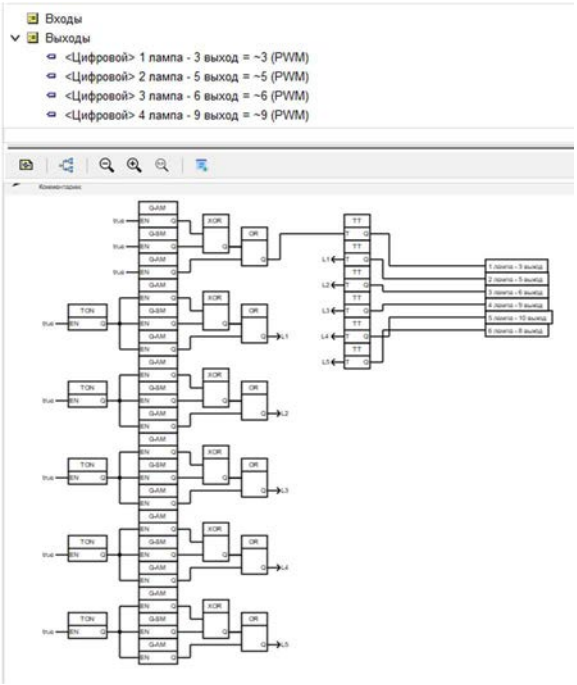


Рис. 1. Пример проекта новогодней гирлянды в FLProg

Примеров готовых проектов масса: от новогодних гирлянд (рис. 1), до промышленных станков (рис. 2) или систем дистанционного управления масляными котлами с их полным контролем. Через неделю-две знакомства с программой вы будете иметь достаточно знаний, чтобы оборудовать ваш дом различными датчиками и детекторами, реле для включения приборов, умным светом и климат контролем. А если воспользоваться программой REMOTE XY (программа для создания графического интерфейса), то этим всем ещё можно будет управлять дистанционно с телефона.

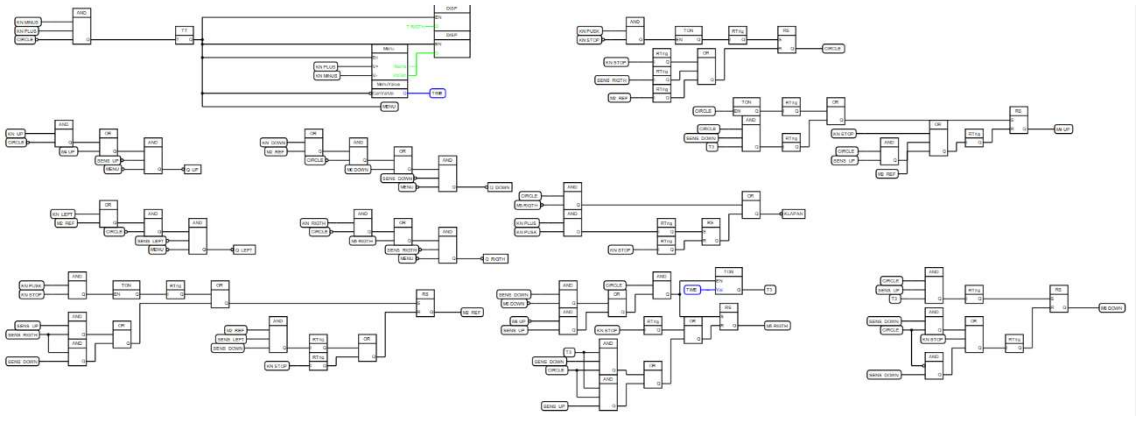


Рис. 2. Пример проекта пескоструйного станка в FLProg

С использованием FLProg можно строить промышленные системы. И это станет выгодным решением для производителя, так как обучить своего инженера не займет много времени, что позволит не вызывать программиста для отладки, ремонта и настройки оборудования в случае необходимости.

Так же хочется добавить: работа над приложением не останавливается и обновления регулярно выходят. У проекта есть свой сайт, на котором члены сообщества пользователей программы общаются между собой, узнают последние новости проекта, находят необходимую информацию по работе с приложением и делятся готовыми проектами.

Из всего вышесказанного хочется сделать несколько выводов. Графическое программирование позволяет сделать создание кибер-физических систем более доступным и помогает популяризировать работу с такими системами, что определенно дает возможность повышать уровень образованности и заинтересованности населения в IT-сфере. На сегодня, FLProg – самая доступная и удобная среда для графического программирования.

Список используемых источников

1. Фантастические «умные» города сегодня. URL: https://habr.com/ru/company/sezinnopolis/blog/598147/ (дата обращения: 25.02.2022).

2. Василенко И. А., Василенко Е. В., Люлько А. Н. «Умный город» XXI века: возможности и риски смарт-технологий в городском ребрендинге / под ред. проф. И. А. Василенко. М. : Международные отношения, 2018. 256 с.

3. Что такое FLProg. URL: https://flprog.ru/chto-takoe-flprog/ (дата обращения: 15.02.2022).

4. Грингард С. Интернет вещей. М. : Альпина Паблишер, 2016. 78 с.

5. Программируем PLC на Arduino с помощью FBD и LAD. URL: https://industriya.com/posts/90-programmiruem-plc-na-arduino-s-pomoschyu-fbd-i-lad.html (дата обращения: 15.03.2022).

6. Технологии современного промышленного программирования. URL: https://news.itmo.ru/ru/education/trend/news/10485/ (дата обращения: 10.03.2022).

УДК 004.738
ГРНТИ 49.43.29

СРАВНИТЕЛЬНЫЙ АНАЛИЗ АРХИТЕКТУРЫ СЕТЕЙ 5G НА ОСНОВЕ РЕКОМЕНДАЦИЙ GSMA И O-RAN

Р. В. Киричек, М. А. Рожков

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

5G – это технологический стандарт пятого поколения для широкополосных сотовых сетей, разработанный 3GPP. В отличие от предыдущих поколений, которые требовали развертывания базовых сетей и сетей радиодоступа на системах одного и того же поколения, вместе образовывая систему 4G, идеология сетей нового поколения 5G предполагает дополнить существующие архитектуры сетей радиодоступа, что позволяет интегрировать элементы разных поколений в разные конфигурации сетей. В то

время как 3GPP определяет как новую базовую сеть 5G, так и новую технологию радиодоступа под названием 5G «New Radio», операторы вольны сами выбирать методологию интеграции системы 5G в свою архитектуру сетей предыдущих поколения. В связи этим с организация GSMA и альянс O-RAN разработали сценарии эволюции архитектуры сетей 4G. В статье рассматриваются ключевые особенности каждой из архитектур, построенной на основе рекомендаций GSMA и O-RAN, их сходство и различия, а также приведены основные плюсы и минусы данных методов построения сетевой инфраструктуры.

сети пятого поколения, радиодоступ, беспроводные сети, виртуализация, стандарт.

В сентября 2015 года был проведён семинар консорциума 3GPP, который положил начало развитие стандарта сетей пятого поколения [1]. В сотрудничестве операторами и производителями сетевого оборудования были разработаны стандарты Stand-Alone и None-Stand-Alone 5G архитектуры [2, 3]. Для большего понимания мы кратко рассмотрим такие ключевые её аспекты как разделение плоскости управления и пользователя (CUPS), сегментация сети (*Network Slicing*), виртуализация сетевых функций (VNF) и конвергентность различных видов сетей радиодоступа (*Access Network*) под единой опорной сетью (*Core Network*).

CUPS позволяет операторам сетей разделить расширенное пакетное ядро (EPC) на уровень управления (CP) и плоскость пользователя (UP), которые могут быть размещены ближе к поддерживаемому приложению [4]. Это позволяет упростить механизмы развертывания и эксплуатацию сети путем распределенного или централизованного развертывания, а также обеспечить масштабирование между функциями плоскости управления и плоскости пользователя, не влияя при этом на функциональность существующих узлов.

Сегментация сети подразумевает разделение физической архитектуры 5G на множество виртуальных сетей или слоёв. Каждый сетевой слой включает в себя функции уровня управления, функции уровня пользовательского трафика и сеть радиодоступа [5].

Виртуальные сетевые функции (VNF) – это программные приложения, которые предоставляют сетевые функции, такие как службы каталогов, маршрутизаторы, брандмауэры, балансировщики нагрузки и др. реализованные в аппаратных комплексов на основе микропроцессоров общего назначения [6].

В то время как 3GPP определяет стандарты архитектуры и ключевые особенности сети пятого поколения, операторы вольны сами выбирать сценарий перехода от сетей 4G к 5G. В связи с этим ассоциация GSMA и альянс O-RAN разработали свои собственные сценарии эволюции сетей четвёртого поколения. Далее на рис. 1 представлена схема эволюции развития архитектуры сетей 4G ассоциаций GSMA [7].

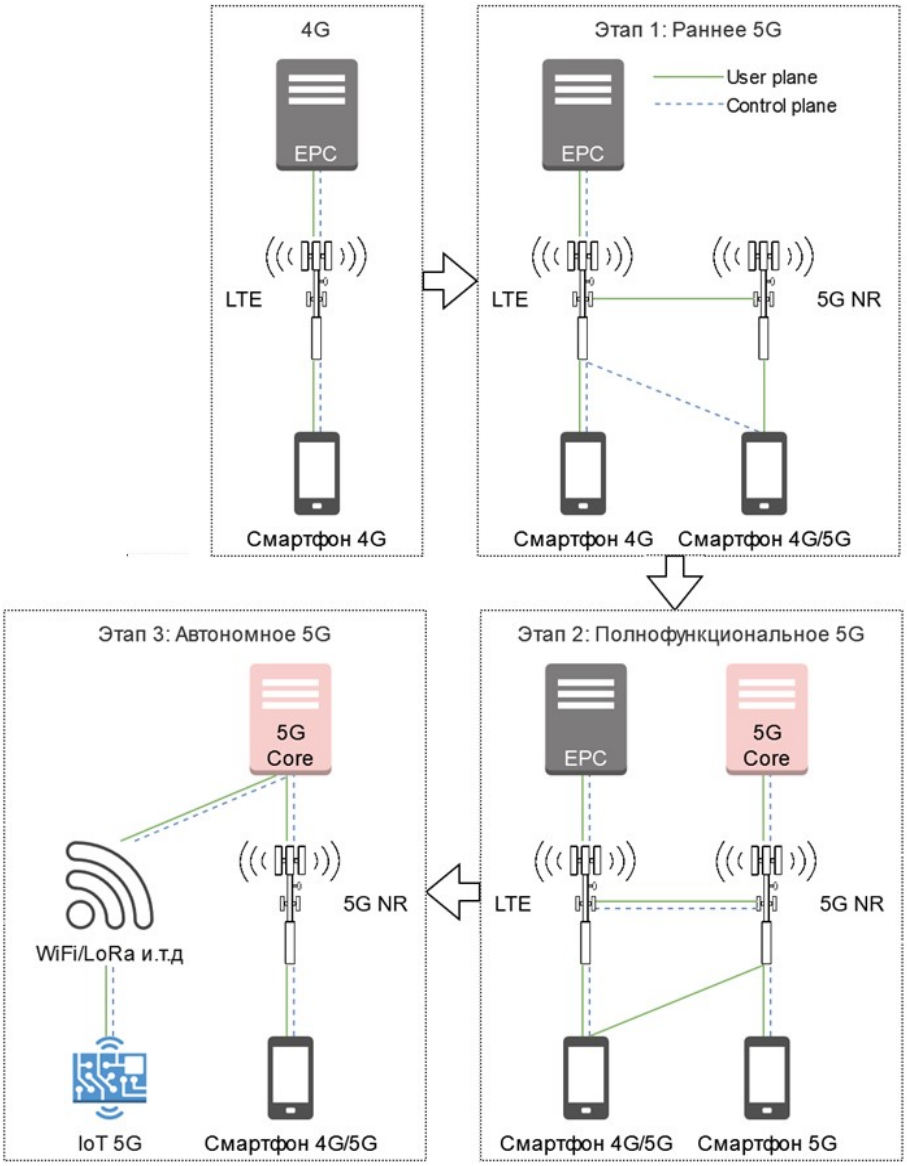


Рис. 1. Схема эволюции развития архитектуры сетей 4G ассоциаций GSMA

Первый этап представляет собой классическую реализацию выделенной сети LTE на базе ядра EPC и базовых станций LTE и 5G NR, при этом пользователь сети 5G имеет двойное подключение к LTE, обрабатывающий уровень управления, и 5G NR, передающий пользовательский трафик. Предполагается, что подобные сети можно развернуть в кротчайшие сроки и при минимальных затратах, но данная реализация не поддерживает представленные стандартом качество обслуживания и сервисы.

Второй этап представляет собой финальную архитектуру комбинированной сети 5G/LTE. Здесь так же, как и на предыдущем этапе используется технология двойного подключения, но уже используется ядро сети 5G и базовые станции LTE с разделением плоскости управления и пользователя, позволяющее реализовать частичную поддержку сервисов и QoS 5G.

Третий этап автономное (*Stand-Alone*) 5G, в котором реализована поддержка всех ключевых аспектов архитектуры 5G описанных в стандарте 3GPP. Таким образом обеспечивается конвергенция различных типов радиосетей, а поддержка сетевых функций LTE осуществляется путём их виртуализации на основе базовых станций 5G NR.

Параллельно GSMA на основе стандартов 5G 3GPP так же разрабатывалась архитектура сетей пятого поколения Open Ran. В её основе лежать применение облачных технологий и внедрение алгоритмов искусственного интеллекта [8]. Сценарии эволюции развития архитектуры сетей 4G альянса O-RAN представлена на рис. 2.

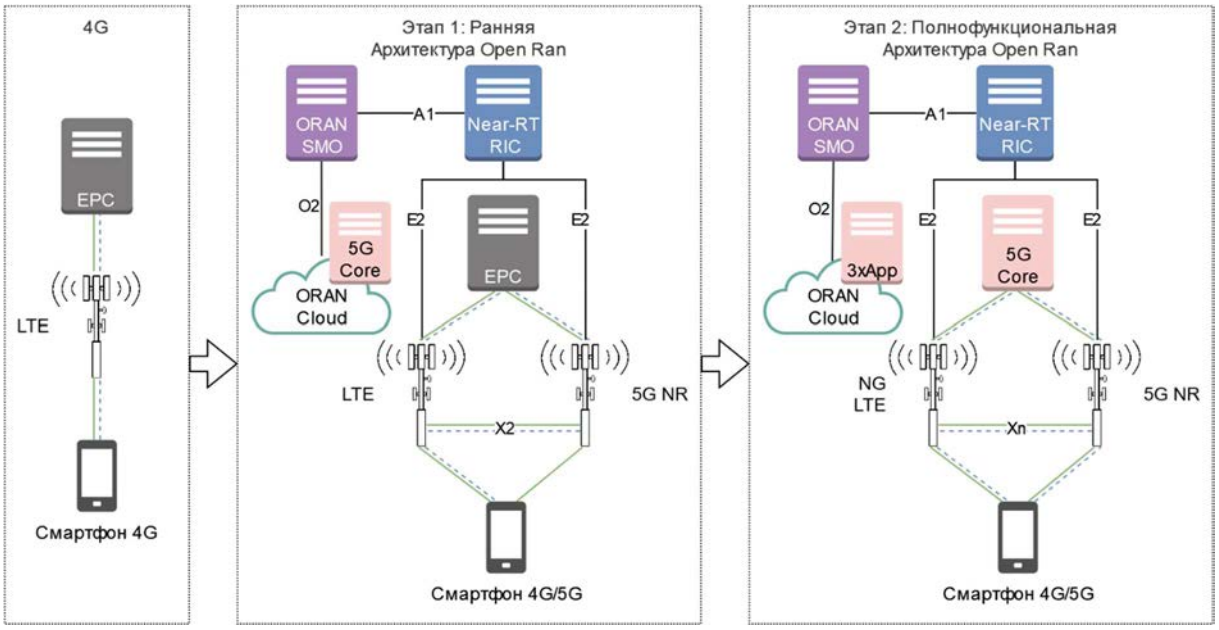


Рис. 2. Сценарии эволюции развития архитектуры сетей 4G альянса O-RAN

Как можно заметить базовая структура сети первого этапа архитектуры O-Ran совпадает с соответствующим этапом ассоциации GSMA, но с некоторыми ключевыми изменениями. Так, например, у нас добавляются платформы Near-RT Ric, выполняющее функции чувствительных ко времени сервисов (такие как балансировка нагрузки, передача обслуживания и контроль интерференции и помех), SMO и виртуализированное на базе облачных технологий ядро сети 5G, позволяющее реализовать часть сервисов и требований QoS описанных в стандарте 5G 3GPP[9].

На втором этапе уже используется полноценное ядро сети 5G, при этом облако O-Ran предполагается задействовать для обучение моделей оптимизации работы RAN и сторонних приложений, а взаимодействие различных типов радиосетей обеспечить с помощью протокола Xn.

Заключение

Оба подхода эволюции удовлетворяют требованиям к архитектуре сетей пятого поколения выдвинутыми консорциумом 3GPP. В то же время сценарий построения архитектуры Oran предполагает частичную реализацию сервисов 5G посредством виртуальных сетевых функций с применением облачных технологий. Так же 5G Oran предоставляет сервисы для дальнейшей поддержки стандартов мобильной связи предыдущего и последующих поколений, но использование дополнительного оборудования и сервисов сказывается на стоимости перехода к 5G, расходы на которые предполагается снизить путём применения open source технологий [10], а также требует разработки и стандартизации интерфейсов ORAN со стороны регулирующих органов и поставщиков оборудования.

Список используемой литературы

1. Sasha Sirotkin (Editor) 5G Radio Access Network Architecture: The Dark Side of 5G. Wiley-IEEE Press. 2020. 448 Pages. ISBN: 978-1-119-55088-4

2. 3GPP TR38.801, “Radio access architecture and interface”, Rel. 14.

3. 3GPP TR23.799, “Study on Architecture for Next Generation System”, Rel. 14.

4. Ian Leyva-Pupo, Alejandro Santoyo-González, Cristina Cervelló-Pastor A Framework for the Joint Placement of Edge Service Infrastructure and User Plane Functions for 5G // Department of Network Engineering, Universitat Politècnica de Catalunya (UPC), 08860 Castelldefels, Spain, 2019.

5. Мухизи С., Киричек Р. В. Анализ технологии слайсинга в сетях связи пятого поколения // Информационные технологии и телекоммуникации. 2017. Том 5. № 4. С. 57–63.

6. Hendrik Moens, Filip De Turck VNF-P: A Model for Efficient Placement of Virtualized Network Functions // Ghent University – iMinds, Department of Information Technology Gaston Crommenlaan 8/201, B-9050 Gent, Belgium, January 2014.

7. GSMA, “Road to 5G:Introduction and Migration”, April 2018.

8. O-RAN ALLIANCE e.V, O-RAN.WG1.OAM-Architecture-v04.00, Buschkauler Weg 27, 53347 Alfter, Germany, Register of Associations, Bonn VR 11238, VAT ID DE321720189, 2021.

9. O-RAN ALLIANCE e.V, O-RAN.WG1.O-RAN-Architecture-Description-v03.00, Buschkauler Weg 27, 53347 Alfter, Germany, Register of Associations, Bonn VR 11238, VAT ID DE321720189, 2021.

10. Киричек Р. В., Рожков М. А. Обзор архитектуры сетей пятого поколения O-RAN // Актуальные проблемы инфотелекоммуникаций в науке и образовании. X Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2021. Т. 1. С. 471–474.

УДК 004.735
ГРНТИ 49.37.29

ИССЛЕДОВАНИЕ ФУНКЦИОНИРОВАНИЯ ФРАГМЕНТА СЕТИ LPWAN В УСЛОВИЯХ ПРЕДНАМЕРЕННЫХ ЭЛЕКТРОМАГНИТНЫХ ВОЗДЕЙСТВИЙ

Р. В. Киричек, Е. Д. Филин

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Безопасность Интернета вещей является важнейшей темой для обсуждения и осуществления научной деятельности, и большое количество работ подтверждают этот факт. Одним из вариантов реализации угроз безопасности Интернета вещей (далее - ИВ) является осуществление преднамеренных электромагнитных воздействий (далее – ПДЭМВ) на каналы передачи данных устройств ИВ. Электромагнитной помехой называется осуществление электромагнитного возмущения на компонент системы с целью ухудшения функциональности или производительности. Для данного типа воздействия характерно проведение атаки без каких-либо демаскирующий признаков на расстоянии, не позволяющем обнаружить объект воздействия на канал связи. Воздействие ПДЭМВ наиболее критично для беспроводных каналов передачи данных, работающих в реальном времени, в связи с чем является актуальным проведение исследований, связанных с изучением механизмов деструктивных воздействий на средства связи, разработка моделей и методов противодействия, а также модернизация нормативно-правовых документов. В данной работе проводится анализ проводимых исследований по ПДЭМВ на энергоэффективные сети дальнего радиуса действия (далее – LPWAN).

LPWAN; LoRaWAN; LoRa; IEMI.

Техническую устойчивость любой системы можно представить как совокупность 4R: Robustness (надежность системы в целом), Redundancy (наличие избыточных элементов), Rapidity (скорость восстановления) и Resources (способности к управлению кризисными ситуациями и мобилизации усилий). Чтобы иметь полную информацию о защищаемой системе, необходимо знать состав аппаратного и программного обеспечения, настройки и возможные уязвимости. Несмотря на механизмы безопасности, используемые в различных протоколах, технология LPWAN уязвима для широкого спектра атак. В [1] рассматривается сетевая архитектура и механизмы безопасности технологий LPWAN, а также проводится анализ уязвимостей LoRaWAN. Приведены и описаны типы атак, такие как компрометация устройств и ключей сети, повторное воспроизведение и червоточина. В [2] осуществлен анализ уязвимостей технологий LPWAN, таких как

LoRaWAN, Sigfox и NB-IoT и описаны три сценария атак. Проведённый анализ показывает, что в текущем состоянии технологию Sigfox не рекомендуется использовать для приложений с критическими данными. LoRaWAN и NB-IoT предлагают достаточные гарантии безопасности. Также описана атака глушения, которая может быть направлена на физический и канальный уровни модели OSI. При помехе на физическом уровне атакующий отправляет широкополосный сигнал с более высоким отношением сигнал/шум (SNR), чем на приемнике получателя. При помехе на канальном уровне атакующий оказывает воздействие только на определенные части сообщения, чтобы пакет был отброшен получателем. В [3] проведен анализ безопасности LoRaWAN. Использование шифрования обеспечивает оптимальную безопасность сети, но при этом каналы связи все еще подвержены создаваемым помехам, которые могут вызвать отказ в обслуживании устройств. Глушение открывает возможности для осуществления различных методов атак, таких как атака типа повторное воспроизведение и червоточина, которые могут нанести больший ущерб сети, позволяя устройствам злоумышленника проникать в сеть незамеченными и передавать данные, которые могут нанести вред сети.

В [4] рассмотрено воздействие сверхкоротких электромагнитных импульсов (далее – СК ЭМИ), являющихся разновидностью сверхширокополосных сигналов. Особенностями СК ЭМИ является длительность импульсов порядка единиц – десятков наносекунд, фронты сигналов порядка десятков – сотен пикосекунд и частотой следования до единиц мегагерц.

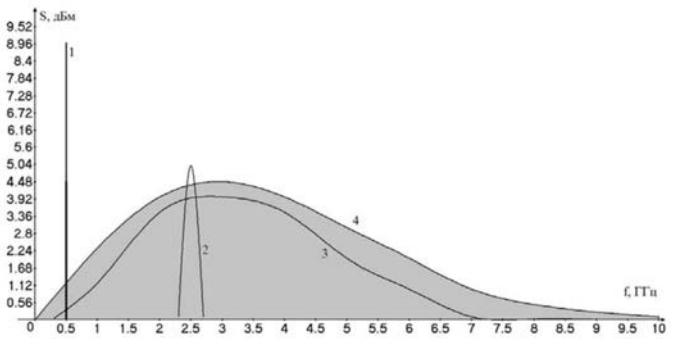


Рис. 1. Условные спектры сигналов.
1 – узкополосный, *2* – широкополосный,
3 – сверхширокополосный,
4 – сверхкороткий электромагнитный импульс

В результате ПДЭМВ на беспроводную сеть передачи данных происходит искажение и блокирование информации, происходящее вследствие приема на устройстве как полезных сигналов, так и СК ЭМИ, которые изменяют форму полезных сигналов. Главной особенностью воздействия СК ЭМИ является формирование импульсом спектра, перекрывающего спектр широкополосного и сравнимого со спектром сверхширокополосного сигнала. Исходя из особенностей СК ЭМИ, таких как широкополосность и относительно постоянной спектральной плотности мощности сигнала, может оказывать различное влияние на различные системы беспроводной связи при одних и тех же энергетических характеристиках сигналов.

На рис. 1 изображена характеристика влияния СК ЭМИ на сверхширокополосные, широкополосные и узкополосный линии связи. По степени воздействия наиболее сильное воздействие СК ЭМИ оказывает на сверхширокополосные линии связи, далее на широколосные и узкополосные.

СК ЭМИ осуществляют воздействие на каналы передачи информации между современными устройствами перекрытием спектром помех полезных сигналов. СК ЭМИ характеризуется длительностью импульса менее 10 нс, которые могут быть как одиночными, так и следовать с определенной частотой повторения. Необходимость исследований влияния СК ЭМИ на радиоэлектронные средства обусловлена угрозой воздействия генераторов излучения на каналы передачи информации в террористических целях, а также простотой изготовления и применения данного типа воздействия. В [5] представлен метод оценки устойчивости критической инфраструктуры ПДЭМВ, а также осуществлен анализ опубликованных ранее подходов оценки рисков ПДЭМВ, оказываемых на системы критической инфраструктуры. Приводятся вопросы и показатели, включая возможные варианты ответов, проведя анализ которых можно сделать выводы об угрозах ПДЭМВ на определённую систему, а также приводится оценка определенной системы в контексте возможных вариантов сценариев осуществления ПДЭМВ, включающая показатели для анализа. В [6] приведены три вида помех: повреждение, насыщение и глушение. При повреждении высокомощные помехи могут повредить малошумящий усилитель (LNA), что приведет к постоянному отказу в обслуживании (DoS). Обычный уровень поражения LNA составляет 34 дБм в случае узкополосной помехи с шириной импульса более 1 мкс. Внеполосные помехи могут быть ослаблены входным фильтром, что позволит избежать повреждений. Однако, внутриполосные помехи не могут быть отфильтрованы. При насыщении мощный источник помех может вызвать переполнение тракта приемника и снизить чувствительность на прием сигнала. Высокоизбирательные приемники более подвержены к данному виду помехи: деградация происходит на высокочастотном каскаде, в то время как избирательность находится на каскаде промежуточной частоты, высокий динамический диапазон приемника повышает устойчивость к насыщению. При глушении маломощный источник помехи, создающий сигнал с сопоставимыми характеристиками по сравнению с полезным, может маскировать сигнал и вызывать отказ в обслуживании (DoS) в системе беспроводной связи. Если отношение сигнал / шум слишком низкое, то приемник не способен обнаружить и декодировать полезный сигнал. Эффективность данного вида атаки зависит от отношения помеха / сигнал. Высокоизбирательный приемник более устойчив к данному виду помехи. Для внутриканальных помех стратегии защиты заключаются в снижении уровня электромагнитного излучения, умных антеннах и контроле ошибок. В [7] осуществлен обзор содержания стандарта IEC 61000-4-

36 (2020) «Электромагнитная совместимость (ЭМС). Часть 4-36. Техника испытаний и измерений. Методы определения невосприимчивости к преднамеренным электромагнитным помехам (IEMI) оборудования и систем». В данном стандарте устанавливаются уровни тестирования для различных типов ПДЭМВ, включая гипополосный, мезополосный и гиперполосный тип полос, а также описываются технические особенности трех групп, осуществляющих ПДЭМВ: новичка, квалифицированного и специалиста.

В работе [8] рассмотрены определяющие параметры СК ЭМИ, такие как энергопотенциал источника, частота повторения импульсов и межимпульсный интервал следования импульсов в пакете. Энергопотенциал источника (FOM) рассчитывается как произведение напряженности электрического поля на расстояние, на котором оно образовано, то есть это напряженность поля на расстоянии 1 м. от источника. Частота повторения импульсов в единицу времени влияет на мощность образуемого поля, исходя из которого можно оценить спектральную плотность мощности. На рис. 2 показаны параметры СКИ ЭМИ.

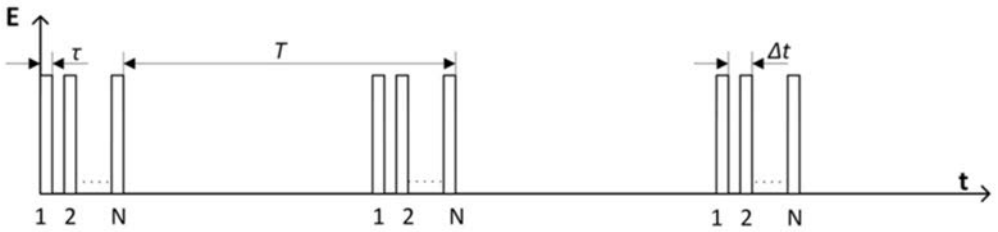


Рис. 2. Параметры СКИ ЭМИ: τ – длительность импульса, T – период следования, Δt – интервал между импульсами в пакете, N – количество импульсов в пакете

Заключение

Приведенный обзор работ по тематике обеспечения защиты информации показывает, что проведение исследований, связанных с исследованием ПДЭМВ на устройства и каналы связи Интернета вещей, является актуальным. В дальнейших работах будет проводиться анализ и исследование устойчивости каналов связи LPWAN на устойчивость к данному типу воздействий.

Список используемых источников

1. Smilty Chacko, Mr. Deepu Job. Security mechanism and Vulnerabilities in LPWAN. IOP Conf. Series: Materials Science and Engineering 396. 2018;

2. Florian Laurentiu Coman, Krzysztof Mateusz Malarski, Martin Nordal Petersen and Sarah Ruepp. Security Issues in Internet of Things: Vulnerability Analysis of LoRaWAN, Sigfox and NB-IoT. IEEE. 2019.

3. Michael Santamaria and Alan Marchiori. Demystifying LoRaWAN Security and Capacity. 2019 29th International Telecommunication Networks and Applications Conference (ITNAC). 2019.

4. Хоанг Л. Ч., Киричёк Р. В. Аналитический обзор по исследованиям влияния преднамеренного электромагнитного воздействия на беспроводные сети // Информационные технологии и телекоммуникации. 2017. Т.5. № 1. С. 114–125.

5. Thorsten Pusch, Marian Lanzrath, Michael Suhrke. IEMI Resilience Assessment of Critical Infrastructures. 2019 International Symposium on Electromagnetic Compatibility – EMC Europe 2019, Barcelona, Spain, September 2-6, 2019.

6. Stefan van de Beek, Mirjana Stojilovic, Nicolas Mora, Marcos Rubinstein, Farhad Rachidi-Haeri, Frank Leferink. Protection Strategy against IEMI for Wireless Communication Infrastructures. 2016 International Symposium on Electromagnetic Compatibility – EMC Europe 2016, Wroclaw, Poland, September 5-9, 2016.

7. William A. Radasky, Richard Hoad. Recent Developments in High Power EM (HPEM) Standarts with Emphasis on High Altitude Electromagnetic Pulse (HEMP) and Intentional Electromagnetic Interference (IEMI). IEEE. 2020.

8. Боев С. Ф., Пименов П. Н., Пронин С. А., Шевырев А. В. Влияние параметров сверхкороткоимпульсного электромагнитного излучения на функционирование радиоэлектронных средств // Труды МАИ. 2017. № 93.

УДК 004.7
ГРНТИ 49.33.29

МОДЕЛЬ ОБЪЕДИНЕНИЯ ТЕСТОВЫХ СРЕД ДЛЯ СЕТЕЙ 5G/IMT-2020

Р. В. Киричек, А. Н. Черкасова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В настоящее время сети 5G/IMT-2020 находятся на этапе тестирования используемых в них технологий. Активно создаются и объединяются различные испытательные стенды. В данной статье рассматривается обобщенная модель объединения тестовых сред, необходимая для комплексного тестирования сетей 5G/IMT-2020.

тестирование, 5G/IMT-2020, API.

Сети 5G/IMT-2020 интегрируют в себе достижения мобильных и фиксированных сетей связи и сочетают в себе новые архитектурные подходы по организации взаимодействия [1]. Такие сети становятся все более сложными для тестирования с использованием автономных испытательных стендов. Для их комплексного тестирования необходимы различные возможности и ресурсы, расположенные в различных испытательных средах. В связи с чем существует необходимость создания комплекса объединённых тестовых сред для тестирования сложных технологий.

Такой комплекс объединённых тестовых сред, можно изобразить в виде схемы, состоящей из различных функциональных блоков.

Эталонная модель объединения тестовых стендов, представленная на рисунке, состоит из частей, связанных между собой опорными точками Rfp и программными интерфейсами API [2].

API представляют собой средства, с помощью которых функциональный блок предоставляет услуги другому функциональному блоку на другом конце опорной точки Rfp.

Rfps связывают между собой функциональные блоки, и могут быть реализованы как с помощью API, так и с помощью различных протоколов.

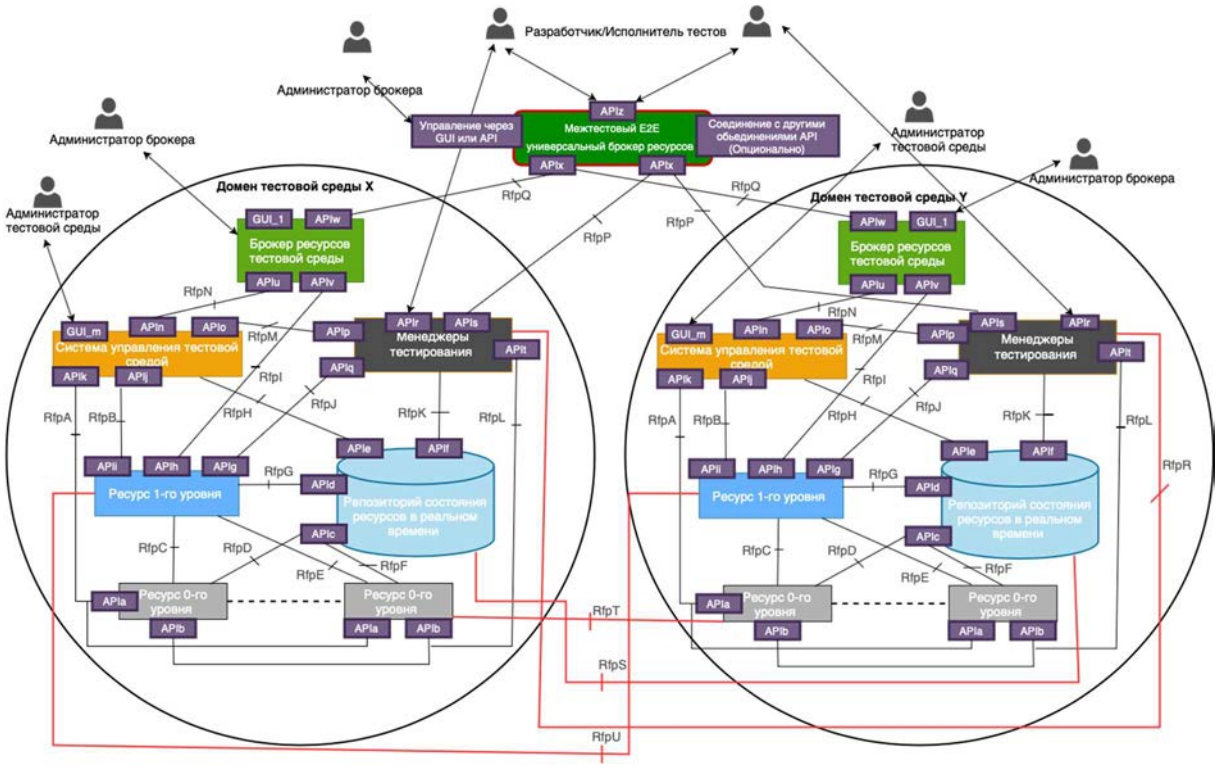


Рисунок. Общая модель для объединения тестовых сред

Эталонная модель включает в себя следующие компоненты:

1) Домен тестовой среды (Testbed domain)

Домен тестовой среды представляет собой обобщенную модель тестовой среды, имеющую возможность объединения с другой тестовой площадкой или тестовыми площадками для формирования объединения тестовых сред.

При этом внутренние функциональные блоки и опорные точки (Rfps) могут быть дополнительно детализированы при создании тестового стенда конкретного типа, например, тестового стенда сети радиодоступа RAN или тестового стенда Интернета вещей IoT [3] и т. д.

В целом домен тестовой среды состоит из следующих функциональных блоков:

- *Брокер ресурсов тестовой среды (Testbed resource broker)*

Данный функциональный блок является точкой входа для пользователей тестового стенда для запроса ресурсов через универсальный брокер ресурсов End-to-End (E2E). Ресурсы могут быть запрошены пользователями тестового стенда как для использования в тестовых сценариях автономным способом (только в пределах домена тестового стенда), так и для использования в объединённых тестовых средах с другими возможностями и ресурсами, размещенными в других местах.

Запросы пользователей могут быть либо приняты, либо отклонены брокером ресурсов тестового стенда.

•*Система управления тестовой средой (Testbed management system)*

Система управления тестовой средой позволяет предоставлять услуги тестовой среды потенциальным пользователям: устанавливать связь с другими испытательными стендами, подключать или отключать отдельные компоненты внутри блока или через другие испытательные стенды, в соответствии с ранее принятыми политикам и соглашениям.

Всеми активами тестового стенда управляет администратор тестовой среды, используя при этом для управления графический интерфейс.

•*Менеджеры тестирования (Test managers)*

Этот функциональный блок представляет собой блок, который используется пользователями тестовой среды для разработки, компиляции и выполнения тестов.

Пользователь тестовой среды получает доступ к экземпляру менеджера тестов, предоставленный брокером ресурсов тестовой среды целевого тестового стенда после принятия запроса, отправленного пользователем ранее через межтестовый универсальный брокер ресурсов E2E для объединённых тестовых сред.

Затем пользователь тестовой среды может либо использовать набор готовых тестов на менеджере тестирования, либо же загрузить несколько наборов тестов самому извне, если это позволяет домен тестовой среды, а после скомпилировать и/или выполнить тестовые примеры.

•*Ресурс 1-го уровня (Level-1 resource)*

Данный функциональный блок может рассматриваться в виде компоненты управления ресурсами, оркестровки и контроля системы.

Этот функциональный блок, может рассматриваться в определенном сценарии тестирования либо как тестируемый компонент или тестируемая система, либо как ресурс, необходимый для тестового сценария.

В пределах концепции Network Slicing – ресурс 1-го уровня расположен на уровне архитектуры управления и контроля базовой сетевой инфраструктуры. Примерами такого ресурса уровня 1 являются OSS/BSS, универсальный оркестратор услуг E2E, контроллер SDN и др.

Концепция многоуровневой нарезки Network Slicing играет важную роль в построении домена тестовой среды, так как необходимо обеспечивать поддержку работы нескольких независимых пользователей тестового стенда, для которых важно запускать тесты независимо друг от друга.

•*Ресурс 0-го уровня (Level-0 resource)*

Аналогично Ресурсу 1-го уровня, данный функциональный блок может рассматриваться в определенном сценарии тестирования как тестируемый компонент или тестируемая система, или же как ресурс, необходимый для тестирования.

В концепции Network Slicing Ресурс 0-го уровня располагается на уровне сетевой инфраструктуры. Примерами ресурса 0-го уровня могут быть стек протоколов, физическая сетевая функция PNF или виртуализированная сетевая функция VNF в целом, сетевой коммутатор, маршрутизатор, базовая станция и др.

•*Репозиторий состояния ресурсов в реальном времени (Real-time resources state repository)*

Данный функциональный блок представляет собой базу состояний ресурсов тестовых сред в реальном времени, которые могут рассматриваться в определенном тестовом сценарии как тестируемый компонент или тестируемая система, или же как ресурсы, необходимые для тестирования.

Состояние ресурсов 1-го и 0-го уровня должно постоянно отслеживаться в реальном времени, чтобы брокер ресурсов тестовой среды мог иметь актуальную информацию о возможности размещения новых тестовых сценариев или запросов от пользователей тестовой среды и взаимодействовать с оркестрантами для создания новых срезов ресурсов для обслуживания новых поступающих требований.

2) Межтестовый E2E универсальный брокер ресурсов (Inter-testbed E2E universal resource broker for testbeds federation)

Этот функциональный блок представляет собой основную точку входа в систему объединенных тестовых площадок для потенциальных пользователей.

Межтестовый универсальный брокер ресурсов E2E для объединения тестовых сред поддерживает информационный реестр тестовых площадок. Он позволяет потенциальному пользователю услуг тестовой среды, т.е. разработчику/исполнителю тестов, найти тестовые площадки, которые доступны и принимают новые запросы в данный момент времени, а также позволяет получать информацию о взаимосвязи тестовых сред.

Кроме того, предоставляется графический интерфейс управления или API администратору брокера для управления, например, путем настройки политик, регулирующих работу и обработку, а также прием или отклонение запросов на услуги тестовых площадок, поступающих от потенциальных пользователей тестовых сред.

3) Участники

Кроме того, существует несколько ролей участников, которые взаимодействуют с некоторыми функциональными блоками эталонной схемы:

•*Администратор тестовой среды (Testbed admin)*

Участник, который использует интерфейс, предоставляемый тестовой средой, для управления и подготовки тестовой среды, а также для взаимодействия с межтестовым универсальным брокером ресурсов E2E при объединении тестовых сред. Администратор тестовой среды устанавливает связь с другими тестовыми площадками, которые должны быть связаны с данной тестовой площадкой, чтобы обеспечить объединение ресурсов для потенциальных пользователей объединенных тестовых сред.

•*Администратор брокера (Broker admin)*

Участник, который использует интерфейс, предоставляемый брокером ресурсов тестовой среды, для управления брокером ресурсов тестовой среды. Например, для настройки политик, регулирующих его операции и обработку, а также прием или отклонение запросов на услуги тестового стенда, поступающих от потенциальных пользователей тестового стенда.

•*Разработчик/Исполнитель тестов (Test suite/cases designer and test executer).*

Участник, который использует API и/или соответствующий графический интерфейс, предоставляемый межтестовым универсальным брокером ресурсов E2E для объединённых тестовых сред, для запроса предоставления услуг на тестовой среде (независимо от того, должны ли запрашиваемые услуги предоставляться одной тестовой площадкой или несколькими объединенными тестовыми площадками). Эта роль представлена как комбинированная роль для разработчика и исполнителя тестов, но может быть разделена на отдельных участников.

Таким образом, количество тестовых стендов для сетей 5G/IMT-2020, имеющих собственные API и различные ресурсы и возможности, возрастает. Кроме того, исходя из сложности новых ИКТ-технологий, существует потребность использования вместе несколько разнообразных тестовых площадок одновременно. Все это вызывает необходимость использования единой модели взаимодействия тестовых систем для того, чтобы облегчить взаимодействие различных заинтересованных сторон, например, таких как разработчиков или операторов связи.

Данная модель позволяет разрабатывать согласованные и совместимые стандарты и рекомендации, относящихся к тестированию сетей 5G/IMT-2020.

Список используемых источников

1. Волков А. Н., Мутханна А. С. А., Кучерявый А. Е. Сети связи пятого поколения: на пути к сетям 2030 // Информационные технологии и телекоммуникации. 2020. Том 8. № 2. С. 32–43. DOI 10.31854/2307-1303-2020-8-2-32-43

2. ITU-T Recommendation Q.4068. Open application program interfaces (APIs) for interoperable testbed federations. ITU-T, 2021

3. Agarwal, Rachit & Gómez Fernández, David & Elsaleh, Tarek & Gyrard, Amelie & Lanza, Jorge & Sánchez, Luis & Georgantas, Nikolaos & Issarny, Valérie. (2016). Unified IoT ontology to enable interoperability and federation of testbeds. 70-75. 10.1109/WF-IoT.2016.7845470.

УДК 004.75
ГРНТИ 20.15.05

ФУНКЦИОНАЛЬНАЯ МОДЕЛЬ ПРОТОТИПА ПРОГРАММНОГО СРЕДСТВА ПОДМЕНЫ МЕТОК L2 VPN MPLS-ТУННЕЛЕЙ

А. В. Кирьянов, А. Ю. Торопцев

Академия Федеральной службы охраны Российской Федерации

В процессе использования виртуальных частных туннелей L2 VPN MPLS возможно использование меток MPLS, обозначающих сеть используемого туннеля, для упрощения верификации типа трафика, проходящего по нему. Для исключения данной возможности произведена работа по разработке прототипа программного средства подмены меток L2 VPN MPLS туннелей.

конфиденциальный трафик, MPLS L2 VPN, идентифицирующие признаки.

Для описания функциональных возможностей программного средства и создания упрощенного представления разрабатываемого прототипа была разработана функциональная модель (рис.).

Функциональные модули рассматриваемого программного средства следующие:

1. «Модуль интерфейса пользователя» – предназначен для управления программным средством при помощи встроенного в операционную систему консольного терминала.

2. «Модуль выбора интерфейса обработки» – предназначен для указания сетевых интерфейсов вычислительной техники, с которыми будет взаимодействовать программное средство.

3. «Модуль выбора режима работы» – предназначен для указания режима работы программного средства: пропуск трафика без изменения; сбор меток MPLS [1, 2], циркулирующих в сети; пропуск трафика с изменением меток MPLS.

4. «Модуль захвата пакета данных» – предназначен для сканирования выбранного интерфейса и сбора приходящих пакетов данных, для дальнейшей их обработки.

5. «Модуль обработки пакета данных» – предназначен для передачи полученного пакета данных в системы, реализующие проверки полей IP-датаграммы.

6. «Модуль формирования базы меток MPLS» – предназначен для заполнения базы данных меток MPLS значениями меток, которые будут использоваться при подмене исходной метки.

7. «Модуль проверки метки MPLS» – предназначен для сравнения MPLS метки полученной из полей захваченной IP-датаграммы, с хранящимися в БД MPLS метками и выдачи информации о возможном значении метки на модификацию.

8. «Модуль проверки MAC-адреса» – предназначен для сравнения MAC-адреса источника пакета данных, полученный из полей захваченной IP-датаграммы, с хранящимися в базе данных (БД) разрешенными MAC-адресами.

9. «База данных MAC-адресов» – предназначена для хранения разрешенных MAC-адресов.

10. «База данных меток MPLS» – предназначена для хранения MPLS меток, которые должны быть изменены и метки им соответствующие после модификации.

11. «Модуль разрешения модификации пакета данных» – предназначен для принятия решения о модификации пакета на основе аккумулирования информации о проведенных до этого проверок.

12. «Модуль модификации пакета данных» – предназначен для произведения модификации пакета данных путем подмены IP-адреса источника и смены MPLS метки в соответствии с разработанным алгоритмом.

13. «Модуль передачи пакета данных» – предназначен для передачи обработанного пакета данных в канал связи через выделенный сетевой интерфейс передачи.

Алгоритм прохождения захваченного пакета в режиме подмены меток следующий:

Из канала связи пакет попадает в «Модуль захвата пакета данных», который передает его в «Модуль обработки пакета данных». Там выделяются

MAC-адрес источника и MPLS метка, если она имеется. Для дальнейшего прохождения пакета необходимо, чтобы «Модуль проверки MAC-адреса» сравнил MAC-адрес источника с адресами в «БД MAC» и выдал разрешение. Метка MPLS отправляется в «Модуль проверки метки MPLS» и в зависимости от выбранного режима работы проверяется на наличие в «БД MPLS» совпадения и информации о подмене, или добавляется новая метка с формированием подменных меток в «Модуле формирования базы меток MPLS». Далее пакет попадает в «Модуль разрешения модификации», который по информации, полученной от предыдущих модулей делает решение, производить подмену меток или нет. При получении положительного результата пакет переходит в «Модуль модификации пакета данных», где непосредственно производиться преобразование пакета данных. При отрицательном результате преобразование не производится. Далее пакет передается в канал связи.

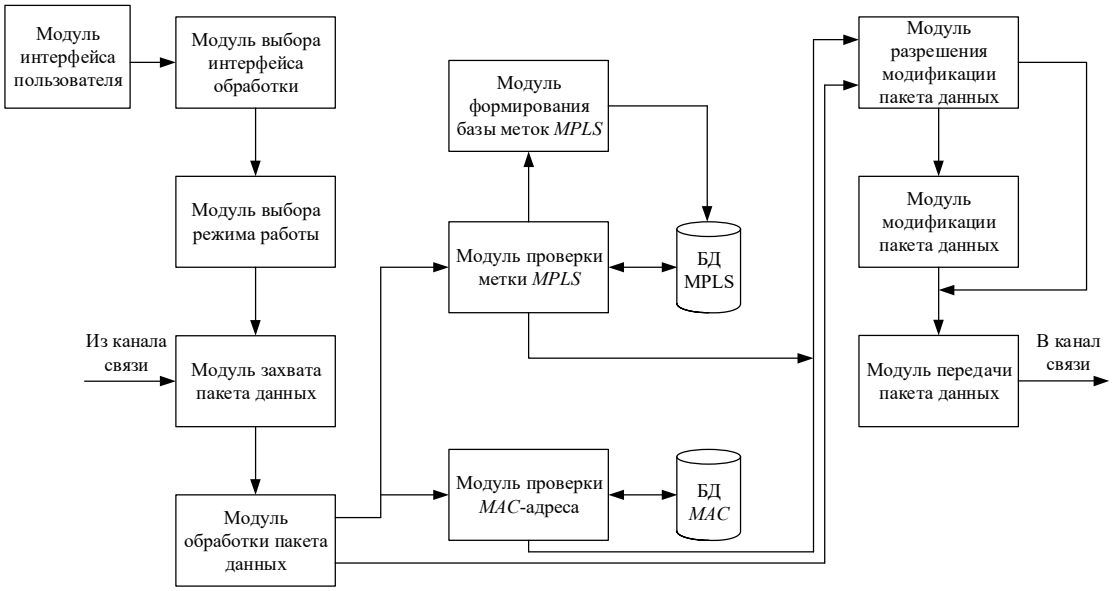


Рисунок. Функциональная модель разработанного программного средства подмены меток L2 VPN MPLS туннелей

Такой алгоритм работы позволяет избавиться от постоянных меток MPLS, заменяя их на созданный в «БД MPLS» набор подменных меток благодаря псевдослучайному методу выбора, реализованному в «Модуле проверки метки MPLS».

Реализация программного средства на основе рассмотренной функциональной модели даёт возможность устранить идентификацию трафика с использованием MPLS меток, которые присваиваются определенной сети туннеля L2 VPN MPLS [3, 4].

Список используемых источников

1. RFC RFC 5462 // IETF Documents. URL: https://datatracker.ietf.org/doc/html/rfc5462 (дата обращения: 15.03.2022).
2. Васинев Д. А. Транспортировка данных в IP-сетях: учебное пособие / под общ. ред. Д. А. Васинева. Орёл: Академия ФСО России, 2017. 361 с.
3. RFC RFC 4664 // IETF Documents. URL: https://datatracker.ietf.org/doc/html/rfc4664 (дата обращения: 15.03.2022).
4. RFC RFC 6624 // IETF Documents. URL: https://datatracker.ietf.org/doc/html/rfc6624 (дата обращения: 15.03.2022).

УДК 654.1
ГРНТИ 50.41.23

РАЗРАБОТКА БИЗНЕС-ПРОЦЕССА ПОДКЛЮЧЕНИЯ УСЛУГИ НА ОСНОВЕ TM FORUM OPEN DIGITAL ARCHITECTURE

С. В. Кисляков, В. В. Майоров

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

По мере проникновения телекоммуникационных технологий в другие сферы деятельности, ориентированные только на телекоммуникационную сферу OSS/BSS стали трудно применимыми. С 1995 года члены TM Forum создавали концепцию автоматизации операторов связи – NGOSS/Frameworx. Но на сегодняшний день инфо-телекоммуникационные технологии являются большой частью практически во всех сферах жизни – банков, здравоохранения и т.д. Концепция NGOSS/Frameworx не позволяет свободно автоматизировать IT-решения для других сфер деятельности. Поэтому эволюционной ступенью в направлении автоматизации других отраслей члены TM Forum начали создание новой концепции под названием Open Digital Architecture (ODA). При этом ODA будет продолжать поддерживать автоматизацию операторов связи. Поставщики программных решений будут вынуждены применять новые принципы и рекомендации для своих разработок. В данной работе был разработан на основе ODA бизнес-процесс подключения услуги клиенту.

открытая цифровая архитектура, Open Digital Architecture, ODA, eTOM, Operations Support System, Business Support System.

Введение

На текущий момент на рынке телекоммуникаций, операторов и поставщиков услуг связи появляется всё больше новых компаний, которые предоставляют своим пользователям набор идентичных услуг. Тем самым они находятся в среде естественного конкурентного рынка и ведут постоянную

борьбу за внимание и привлечение новой клиентской аудитории. Операторам приходится идти по пути понижения стоимости своих услуг, при этом сохраняя или даже улучшая качества предоставления услуг. При построении новых бизнес-процессов поставщики цифровых услуг связи опираются на рекомендации NGOSS/Frameworx, которые были разработаны в рамках некоммерческой организации TeleManagement Forum исключительно для сферы телекоммуникаций. Благодаря NGOSS/Frameworx поставщикам цифровых услуг предоставляется возможность уменьшить временные затраты на реализацию процессов и снизить эксплуатационные расходы, за счёт внедрения систем поддержки операционной деятельности – OSS (Operations Support Systems). На данный момент многие предприятия занимаются активной разработкой и вносят вклад в архитектуру ODA (Open Digital Architecture), которая задает новое видение систем эксплуатационной поддержки бизнеса, а также де-факто стандарт для проектирования открытых цифровых платформ. В разработку ODA входят актуальные и постоянно обновляющиеся идеи от множества групп разработчиков. Разработчики показывают своё стремление предоставить архитектуру на основе моделей, метаданных, микросервисов и четкого набора нормализованных API. В рамках ODA члены TM Forum создают общие требования и рекомендации, которые в будущем будут лежать в основе архитектуры информационных систем. Целью данной работы является разработка бизнес-процесса подключения услуги для оператора связи с использованием ODA.

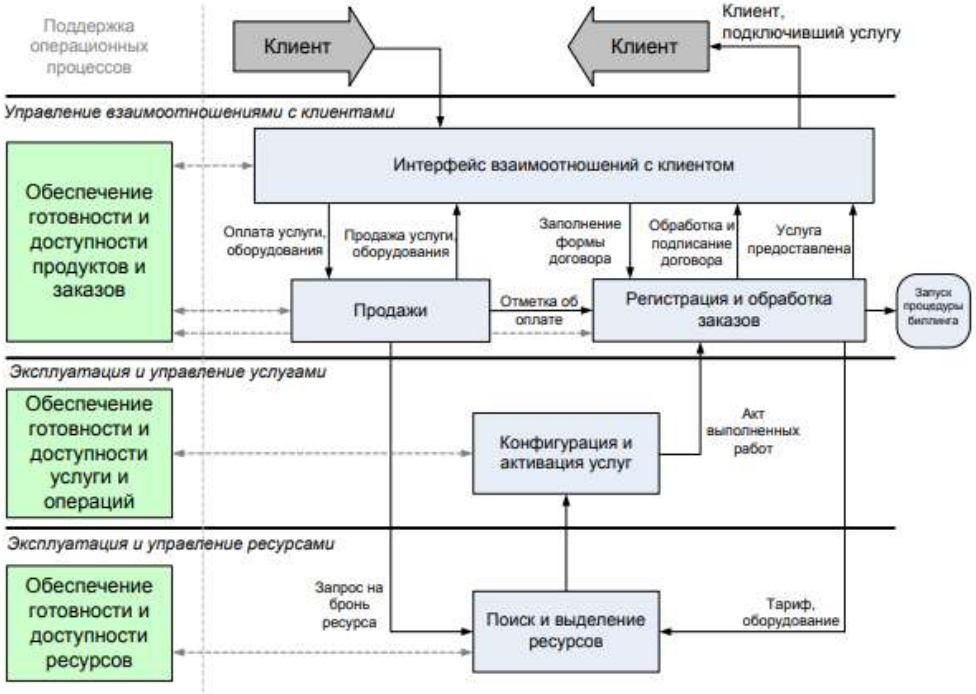


Рис. 1. Бизнес-процесс подключения услуги, разработанный на основе карты eTOM

Бизнес-процесс подключения услуги, разработанный на основе карты eTOM включал в себя следующие группировки бизнес-функций (рис. 1): «Интерфейс взаимоотношений с клиентом», «Регистрация и обработка заказов», «Продажи», «Конфигурация и активация услуги», «Поиск и выделение ресурсов». В области «Операционная поддержка и готовность» задействованы: «Обеспечение готовности и доступности продуктов и заказов», «Обеспечение готовности и доступности услуги и операций», «Обеспечение готовности и доступности ресурсов». При получении уведомления о наличии технической возможности для предоставления услуги клиент заполняет договор, а через функциональность «Продажи» оформляются документы на оплату и оборудования. Здесь же происходит бронирование ресурса и оборудования под необходимый тариф. Далее происходят «Активация и конфигурация услуг». В тот же момент начинается выполнение процедуры биллинга. Отметка об оплате клиентом услуги и оборудования через электронный банковский функционал должна поступать в базу данных.

Анализ функциональной архитектуры ODA

Структура функциональных блоков ODA отлична от структуры eTOM. Каждый из функциональных блоков ODA представляет собой группу бизнес-функций, которые реализуются внутри предприятия поставщика цифровых услуг. Функциональная архитектура ODA нацелена на замену сложившейся архитектуры TM Forum Frameworx [1].

Блок управления взаимодействием (Engagement Management) представляет собой место взаимодействия между предприятием и его экосистемой и обеспечивает цифровое безопасное взаимодействие всех взаимосвязанных сторон. Блок управления взаимоотношениями с партнерами (Party Management) обрабатывает все взаимодействия и данные, связанные с предприятием, и включает совокупность процессов идентификации, которые необходимы для управления отношениями сторон. Блок управления маркетингом и продажами (Core Commerce Management) представляет собой часть предприятия, которая занимается обеспечением прибыльного обмена товарами и услугами. Производственный блок (*Production Block*) отвечает за доставку и управление жизненным циклом служб клиентского и ресурсного обслуживания. Блок интеллектуального управления (*Intelligence Management*) использует аналитические данные для выработки данных для поддержки принятия решений, исполнения рекомендаций. Более глубокий анализ функциональности блоков ODA представлен в таблице.

ТАБЛИЦА. Сравнение функциональных блоков eTOM и ODA

eTOM	ODA
Функциональность блока операционных процессов (Operations): • Управление взаимоотношениями с клиентами • Эксплуатация и управление услугами • Эксплуатация и управление ресурсами • Управление связями с поставщиками/партнерами	Функциональность блока управления архитектурой предприятия (Engagement Management): • Пользовательские интерфейсы • Аутентификация и авторизация • Управление жизненным циклом взаимодействия с пользователем • Управление клиентским путешествием • Доступ к контенту • Агрегация контента • Персонализация контента • Управление пользовательским интерфейсом (оркестровка)
Функциональность блока стратегия, инфраструктура и продукт (Strategy, Infrastructure & Product): • Управление маркетингом и предложением • Разработка и управление услугами • Разработка и управление ресурсами • Разработка и управление цепочками поставок	Функциональность блока управления бизнесом (Core Commerce Management): • Управление продуктом • Управление предложениями • Управление запасами • Управление заказами • Управление лояльностью
Функциональность блока управления предприятием (Enterprise Management): • Стратегическое и производственное планирование • Управление рисками предприятия • Управление эффективностью предприятия • Управление знаниями и исследованиями • Управление финансами и активами • Управление связями с заинтересованными лицами и внешними сторонами • Управление персоналом	Функциональность блока управления маркетингом и взаимодействия с рынком (Party Management): • Управление платежным аккаунтом • Управление взаимоотношениями с партнерами • Управление взаимоотношениями с клиентами • Оплата • Выставление счетов
	Функциональность производственного блока (Production Block): • Управление услугами • Управление ресурсами
	Функциональность блока интеллектуального управления (Intelligence Management): • Сбор и анализ операционных данных

eTOM	ODA
	• Отслеживание действий • Отслеживание бюджета, обеспечение доходов или выявление мошенничества на основе анализа трафика • Использование больших объемов данных

Из таблицы видно, что блоки должны будут наполняться данными из eTOM, поэтому Open Digital Architecture станет высоко уровневой моделью, а карты eTOM и TAM продолжат оставаться ориентированными сугубо на сферу телекоммуникаций [2]. Таким образом, бизнес-процесс подключения услуги на основе ODA может выглядеть как показано на рис. 2. Обращение клиента, анализ технической возможности подключения услуги перешли в Блок управления маркетингом. Функции формирования заявки сгруппированы в Производственном блоке.

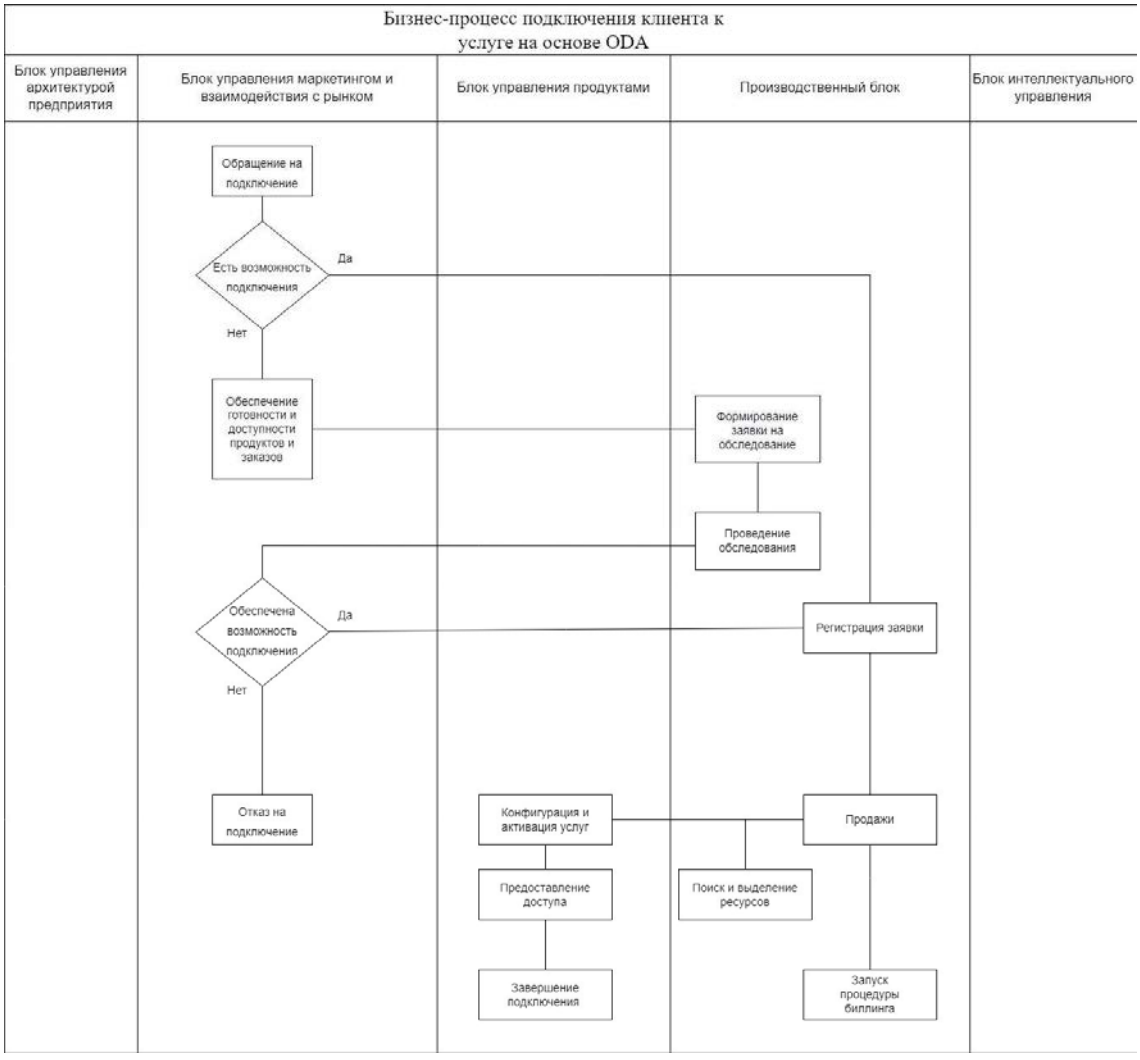


Рис. 2. Бизнес-процесс подключения услуги клиенту, разработанный на основе ODA

Заключение

ODA является высокоуровневой моделью, позволяющая разрабатывать бизнес-процессы за пределами сферы телекоммуникаций и автоматизировать их при помощи программных систем. Однако TM Forum сохраняет преемственность по отношению к своим более ранним разработкам, в частности карта eTOM и модель SID продолжают использоваться для автоматизации операторской деятельности и становятся частью ODA. Результатом данной работы является разработанный на основе ODA бизнес-процесс подключения услуги оператора связи клиенту.

Список используемых источников

1. Гольдштейн А. Б., Кисляков С. В., Феноменов М. А. Методы разработки систем управления сетями пятого поколения: учебное пособие. СПб.: СПбГУТ, 2021. 59 с.
2. IG1167 6.0.0. URL: https://www.tmforum.org/resources/standard/ig1167-oda-functional-architecture-exploratory-report-v6/ (дата обращения: 10.03.2022).

УДК 004.02
ГРНТИ 50.41.23

ИССЛЕДОВАНИЕ ХАОТИЧНОСТИ ТЕЛЕКОММУНИКАЦИОННОГО ТРАФИКА ДЛЯ ПРИМЕНЕНИЯ В РАЗЛИЧНЫХ СЦЕНАРИЯХ УПРАВЛЕНИЯ СЕТЬЮ

С. В. Кисляков, М. А. Макар

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Для целого ряда задач управления сетями связи требуется прогнозировать входящую нагрузку или интенсивность трафика, разделять и идентифицировать его. В частности, важной задачей является прогнозирование входящей нагрузки контакт-центра или планирование и размещение контейнеров с запущенными приложениями на fog-узлах сети согласно изменяющемуся спросу на них и нагрузке. Для обеих задач применялись различные подходы – строились тренд-сезонные модели, модели на основе искусственных нейронных сетей, однако результаты пока сложно назвать удовлетворительными. Сложность прогнозирования временных рядов, отражающих нагрузку контакт-центра или требующих какой-то конкретный ресурс, ставит задачу поиска новых подходов. Исследование посвящено анализу параметров процесса, порождаемого трафиком поступающей нагрузки на приложения Интернета Вещей, размещенных на edge/fog узлах сети внутри платформы с применением технологий контейнерной разработки.

теория хаоса, сеть связи, телекоммуникации.

Введение

Хаотическими называют те динамические системы, которые «имеют долговременное апериодическое поведение и демонстрируют чувствительность к значениям начальных условий». Динамическая система трактуется как «система произвольной природы (физической, химической, биологической и т. д.), которая может быть описана в какой-либо математической форме: в форме системы дифференциальных уравнений (обыкновенных и/или в частных производных), в форме отображений пространства» [1]. Теория хаоса (ТХ) позволяет предсказывать поведение сложных систем и прогнозировать последствия воздействия на них. Авторы предполагают, что применение теории хаоса может помочь спрогнозировать поведение инфокоммуникационных систем.

В доступе на сегодняшний день обнаружено совсем небольшое количество исследовательских работ по этой тематике.

В работе [2] была попытка обнаружить DDoS-атаку на сети с помощью теории хаоса. При перегрузке сети паразитным трафиком невозможно передать легитимный трафик. Предложена модель, основанная на ТХ, которая позволяет обнаруживать атакующий трафик во время передачи и фильтровать его. Идея состояла в том, чтобы отличить DDoS-трафик (который предположительно является «хаотичным») и легитимный трафик на сети. В результате был представлен алгоритм, который может предсказывать характер сетевого трафика в динамической системе. С помощью моделирования исследователи доказали, что DDoS-атаки могут быть обнаружены, поскольку они вызывают изменение фазового пространства сети.

В статье [3] была произведена попытка краткосрочного прогнозирования и анализа телеком трафика для построения плана развития предприятия. Операторов связи в Китае беспокоят прогнозы спроса на телекоммуникационный трафик, так как результаты прогнозов напрямую влияют на будущее развитие телекоммуникационных предприятий. Было доказано, что предложенная модель имеет лучший результат прогнозирования.

В [4] производился анализ возникновения хаотических явлений в телеком сетях с целью снижения их влияния на пропускную способность сети.

В [5] обсуждается прогнозирование нагрузки на контакт-центр с целью расчёта количества операторов. Прогнозирование нагрузки позволяет оптимально рассчитывать ресурсы контакт-центра для повышения качества обслуживания клиентов и минимизации финансовых затрат собственника на дополнительных операторов. В результате доказано, что нагрузка на контакт-центр хаотична и на основе исследования предложен оптимальный метод прогнозирования.

Для анализа динамической системы методами ТХ в первую очередь необходимо понять, является рассматриваемая система хаотичной или нет. Существует несколько подходов к решению, среди которых признание получили спектральный анализ, анализ корреляционной размерности и показателей Ляпунова (ПЛ).

Свойство чувствительности системы к начальным условиям предполагает, что две несовпадающие, но очень близкие точки фазового пространства имеют траектории, существенно отдаляющиеся друг от друга с течением времени, в результате чего минимальное изменение значений начальных условий такой системы приводит к существенным её изменениям через определенный промежуток времени. Для измерения скорости расхождения близких траекторий применяется старший показатель Ляпунова (экспонента Ляпунова), положительное значение которого идентифицирует присутствие хаотических процессов в этой системе. Несколько ПЛ образуют спектр Ляпунова при фиксировании расхождений траекторий по каждому из направлений, определяемых координатами фазового пространства.

Показатель Ляпунова в данном случае является самым строгим критерий хаотичности процесса, так как положительный ПЛ указывает на хаотическую динамику, а фрактальная структура орбиты в свою очередь указывает на присутствие странного аттрактора, что не всегда является показательным.

В настоящее время данное понятие, «странный аттрактор», приобрело больше собирательный смысл, который используют, когда хотят подчеркнуть хаотичность изучаемой системы [6], так как известно, что существуют странные нехаотические аттракторы [7], которые имеют фрактальную структуру, но система с таким аттрактором не обладает хаосом ни в каком смысле, поэтому «странная» фрактальная структура напрямую не свидетельствует о хаотичности системы, для этого необходимо выполнение условия с показателем Ляпунова – он должен быть неотрицательным.

Анализ нагрузки на платформы IoT

Современные решения в области Интернета Вещей создаются с применением топологий на базе туманных вычислений с использованием сетевых устройств вне центра обработки данных для обработки для обработки данных ближе к пользователю. Повышение спроса и необходимость в поддержке заданных параметров качества повышает востребованность такого подхода для обработки данных от оконечных устройств.

В качестве основы для создания платформы может быть использован Kubernetes, который позволяет управлять процессами доставки приложений в рамках распределенной инфраструктуры с использованием контейнериза-

ции. Kubernetes предоставляет большой набор готовых компонент для размещения приложений с помощью контейнеров с применением механизмов балансировки нагрузки и масштабирования приложений.

Задачи масштабирования в условиях ограниченных ресурсов на узлах туманных вычислений становятся крайне актуальными. Встроенные механизмы позволяют успешно осуществлять масштабирование с использованием облачной инфраструктуры.

В работе [8] был произведен анализ методов машинного обучения для прогнозирования потребления вычислительных ресурсов контейнерных приложений в кластере. В качестве решения были применены методы машинного обучения и получены сравнительные оценки для каждого из них, а также описан сценарий их внедрения для оптимизации задач масштабирования приложений на базе туманных вычислений.

Авторы данной статьи предполагают, что для анализа и прогнозирования в данной области могут применяться методы ТХ. Для этого в первую очередь необходимо вычислить старший показателя Ляпунова (СПЛ) для детектирования присутствия хаоса в трафике поступающей нагрузки на приложения Интернета Вещей, размещенных на edge/fog узлах сети внутри платформы с применением технологий контейнерной разработки.

Для анализа данных воспользуемся пакетом TISEAN 3.0.1, предназначенного для анализа временных рядов с помощью методов, основанных на теории нелинейных детерминированных динамических систем (ТХ) [9]. Программный пакет установлен на виртуальную машину с операционной системой Ubuntu 16.04, развернутой на основе Oracle VM VirtualBox.

Вычисления производились с помощью утилиты lyap_k. Данная утилита оценивает СПЛ заданного набора скалярных данных с помощью алгоритма Канца [10]. Результатом работы является функция логарифма коэффициента разбегания траекторий от времени:

$$S(\varepsilon, m, \Delta n) = \frac{1}{N}\sum_{n_0=1}^{N} \ln\left(\frac{1}{|U(S_{n_0})} \times \sum_{S_n \subset U(S_{n0})} \left|S_{n_0+\Delta n} - S_{n+\Delta n}\right|\right), \quad (1)$$

где ε – окрестность точки S_{n_0}; m – размерность пространства; Δn – время; $U(S_{n_0})$ – окрестность точки S_{n_0} диаметра ε.

Если данная функция имеет линейный участок, на котором она возрастает, то тангенс угла наклона прямой, аппроксимирующей данный участок, будет максимальным показателем Ляпунова.

На вход подавались значения трафика. Выборки соответствуют разному времени нагрузки на приложения, соответственно, имеют разную ин-

тенсивность поступления трафика. В результате применения утилиты получаем графики со значениями коэффициента растяжения с разными ε, образующими Ляпуновский спектр, представленный на рис.

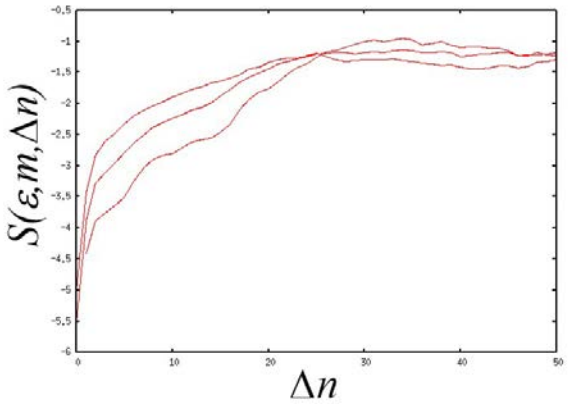


Рисунок. Спектр показателей Ляпунова

Выводы и дальнейшие исследования

По полученному графику видно, что он имеет пологий участок, что говорит о том, что в анализируемых данных присутствует экспоненциальное изменение расстояний между траекториями (экспоненциальной расходимости) и, вследствие этого, у процесса есть признаки хаотичности.

Вычисление старшего показателя Ляпунова, который однозначно скажет, хаотичен ли процесс, является следующим шагом исследования, но на данном этапе можно утверждать, что данные подходят для анализа с точки зрения Теории Хаоса.

Список используемых источников

1. Lorenz E. N. Deterministic nonperiodic flow // Journal of the Atmospheric Sciences. 1963. № 20 (2). pp. 130–141.

2. Chonka, A., Singh, J., & Zhou, W. Chaos theory based detection against network mimicking DDoS attacks // IEEE Communications Letters. 2009. 13 (9). pp. 717–719.

3. Li, F., Xin, Z. H., Li, M., & Shen, Z. W. (2010). An Empirical Research on Telecommunication Traffic Forecasting Based on Chaos Theory // 2010 International Conference on Management and Service Science.

4. Karpukhin, A., Kirichenko, L., Gritsiv, D., & Tkachenko, A. Mathematical modelling of infocommunication systems by means of chaos theory methods // 2014 First International Scientific-Practical Conference Problems of Infocommunications Science and Technology.

5. Гольдштейн А. Б., Кисляков С. В., Феноменов М. А. Методы теории хаоса для задач динамического управления контакт-центрами // Труды учебных заведений связи. 2021. № 7 (2). С. 18–23.

6. Лоскутов Александр. Математические основы хаотических динамических систем // Курс лекций. Успехи физ. наук. 2007. Т. 177, No 9. С. 989–1015.

7. Grebodgi C., Ott E., Pelican S., Yorke J. Strange attractor that are not chaotic // Physica. 1984. Vol. D13.

8. Кисляков С. В., Мордвинов Е. Ю. Анализ методов машинного обучения для прогнозирования потребления вычислительных ресурсов контейнерных приложений в кластере // Актуальные проблемы инфотелекоммуникаций в науке и образовании. X Юбилейная Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4 т. СПб.: СПбГУТ, 2021. Т. 1. С. 480–484.

9. TISEAN 3.0.1 Nonlinear Time Series Analysis // URL: https://www.pks.mpg.de/tisean/Tisean_3.0.1/index.html (дата обращения: 01.03.2022)

10. Hegger, R., Kantz, H., & Schreiber, T. Practical implementation of nonlinear time series methods: The TISEAN package Chaos // An Interdisciplinary Journal of Nonlinear Science. 1999. 9 (2). pp. 413–435.

УДК 004.052
ГРНТИ 50.41.01

МЕТОДИКА ОБНАРУЖЕНИЯ МЕСТОПОЛОЖЕНИЯ НАРУШИТЕЛЯ, РЕАЛИЗУЮЩЕГО АТАКУ ДЕАУТЕНТИФИКАЦИИ НА СЕТЬ IEEE 802.11

А. Ю. Кистуга, М. М. Ковцур, М. П. Петров, В. П. Шабанов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В настоящее время беспроводные сети набирают популярность, они стали более распространенными и доступными. Из-за большой популярности участились атаки на беспроводные сети семейства IEEE 802.11, поэтому требуются новые методы и технологии, чтобы их защитить. Одна из популярных атак, которая используется злоумышленниками – это атака деаутентификации. В докладе представлена методика обнаружения местоположения злоумышленника, проводящего атаку деаутентификации на беспроводную сеть семейства IEEE 802.11.

деаутентификация, сети IEEE 802.11, методика обнаружения нарушителя.

Деаутентификация – это одна из разновидностей атак на беспроводную сеть (рис. 1), суть которой заключается в отключении клиентов от их точек доступа [1].

Большинство атак деаутентификации являются довольно простыми в реализации и используют хорошо документированные недостатки в том, как беспроводные устройства управляют соединениями. Поскольку такие пакеты, использующиеся для управления соединением не зашифрованы, злоумышленнику легко создать поддельные пакеты после прослушивания беспроводных каналов поблизости.

Протоколы семейства IEEE 802.11 описывают возможность использования специальных кадров для деаутентификации беспроводного клиента, посылаемых точкой доступа или самим клиентом.

Злоумышленнику необходимо узнать только MAC-адреса жертвы и точки доступа, которые передаются в открытом виде. Получить их можно выполнив простое прослушивание окружающей радио среды средствами набора утилит aircrack-ng или другим подобным ПО.

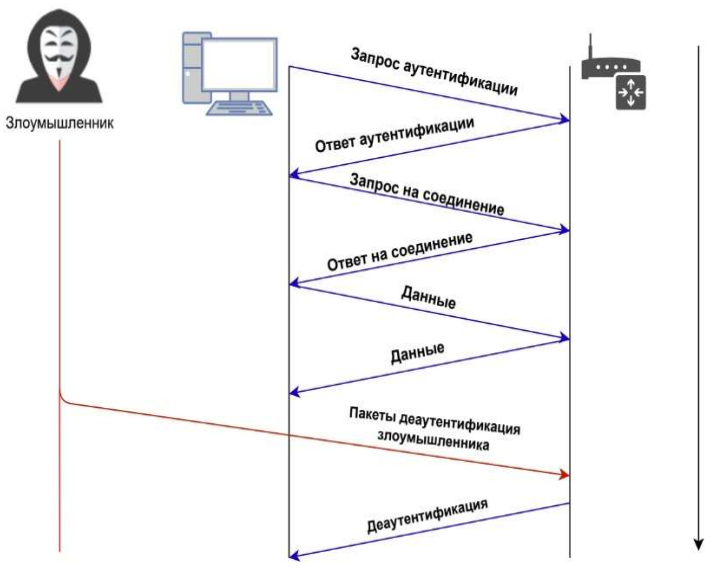


Рис. 1. Пример деаутентификации беспроводного

В случае если беспроводная сеть WLAN не защищена с применением стандарта 802.11w (PMF – *Protected Management Frame*), все устройства которые подключены к данной беспроводной сети могут быть нелегально деаутентифицированы, т. е. отключены злоумышленником. Данную уязвимость можно эксплуатировать для проведение различных атак. К примеру, злоумышленник может деаутентифицировать пользователя, чтобы узнать значение SSID, если название сети изначально скрыто или в качестве ключевого шага при выполнении атаки Evil Twin.

Для проведение атаки требуется перевести сетевую беспроводную карту в режим мониторинга и воспользоваться специализированным программным обеспечением [2].

Несмотря на то, что данный вид атаки может принести довольно много хлопот, её достаточно просто обнаружить с помощью бесплатных программ. В данной статье мы рассмотрим методику, как администратор сети может обнаружить атаку и местоположение злоумышленника с применением ноутбука, бесплатной программы Wireshark и беспроводного адаптера

Рис. 2. Фотография рабочей установки

с направленной антенной. Фотография оборудования (ноутбук, беспроводной адаптер) администратора представлена на рис. 2.

Для реализации методики администратор должен перевести свой беспроводной адаптер в режим мониторинга, установить нужный канал и запустить приложение Wireshark. После этого в приложении необходимо выбрать нужный беспроводной интерфейс и активировать перехват трафика беспроводной сети [4]. В Wireshark нужно настроить фильтрацию пакетов деаутентификации с MAC-адресом источника равным адресу точки доступа и/или адресу клиента, так как иначе Wireshark будет перехватывать и отображать много лишней информации. Фильтрация представлена на рис. 3. Используется следующий фильтр – (wlan.fc.type_subtype==0xc)&&(wlan.addr==e0:dc:ff:ec:c8:bd||wlan.addr==d0:be:c3:cd:b0). wlan.fc.type – фильтр пакетов деаутентификации, wlan.addr – адрес злоумышленника и беспроводного клиента.

Рис. 3. Блок-схема методики

Поиск ведется по следующей методике: администратор берет оборудование (ноутбук, беспроводной адаптер и антенна), как показано на рисунке 5, и выполняет перехват пакетов в беспроводной сети. Расположив антенну под углом 30 градусов перпендикулярно земле, поворачивается вокруг своей оси, фиксируя время и градус поворота. Установка в рабочем положении представлена на рис. 4.

(wlan.fc.type_subtype==0xc)&&(wlan.addr==e0:dc:ff:ec:c8:bd || wlan.addr==d0:be:76:c3:cd:b0)

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	XiaomiCo_ec:c8:bd	Tp-LinkT_c3:cd:b0	802.11	66	Deauthentication, SN=3695, FN=0, Flags=.....C
3	0.001234559	Tp-LinkT_c3:cd:b0	XiaomiCo_ec:c8:bd	802.11	66	Deauthentication, SN=3696, FN=0, Flags=.....C
4	0.001940495	XiaomiCo_ec:c8:bd	Tp-LinkT_c3:cd:b0	802.11	66	Deauthentication, SN=3697, FN=0, Flags=.....C
6	0.009038102	Tp-LinkT_c3:cd:b0	XiaomiCo_ec:c8:bd	802.11	66	Deauthentication, SN=3698, FN=0, Flags=.....C
7	0.009689541	XiaomiCo_ec:c8:bd	Tp-LinkT_c3:cd:b0	802.11	66	Deauthentication, SN=3699, FN=0, Flags=.....C
11	0.021324177	XiaomiCo_ec:c8:bd	Tp-LinkT_c3:cd:b0	802.11	66	Deauthentication, SN=3701, FN=0, Flags=.....C
13	0.026203965	Tp-LinkT_c3:cd:b0	XiaomiCo_ec:c8:bd	802.11	66	Deauthentication, SN=3702, FN=0, Flags=.....C
16	0.032122712	XiaomiCo_ec:c8:bd	Tp-LinkT_c3:cd:b0	802.11	66	Deauthentication, SN=3703, FN=0, Flags=.....C

Рис. 4. Фильтрация пакетов Wireshark

Далее администратор анализирует график в Wireshark по полученный из информации о перехваченных пакетах. Максимальное значение пакетов соответствует направлению, в котором находится нарушитель [3]. Пример показан на рис. 5.

Далее администратор перемещается в направлении, определенном в предыдущем шаге, и повторяет предыдущие шаги [5].

Рис. 5. Установка в рабочем положении

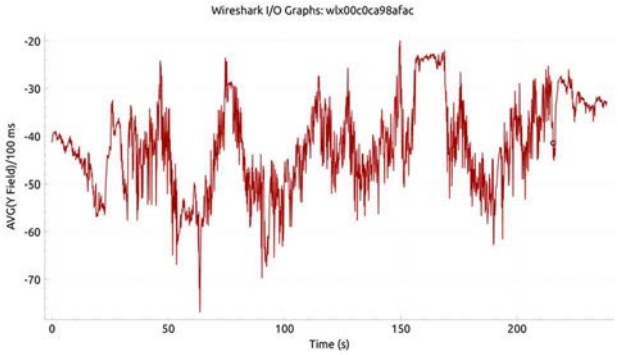


Рис. 6. График пакетов деаутентификации за время сканирования

В данной статье описана методика позиционирования источника деаутентификации с помощью направленной антенны и программы Wireshark. В результате анализа пакетов методика позволяет администратору обнаружить приблизительное местоположение злоумышленника.

Список используемых источников

1. Андрианов В. И., Романов Г. Г., Штеренберг С. И. Экспертные системы в области информационной безопасности // Актуальные проблемы инфотелекоммуникаций в науке и образовании. IV Международная научно-техническая и научно-методическая конференция: сб. науч. ст. СПб.: СПбГУТ, 2015. С. 193–197.

2. Ковцур М. М., Пешков А. И., Мисливский Б. С., Петров В. А., Докшин А. Д. Программа для автоматизированного сбора трафика беспроводных сетей IEEE 802.11 // Свидетельство о регистрации программы для ЭВМ 2021680157, 07.12.2021. Заявка № 2021669199 от 26.11.2021.

3. Герлинг Е. Ю., Ковцур М. М., Фёдорова А. Э. Разработка веб-интерфейса для системы мониторинга беспроводных сетей семейства IEEE 802.11 // Актуальные проблемы инфотелекоммуникаций в науке и образовании X Юбилейная Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2021. С. 224–228.

4. Ахрамеева К. А., Ворошнин Г. Е., Ковцур М. М. Исследование уязвимостей оборудования MIKROTIK к атакам на беспроводные сети // Актуальные проблемы инфотелекоммуникаций в науке и образовании. X Юбилейная Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2021. С. 57–63.

5. Сахаров Д. В., Красов А. В. Миняев А. А., Методика оценки эффективности системы защиты информации территориально-распределенных информационных систем // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2020. № 3. С. 26-32.

6. Дешевых Е. А., Конюхов В. М., Крылов К. Ю., Ушаков И. А. Исследование методов защиты от инсайдерских атак // Актуальные проблемы инфотелекоммуникаций в науке и образовании. IV Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 2-х т. СПб.: СПбГУТ, 2015. С. 310–313.

УДК 621.39
ГРНТИ 49.37.29

ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ РАЗВИТИЯ ГРУППОВОГО ПРИМЕНЕНИЯ БЕСПИЛОТНЫХ ЛЕТАТЕЛЬНЫХ АППАРАТОВ

Я. В. Кичко

Военная орденов Жукова и Ленина Краснознаменная академия связи
имени Маршала Советского Союза С. М. Буденного

В статье рассмотрены тенденции применения беспилотных летательных аппаратов, основные направления их развития в США и России. Проанализированы возможности современных беспилотных летательных аппаратов. Выявлены недостатки существующих комплексов, не позволяющие обеспечить требуемую оперативность передачи данных при групповом применении беспилотных летательных аппаратов.

беспилотные летательные аппараты, групповое применение БПЛА, алгоритмы обмена данными, маршрутизация пакетов данных, распределение потоков, оптимизация системы маршрутных таблиц.

Инновационное развитие оборонно-промышленного комплекса Российской Федерации, сохранение лидерства в разработке и производстве новых (перспективных) образцов (комплексов, систем) вооружений, военной и специальной техники является одной из важных задач для обороны нашей страны [1]. Исследования и разработки в области робототехнических комплексов (систем) военного, специального и двойного назначения входят в приоритетные направления развития науки, технологий и техники [2].

Беспилотный летательный аппарат (БПЛА), искусственный мобильный объект (летательный аппарат), как правило, многоразового использования, не имеющий на борту экипажа (человека-пилота) и способный самостоятельно целенаправленно перемещаться в воздухе для выполнения различных функций в автономном режиме (с помощью собственной управляющей программы) или посредством дистанционного управления (осуществляемого человеком-оператором со стационарного или мобильного пульта управления) [3].

Тенденции развития и применения в военной сфере беспилотной авиационной техники обусловливают активизацию и актуальность разработок по созданию многофункциональных комплексов (МФК) с использованием БПЛА.

МФК создаётся как боевая система, предназначенная для выполнения следующих функций [4]:

– разведывательной – мониторинг участков местности, надводной поверхности, воздушного пространства, объектов промышленности и инфраструктуры; картографирование; наблюдение за участками шоссе, дорог, путей и движущимися транспортными средствами; поиск, обнаружение и сопровождение войсковых объектов (целей);

– ударной (боевой) – обнаружение и поражение стационарных и движущихся объектов (целей), корректировка огня артиллерии, подсветка целей и контроль результатов стрельбы;

– транспортной – доставка, перемещение по воздуху различных грузов.

Наиболее сложными для реализации задачами являются разведка и выполнение ударных функций.

Принципом решения разведывательно-ударных задач является групповое применение БПЛА и объединение всех объектов управления в единый разведывательно-ударный контур.

Групповое применение БПЛА и пилотируемых самолетов имеет очевидные преимущества и позволяет гибко решать широкий круг задач. Вследствие этого проекты такого рода прорабатываются в ряде стран, и некоторые из них уже доведены до летных испытаний того или иного рода. При этом на вооружение такие комплексы пока не принимались.

Проведённый анализ ряда опубликованных документов о развитии беспилотной авиации в США, показывает, что основными направлениями развития комплексов с БПЛА, на период до 2035 года являются:

1. Расширение круга решаемых задач комплексами с БПЛА путем:

– интеграции комплексов с БПЛА в единое информационно-коммуникационное пространство на театре военных действий и в систему управления воздушным движением;

– повышения автономности действий БПЛА и обеспечение управления одним оператором несколькими БПЛА одновременно;

– создания и совершенствования средств видовой и радиотехнической разведки, алгоритмов их работы и обработки сигналов;

– стандартизации аппаратуры и протоколов обмена данными, создания унифицированных станций управления, носимых терминалов отображения разведывательной информации и управления нанесением огневых ударов;

– увеличения скорости передачи и объёмов, передаваемых данных.

2. Выработка тактики и способов применения, пилотируемых летательных аппаратов (ЛА) и БПЛА в единых боевых порядках.

Перспективным является развитие группового применения БПЛА различных типов, требующее информационно-технического сопряжения большого количества абонентов, и позволяющее:

– расширить возможности комплексов с БПЛА при совместном функционировании в разведывательно-ударной системе;

– повысить эффективность и уровень ситуационной осведомленности органов управления войсками за счет повышения полноты, оперативности и актуальности данных, получаемых при множественном применении БПЛА в зоне ответственности.

В США и странах НАТО ведутся работы по перспективным БПЛА группового применения, основными направлениями, которых являются:

- Создание разведывательно-ударных БПЛА, наземного и воздушного старта низкой стоимости.
- Роевой полет «swarm» БПЛА различных классов (включая средние, тяжелые).
- Совместное применение БПЛА и пилотируемых ЛА.

Наиболее значимые работы:

- Программа «Loyal wingman», Boeing Airpower Teaming System – создание БПЛА для применения с пилотируемыми ЛА.
- Программа «Skyborg» – БПЛА с элементами искусственного интеллекта.
- Создание разведывательно-ударного БПЛА XQ-58 «Valkyrie».
- Создание БПЛА воздушного старта X-61A «Gremlin».

Оборонная промышленность России так же прорабатывает новые концепции и решения в области беспилотной авиации. В марте 2021 г. компания «Кронштадт» представила руководителям Министерства обороны новый проект комплекса группового применения «Молния», который предполагает использования «роя» из нескольких БПЛА, обеспечивающих поддержку пилотируемого самолета [5].

Концепция «роя» предусматривает постоянный обмен данными между отдельными БПЛА и управляющим самолетом. Это позволяет решать любые поставленные задачи и гибко реагировать на различные факторы. В случае изменения обстановки или потери БПЛА задачи могут перераспределяться между активными аппаратами, в том числе, в автоматическом режиме и без участия оператора.

Необходимость повышения полноты, оперативности и актуальности данных, получаемых при множественном применении БПЛА; постоянный обмен данными; рост количества передаваемой информации; требования по сокращению временных циклов управления; несовершенство алгоритмов обмена данными; необходимость передачи больших объемов информации в режиме реального времени и оптимизации системы маршрутных таблиц – это лишь часть проблем, с которыми сталкиваются разработчики комплексов с БПЛА.

Таким образом, в настоящее время существует необходимость и возможность совершенствования алгоритмов обмена данными в комплексах с БПЛА. Это позволит повысить устойчивость сети обмена данными (СОД),

вероятность своевременной доставки сообщения, сократит цикл управления и решить ряд других актуальных проблем.

По своему замыслу, проводимые исследования, укладываются в рамки общего подхода, обозначенного в работах [6–9]. Они направлены на построение оптимального алгоритма управления СОД на сетевом уровне с учетом возможностей радиосредств по установлению связи в различных направлениях, подходящих режимах функционирования и реализации на этой основе множества возможных вариантов построения маршрутов прохождения пакетов сообщений. Направления исследований: выбор стратегии управления группировкой, маршрутизация пакетов в СОД в условии дестабилизирующих воздействий, оптимизация системы маршрутных таблиц, учет и распределение преднамеренных помех.

Список используемых источников

1. О Стратегии национальной безопасности Российской Федерации [Текст]: указ Президента РФ от 2 июля 2021 г. № 400.

2. Об утверждении приоритетных направлений развития науки, технологий и техники в Российской Федерации и перечня критических технологий Российской Федерации: указ Президента РФ от 7 июля 2011 г. № 899, в ред. от 16 дек. 2015 г. № 623.

3. Беспилотный летательный аппарат. URL: http://dev.bigenc.ru/technology_and_technique/text/4087725 (дата обращения: 12.10.2021).

4. Бабич Л. А. Групповое применение разведывательных и ударных беспилотных летательных аппаратов // Молодой ученый. 2019. № 45 (283). С. 3–6.

5. Проект беспилотного комплекса группового применения «Молния». URL: https://topwar.ru/180494-proekt-bespilotnogo-kompleksa-gruppovogo-primenenija-molnija.html (дата обращения: 16.11.2021).

6. Чуднов А. М., Путилин А. Н., Попов А. И. Комплексное управление маршрутизацией пакетов и режимами работы радиосредств в неоднородной сети передачи данных // Радиотехнические и телекоммуникационные системы. 2019. № 1. С. 46–56

7. Чуднов А. М., Курашев З. В. Принципы формирования маршрутных таблиц на основе оптимизации распределения потоков в сети передачи данных // Наукоемкие технологии в космических исследованиях Земли. 2017. Т. 9, № 6. С. 46–51.

8. Чуднов А. М., Кирик Д. И., Курашев З. В. Оптимизация распределения информационных потоков в информационной системе по показателю вероятности своевременной доставки сообщений // Радиотехнические и телекоммуникационные системы. 2017. № 2. С. 41–49.

9. Akyildiz I.F., Wang X. Wireless Mesh Networks, Wiley, Chichester, Advanced. Texts in Communications and Networking. 2009. 324 p.

Статья представлена научным руководителем,
доктором технических наук, профессором А. М. Чудновым.

УДК 621.4
ГРНТИ 49.33.29

СОВРЕМЕННЫЕ ПОДХОДЫ К ВОССТАНОВЛЕНИЮ ИНФОРМАЦИОННОГО ПРОЦЕССА В ЛОКАЛЬНЫХ ВЫЧИСЛИТЕЛЬНЫХ СЕТЯХ

И. С. Ковалёв[1], **О. И. Пантюхин**[2], **В. В. Пащенко**[1]

[1] Военная орденов Жукова и Ленина Краснознаменная академия связи имени Маршала Советского Союза С. М. Буденного

[2]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Рассмотрены современные подходы и методы восстановлению информации в локальных вычислительных сетях. Предложены новые способы восстановления информационного процесса.

резервное копирование, восстановление данных, клонирование дисков, локальная вычислительная сеть, мероприятия технические и организационные.

В автоматизированных системах управления огромную роль играет информация, циркулирующая в локальных вычислительных сетях таких систем. Дестабилизирующие факторы могут привести к различным негативным последствиям, в том числе и к потере этой информации [1].

Потеря информации может происходить по многим причинам, например: неисправность оборудования, технические сбои, ошибки персонала, недостатки программного обеспечения, воздействие вирусов, дестабилизирующее влияние внешней среды и т. д.

Чтобы избежать потерь информации по указанным причинам или, по крайней мере, свести их к минимуму, необходимо проводить мероприятия технического и организационного характера.

Создание резервной копии данных. Для всех пользователей информация, записанная в памяти устройства, имеет большое значение, тем более, если её больше нигде нет, кроме как на конкретном накопителе. Известно, что любое устройство может внезапно выйти из строя. При этом не каждый пользователь доверит данные сервису облачного хранения, да и объёмы могут превышать допустимые или за хранение придётся платить, а в случае наличия носителя-клона с файлами, они будут в безопасности.

Для выполнения оперативного восстановления информационного процесса необходимо заранее выполнить резервное копирование информации [2].

Принято выделять несколько методов резервного копирования, рассмотренных в [3].

На автоматизированном рабочем мете (АРМ) хранится информация о системе, а также все настройки (конфигурационные файлы, сетевые настройки, сведения об установленном и настроенном программного обеспечения данного компьютера. Кроме того, на нём, как правило, хранятся и пользовательские данные. Если же накопитель на жестком магнитном диске (далее по тексту диск) по какой-либо причине повреждён, службе эксплуатации приходится менять его на новый. Восстановление работоспособности начинается с ранее созданной полной копии и предполагает простой процесс запуска специальной программы с указанием пути к полной копии. После такого восстановления и входа в домен АРМ получит файлы пользователя из инкрементных или дифференциальных копий и информационный процесс восстановлен.

Для решения задачи создания хранилища резервной информации с серверов/АРМ службе эксплуатации необходимо определиться с способами создания резервных копий и предварительно рассчитать необходимый объем данного хранилища.

В настоящее время в локальных сетях специального назначения при выполнении резервного копирования (изготовлении полного образа системного диска) производится путем извлечения из АРМ его диска, с которого необходимо произвести резервное копирование и подключение диска к специальному компьютеру (технологическое рабочее место), или выполнение этих работ непосредственно на данном автоматизированном рабочем месте в режиме «покоя», т. е. при выключенном АРМ. Эти действия, как правило, производятся в нерабочее время. Но в тех ситуациях, когда необходимо производить множество различных расчётов, которые невозможно прервать или отложить, задача создания резервных копий откладывается на более позднее время. Все это может отрицательно повлиять на сам процесс восстановления работоспособности из-за несвоевременного копирования информации и, как следствие, отсутствия необходимой для восстановления информации.

Выполнение работ по созданию резервных копий информации и как следствие восстановление информационного процесса может быть организовано несколькими способами.

Первый вариант при отказе программного обеспечения, диска работоспособность АРМ в кратчайшие сроки восстановить работоспособность можно следующим способом.

Успешная загрузка операционной системы (ОС) и вход автоматизированного рабочего места в домен свидетельствуют о работоспособном состоянии данного АРМ. После чего осуществляется проверка наличия полной копии для данной автоматизированного рабочего места. Если копия есть, и, что важно, она актуальна, действий не требуется. При отсутствии полной

копии для данного АРМ происходит оповещение администратора безопасности информации о необходимости выполнения работ по созданию новой актуальной полной копии данного АРМ. Администратор планирует работы по созданию для него полной копии.

На все серверы/АРМ заранее создаются полные рабочие резервные копии для оперативного восстановления информационного процесса и возобновления работы автоматизированного рабочего места.

При изменении настроек любого АРМ, добавлении программ и приложений, на клиентской стороне появляется необходимость в создании новой полной актуальной копии. Также создание полных копий может выполняться по регламенту или при обновлениях программного обеспечения. Частое создание полных копий быстро заполнит доступный объем хранилища, что приведет к невозможности дальнейшего копирования информации.

В повседневной деятельности должностные лица периодически изменяют, создают и получают новые файлы/документы. Для того, чтобы при необходимости восстановить и такие файлы используются методы инкрементного и/или дифференциального резервного копирования. С этой целью производится проверка изменения файлов пользователей за определенный период времени в каталоге пользователя, который работает в данный момент на данном АРМ. Измененные файлы хранятся в домашнем каталоге пользователя. Если файлы подверглись изменениям, то запускается программа по созданию инкрементной и/или дифференциальной копии. Возможна установка программы, которая будет синхронизироваться с этим каталогом и хранилищем на сервере.

На следующем шаге производится проверка времени хранения копий. Если время хранения выше допустимого, производится удаление созданных ранее.

Если же на автоматизированном рабочем месте не загружается ОС или АРМ не может войти в домен, что говорит об его неисправном состоянии, такое автоматизированное рабочее место требуется восстановить. Восстановление можно выполнять или на технологическом рабочем месте при наличии полной копии, используя специальную программу, методом извлечения диска из АРМ и установкой диска в технологическое рабочее место.

При отсутствии полной копии восстановление автоматизированного рабочего места возможно выполнить только непосредственно на нём самом из загрузочного модуля или у установочных дисков, поставляемых промышленностью с последующим выполнением работ по конфигурированию и администрированию данного АРМ. После восстановления самого рабочего места, осуществляется восстановление ранее созданных пользователем рабочих документов по локальной вычислительной сети из инкрементных/дифференциальных копий. После чего планируется и создается новая полная копия.

Для обеспечения высокой надежности во все средства вычислительной техники испльзуемые в качестве серверов/АРМ можно укомплектовать дополнительным диском (далее по тексту – второй диск), на котором устанавливается программа для выполнения полного копирования основного диска. Также второй диск является хранилищем полной копии основного диска. Любая прогрмма из имеющихся [2] выполняет изготовление полной копии при полном «покое» диска с которого она делается, а также и восстановление информации с полной копии производится также при таком состоянии АРМ. Следовательно выполняя загрузку со второго диска нужно тогда, когда нужно выполнить полное копирование диска или нужно срочно восстановить информацию с полной копии в том числе и на новый диск.

После отработки программы производитьсят перезагрузка автоматизированного рабочего места. Пользователь выбирает первый (основной) диск для загрузки ОС и далее работает по вполнени своих работ, по проведению расчетов и иным работам. В случае сбоя/отказа на АРМ пользователю необходимо выполнить загрузку со второго диска и используя установленную на нем программу восстановить информационный поцесс. Измененные за время работы файлы пользователя восстановятся из дифференциальных и инкрементных копий хранящихся на сети в установленном месте. Если же вышел из строя основной диск, служба эксплуатации устанавливает на его место новый диск и дальнейшие работы выполняются аналогично.

Также предлагается использовать способ зеркального клонирование основного диска, который предполагает наличие любого внешнего диска подключаемого к автоматизированного рабочего места создания хранения полной копии. Необходимо чтобы этот диск должен имел объем достаточен для хранения клона основного диска.

Программа клонирования создаст полную копию основного диска, сохраняя всю информацию на второй диск. Процедура представляет собой перенос данных по секторам на другой диск, что позволяет в буквальном смысле «клонировать» основной диск.

В случае необходимости восстановления информации подключается диск на котором имеется клон и производиться восстановление информации.

По окончании процесса клонирования на новом диске информация будет в том же виде, что и было на оригинальном устройстве, то есть с той же операционной системой и её файлами, драйверами, установленным софтом, пользовательскими данными, настройками, паролями и прочими сведениями. При этом есть возможность выполнить полное клонирование как диска, так и или некоторых его разделов. В определённых случаях это покажется более приемлемым вариантом.

Список используемых источников

1. Бережной А. Н. Сохранение данных: теория и практика. М.: ДМК Пресс, 2016. 317 с.
2. Пащенко В. В., Ковалев И. С., Пантюхин О. И., Солодухин Б. В. Повышение устойчивости функционирования локальных вычислительных сетей систем управления специального назначения // Проблемы технического обеспечения войск в современных условиях. Труды V межвузовской научно-практической конференции: сборник. СПб.: ВАС, 2020. 520 с. С. 175–178.
3. Пащенко В. В., Ковалев И. С., Морозов И. В. Задачи службы эксплуатации по организации резервного копирования информации в локальных вычислительных сетях // Проблемы технического обеспечения войск в современных условиях. Труды VI межвузовской научно-практической конференции : сборник. СПб. : ВАС, 2021. 508 с. С. 104–107.

УДК 621.395
ГРНТИ 49.33.35

МЕТОДЫ ПОВЫШЕНИЯ КРИПТОСТОЙКОСТИ СООБЩЕНИЙ

Ю. Ф. Кожанов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Рассматриваются общие принципы симметричного шифрования с закрытыми ключами. Предложены способы повышения криптостойкости системы.

шифрование, дешифрование, криптостойкость.

Классическая модель криптосистемы приведена на рис. 1. В модели присутствуют три участника: два легальных пользователя и злоумышленник.

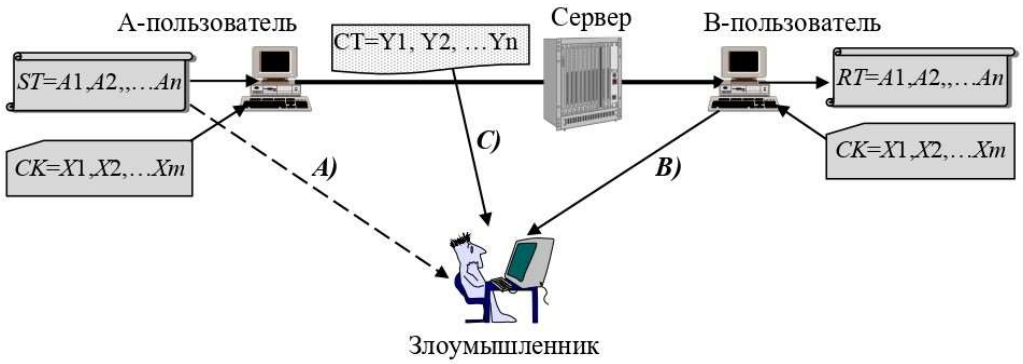


Рис. 1. Классическая модель криптосистемы

Легальные пользователи обмениваются между собой конфиденциальной информацией [1]. Для того чтобы она была недоступна посторонним лицам, сообщение на передаче преобразуется в нечитаемый (зашифрованный) текст, который получается перемешиванием открытого текста с элементами ключа шифрования по определенному алгоритму (программе).

На приеме легальный пользователь, используя ключ дешифрования, восстанавливает исходный текст. Ключи шифрования и дешифрования могут совпадать или отличаться.

Задача злоумышленника заключается в перехвате и чтении всех передаваемых сообщений. При этом предполагается, что злоумышленник имеет возможность подключения к каналу связи и ему доступны

A) Некоторые открытые тексты.

B) Алгоритм шифрования\дешифрования передаваемых сообщений.

C) Зашифрованный текст.

Первое предположение основано на том, что злоумышленник может быть знаком с ***некоторыми*** открытыми текстами, которые могут быть похищены, подсмотрены или скопированы его соучастником.

Алгоритм шифрования\дешифрования во многих случаях не является секретом.

Зашифрованный текст легко перехватывается при использовании незащищенного канала связи.

Поэтому единственным секретом является только ключ дешифрования, который при его дискредитации и позволяет злоумышленнику читать ***все*** передаваемые зашифрованные сообщения.

Легальный А-пользователь передает открытый текст $ST=A1, A2,\ldots An$, который шифруется секретным ключом $CK=X1, X2,\ldots Xm$ с использованием некоторой математической или логической функции F.

На приеме легальный В-пользователь с помощью обратных преобразований (функции F^{-1}) и того же ключа CK восстанавливает из принятого зашифрованного текста CT исходный открытый текст $RT=ST$.

Цель злоумышленника, которому доступны только зашифрованный текст (все Yi) и алгоритмы шифрования/дешифрования (F и F^{-1}), заключается в подборе такого значения CK (всех Xi), чтобы при их использовании получить осмысленный текст ST.

Процесс шифрования можно представить в виде системы из n уравнений вида

$$Y1 = F(A1, X1, X2, \ldots Xm)$$
$$Y2 = F(A2, X1, X2, \ldots Xm)$$
$$\ldots$$
$$Yn = F(An, X1, X2, \ldots Xm),$$

в которой в шифровании каждого символа участвуют все символы ключа.

Процесс дешифрования можно представить в виде системы из n уравнений вида

$$\begin{aligned} A1 &= F^{-1}(Y1, X1, X2, ...Xm) \\ A2 &= F^{-1}(Y2, X1, X2, ...Xm) \\ &... \\ An &= F^{-1}(Yn, X1, X2, ...Xm), \end{aligned} \quad (1)$$

в которой имеем $(n+m)$ неизвестных.

При известных $CK=(X1,X2,\ldots Xm)$ и $CT=(Y1,Y2,\ldots Yn)$ с помощью функции F^{-1} из (1) нормально вычисляются все Ai, что и является целью дешифрования текста.

Задача дешифрации решается, если злоумышленнику известен открытый текст *ST*, который может быть похищен, подсмотрен или скопирован его соучастником. В этом случае появляется целевая функция и при известных Ai, Yi и F^{-1} путем подбора определяются все Xi, т. е. вскрывается значение секретного ключа.

Система (1) при случайных значениях Ai, Yi и известных и F^{-1} принципиально не решается относительно Xi, поскольку отсутствует целевая функция (осмысленный или известный текст).

Чтобы затруднить подбор ключа используется несколько способов, некоторые из которых приведены ниже.

1. Использование секретных ключей большой длины (m), включающие в себя буквы, цифры и некоторые символы.

При вводе ключа короткой длины производится его искусственное расширение за счет использования уже введенных символов. Например, пусть секретный ключ *CK* состоит из 3-х символов D, E, F (коды 68, 69,70) и его нужно расширить до 8 с использованием функции a·bmod251, где a и b – предпоследняя и последняя цифры текущего ключа. Тогда четвертый код ключа равен 69·70mod251=61, пятый – 70·61mod251=3, шестой – 61·3mod251=183, седьмой – 3·183mod251=47, восьмой – 183·47mod251=67. Коды расширенного ключа D, E, F, =, ETX, I, /, C.

2. Использование одноразовых ключей при каждом сеансе связи.

В этом случае даже наличие у злоумышленника текущего секретного ключа не дает ему возможность читать все последующие сообщения. Для реализации этого способа используется отдельный канал связи для передачи нового значения ключа. Например, А-пользователь по ISDN-сети сообщает очередной ключ шифрования в виде фразы «Давай поговорим сегодня». Эта фраза, точнее кодовое значение символов, и будут использованы в качестве ключа при сеансе связи, но уже через Интернет.

3. Сокрытие источника передачи информации.

Способ предусматривает назначение временного идентификатора источнику (псевдонима) при каждом новом сеансе связи. В сетях связи мобильных абонентов соответствие временного идентификатора TMSI истинному значению IMSI хранится на сетевом сервере. Это позволяет маскировать источник информации, ключ которого возможно скомпрометирован. В IP-сетях следует использовать динамический IP-адрес.

4. Передача провокационных сообщений.

Суть метода состоит в передаче бессмысленных сообщений в случайные промежутки времени. Легальный пользователь после дешифрации просто отбросит это сообщение. То же самое сделает и злоумышленник, отбросив как неверный, даже правильно подобранный ключ.

Список используемых источников

1. Шнайер Брюс. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. М.: Триумф, 2002. 600 с.

УДК 621.391
ГРНТИ 49.33.29

АНАЛИТИЧЕСКАЯ ОЦЕНКА ПОГРЕШНОСТИ ОПРЕДЕЛЕНИЯ МЕСТОПОЛОЖЕНИЯ В WI-FI СЕТИ

Е. В. Кокорева, А. Е. Костюкович

Сибирский государственный университет телекоммуникаций и информатики

Поскольку локальные беспроводные сети Wi-Fi, обеспечивающие мобильный доступ к Интернету, имеются во всех современных организациях и учреждениях, само собой напрашивается применять их для организации систем локального позиционирования. Статья посвящена аналитической оценке ошибки вычисления координат мобильного объекта внутри помещений без учёта многолучевого распространения сигнала, замираний и других помех.

Wi-Fi, геолокация, определение местоположения, точность, погрешность, вычисление координат объекта, латерация.

Широкое распространение в настоящее время приобретают мобильные приложения, основанные на LBS службах. Охранные системы, логистика и обслуживание складов, медицинские приложения, навигация в торговых

центрах, учебных заведениях и учреждениях культуры – это неполный перечень услуг, для предоставления которых необходимо определить местоположение объекта.

В данной статье рассматривается оценка точности позиционирования методом латерации (трилатерации), основанным на измерении параметра относительного времени прибытия TDOA (англ. *Time Difference Of Arrival*), учитывающего время распространения сигнала от антенны передатчика до антенны приемника и обратно [1].

Анализ методики применения этого параметра к определению координат мобильного объекта внутри помещения позволяет оценить потенциальную точность и возможные погрешности методов позиционирования на основе протокола измерения точного времени FTM (англ. *Fine Timing Management*) и, учитывая эти оценки, определить зону радиопокрытия и оптимального размещения точек доступа.

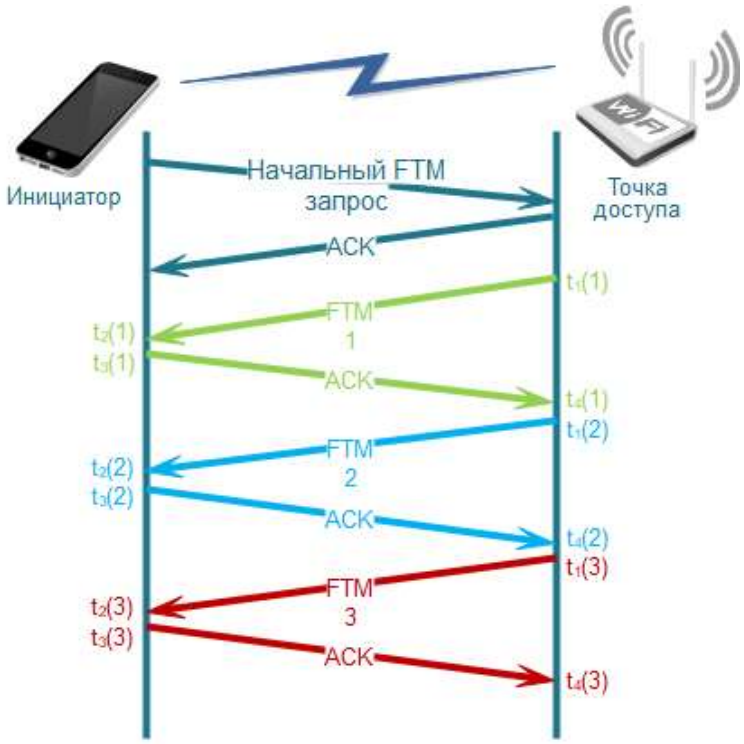


Рис. 1. Передача нескольких FTM запросов для измерения временных меток

Поскольку оценка времени распространения сигнала зависит не только от расстояния между объектами, но в значительной степени и от шума в радиоканале, для получения более точных результатов производят измерения времени отправки и приёма нескольких пакетов (рис. 1) [2, 3]. Обмениваясь запросами FTM и ответами ACK, станция (мобильный абонент) и точка доступа засекают временные метки t_1, t_2, t_3, t_4, по которым будет определяться расстояние между передатчиком и приёмником.

Протокол FTM позволяет оценивать расстояние между антеннами устройств Wi-Fi и обеспечить более высокую точность измерения по сравнению с другими методами. Так как определение расстояния производится путем измерения времени прохождения сигнала между объектом (терминалом) и точкой доступа, а затем простым линейным пересчетом этого времени в расстояние, то можно отметить следующие преимущества FTM:

– время «полета» сигнала линейно зависит от дальности, в отличие, например, от уровня принимаемого сигнала RSSI (англ. *Received Signal Strength Indicator*);

– время переднего фронта сигнала по сравнению с амплитудой сигнала меньше зависит от отношения сигнал/шум, а при достаточной полосе пропускания и от влияния замираний, вызванных многолучевым распространением.

Учитывая сказанное выше, можно ожидать, что точность систем обнаружения местоположения, основанных на измерении времени с разрешением до нескольких наносекунд, также будет меньше зависеть от многолучевости, на линии прямой видимости по сравнению с другими системами [4].

Расстояния от точек доступа определяются по формуле (1).

$$R = c \cdot t_p, \text{ м}, \tag{1}$$

где c – скорость света; t_p – задержка распространения, измеренная по времени отправки и приёма сигнала.

Среднеквадратическая ошибка времени распространения сигнала в зависимости от значения SNR (отношения Сигнал/Шум) в беспроводном канале определяется по формуле (2).

$$\sigma_t = \frac{T_r}{\sqrt{2 \cdot SNR}}, \tag{2}$$

где $T_r = 1/B_{bp}$ – время нарастания фронта импульса; B_{bp} – ширина полосы канала [2].

Для анализа были взяты значения ширины полосы, наиболее часто используемые при настройке Wi-Fi сети: для диапазона 2,4 ГГц – 20 МГц; для диапазона 5 ГГц – 40 МГц.

Результаты аналитического моделирования систем определения местоположения приведены на рис. 2 и 3.

Рисунки иллюстрируют сравнительную характеристику значений погрешности измерений, полученных двумя методами: с измерением задержки распространения (FTM) и с измерением уровня сигнала на входе приёмного устройства (RSSI) в зависимости от расстояния между передающей и приёмной антеннами.

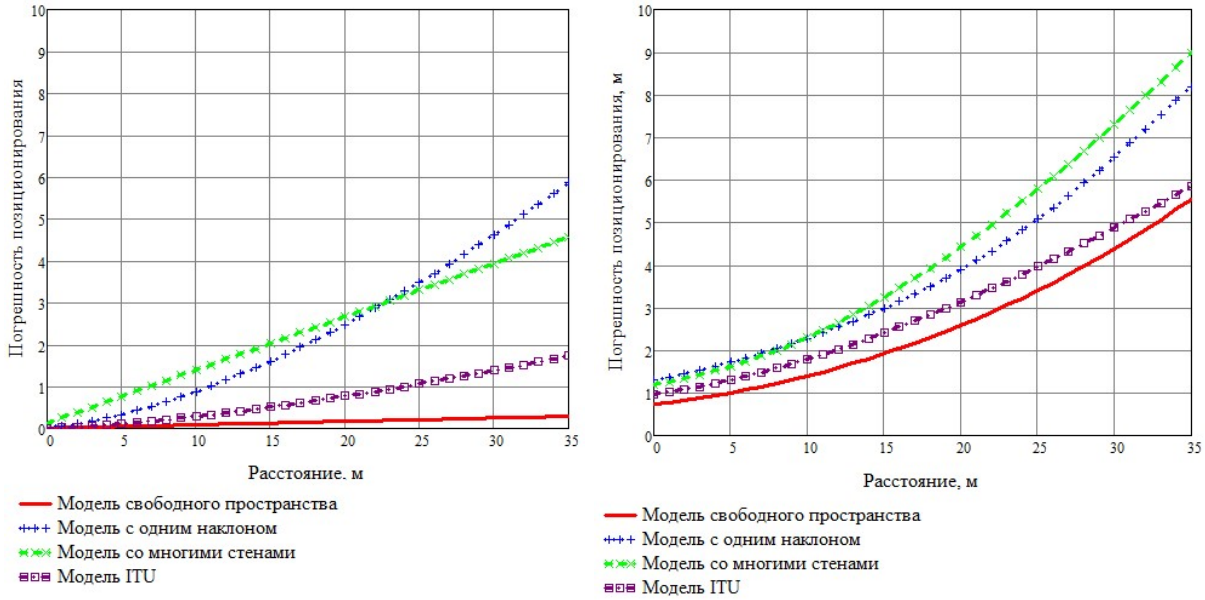
На рис. 2–3(а) изображены значения ошибки определения местоположения методом FTM при вычислении расстояний между приёмником и передатчиком различными моделями определения потерь мощности сигнала на трассе распространения радиоволн [5, 6].

При этом значение SNR определяется выражением:

$$SNR = P_T - L(d) - Noise \qquad (3)$$

где P_T – мощность на выходе передающей антенны, дБм; $L(d)$ – потери мощности на трассе распространения сигнала, дБ; *Noise* – среднее значение мощности шума в канале, дБм.

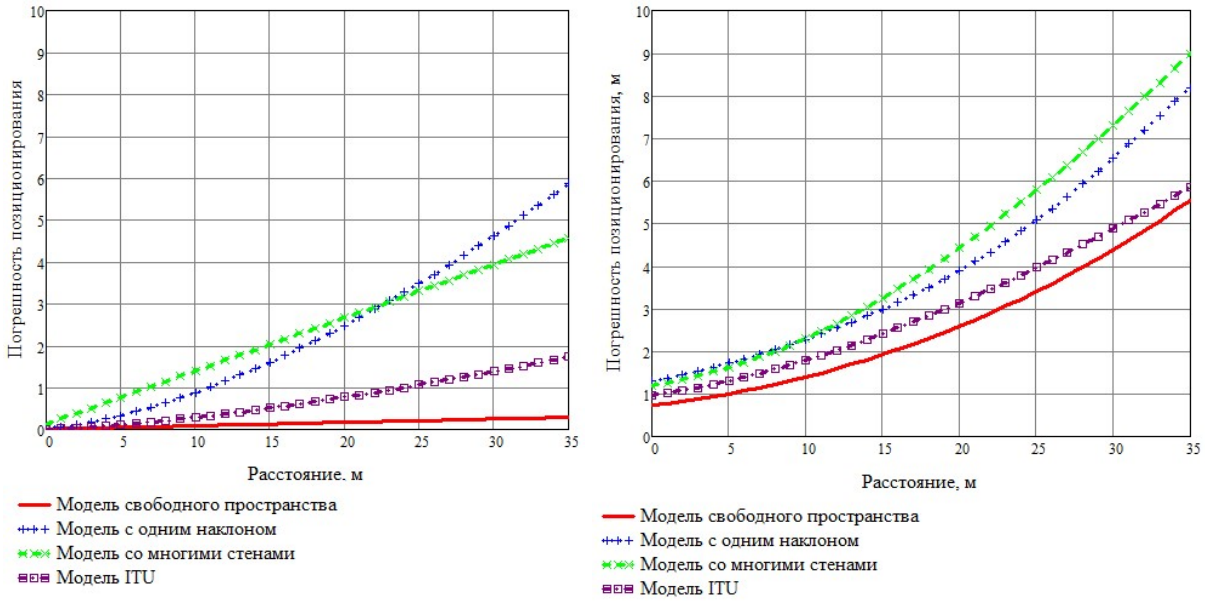
Для сравнения на рис. 2–3(б) приведены аналогичные зависимости, только для погрешностей определения местоположения методом измерения RSSI.



а) б)

Рис. 2. Сравнительная характеристика ошибки позиционирования, полученной с помощью различных моделей PPB, при передаче сигнала на частоте 2,4 ГГц: а) методом FTM; б) методом RSSI

Из рис. 2–3 также становится понятно, что погрешность определения местоположения в системе, основанной на измерении времени, в идеальных условиях меньше, чем погрешность в системе, основанной на измерении мощности сигнала. При этом увеличение расстояния от точки доступа до объекта относительно слабо сказывается на точности измерений в системе FTM.



а) б)

Рис. 3. Сравнительная характеристика ошибки позиционирования, полученной с помощью различных моделей PPB, при передаче сигнала на частоте 5,0 ГГц: а) методом FTM; б) методом RSSI

Конечно, для получения более точной оценки необходимо учитывать не только шум в канале, но и замирания, обусловленные конфигурацией помещения, многолучевым распространением сигнала, а также потери мощности при прохождении через перегородки и перекрытия, которые влияют как на уровень RSSI, так и на время задержки передачи пакетов. Но и грубая оценка погрешности измерений, приведенная в данной статье, может повлиять на выбор методики определения местоположения с приемлемым качеством.

Список используемых источников

1. Pradhan S., Bae Y., Pyun J. Y., Ko N. Y., Hwang S. Hybrid TOA trilateration algorithm based on line intersection and comparison approach of intersection distances // Energies. 2019. Vol. 12 (9). URL : https://www.mdpi.com/journal/energies/special_issues/wireless_communication (дата обращения: 23.01.2022).

2. Bensky A. Wireless Positioning Technologies and Applications. 2nd Ed. Boston. London : Artech House. 2016. 450 p.

3. Comparison of 2.4 GHz WiFi FTM- and RSSI-Based Indoor Positioning Methods in Realistic Scenarios // Bullmann M., Fetzer T., Ebner F., Ebner M., Deinzer F., Grzegorzek M. Sensors. 2020. V. 20 (16).

4. Banin L., Schatzberg U., Amizur Yu. WiFi FTM and Map Information Fusion for Accurate Positioning // International Conference on Indoor Positioning and Indoor Navigation (IPIN). Alcalá de Henares, 2016.

5. Дощинский И. В. Оптимизация методов определения местоположения объектов внутри помещений в сети Wi-Fi // Материалы Российской научно-технической конференции «Обработка информации и математическое моделирование». Новосибирск: СибГУТИ, 2020. С. 5–9.

6. Кокорева Е. В., Костюкович А. Е. Результаты натурных испытаний системы определения местоположения в сети Wi-Fi // Экономика и качество систем связи. Москва. 2021. № 3 (21). С. 64–71.

УДК 621.391
ГРНТИ 49.33.29

ПОВЫШЕНИЕ ТОЧНОСТИ ЛОКАЛЬНОГО ПОЗИЦИОНИРОВАНИЯ ОПТИМИЗАЦИЕЙ РАЗМЕЩЕНИЯ ТОЧЕК ДОСТУПА

Е. В. Кокорева, К. И. Шурыгина

Сибирский государственный университет телекоммуникаций и информатики

Применение сетей Wi-Fi для построения системы определения местоположения объектов внутри помещений представляет собой наиболее простой и экономически выгодный способ. Позиционирование в такой системе осуществляется на основе измерения уровня мощности принимаемого сигнала RSSI с применением метода латерации (трилатерации) для вычисления координат цели. Статья посвящена повышению точности определения координат путем коррекции сетевой структуры в соответствии с частотно-территориальным планированием.

территориально-частотное планирование, точность, погрешность, Wi-Fi сеть, точка доступа, позиционирование.

Определение координат мобильного объекта на основе измерения параметра RSSI требует учёта электромагнитной обстановки в помещении и выполнения определённых требований к построению сети, которая служит инструментом позиционирования. Анализ результатов применения метода латерации (трилатерации) к определению местоположения абонента в эталонных точках (с известными координатами) показал, что для достижения требуемой точности необходимо тщательное территориально-частотное планирование при расстановке точек доступа [1, 2].

Опытным и аналитическим путём было установлено, что для того, чтобы значение погрешности измерений по RSSI попадало в диапазон 5-7 м, расстояние между приёмными и передающими антеннами (между точкой доступа и мобильным объектом) не должно превышать 15 м и, соответственно, уровень мощности сигнала, поступающего от каждой из точек доступа на вход приёмного устройства, должен иметь значение не ниже -65 дБм [3].

Сеть Wi-Fi, в которой были произведены эксперименты, разрабатывалась с целью обеспечения персонала беспроводным доступом к сети Интернет со скоростью не менее 1 Мбит/с, и из этих же соображений производилась расстановка точек доступа в помещениях тестовой зоны.

Для отображения карт радиопокрытия помещений, представленных на рис. 1–2, применялось программное обеспечение D-link Wi-Fi Planner, представляющее собой планировщик беспроводных сетей с возможностью гибко конструировать помещения различной сложности и радиопроницаемости [4].

Рис. 1 отображает электромагнитную обстановку в сети Wi-Fi в виде тепловой карты, существовавшей до начала реализации данного проекта.

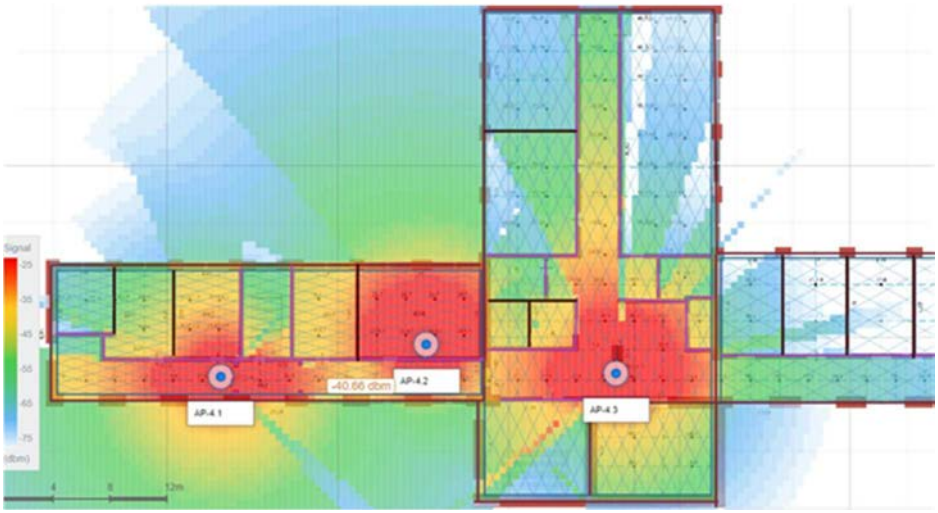


Рис. 1. Покрытие сети в экспериментальной зоне
до территориально-частотного планирования

Выше было отмечено, что изначальное положение точек доступа, приемлемое для обеспечения доступа к Интернету, не отвечало требованиям, заданным системой определения местоположения при определении координат объекта на основе измерения параметра RSSI. На рисунке можно видеть большое количество помещений с низким уровнем мощности или вообще недоступных для радиосигнала, поступающего от точек доступа экспериментальной сети.

На рис. 2 приведена тепловая карта после оптимизации размещения точек доступа, выполненной в результате частотно-территориального планирования с целью обеспечения улучшения определения местоположения.

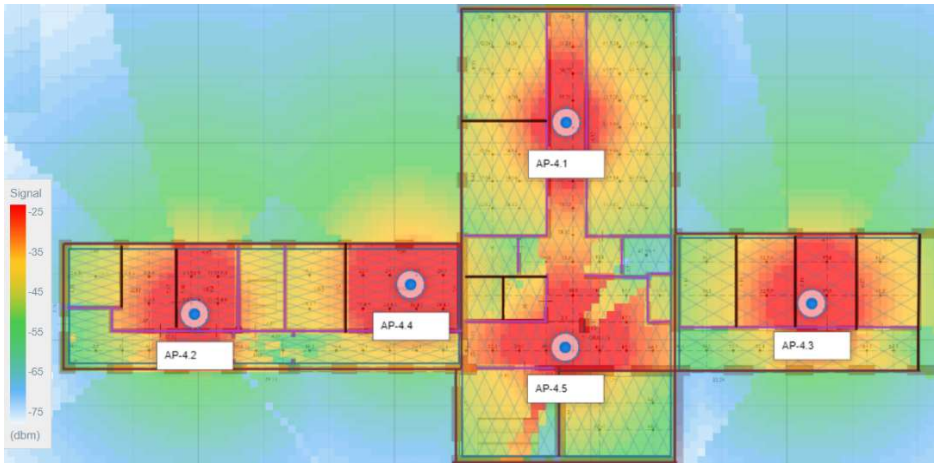


Рис. 2. Покрытие сети в экспериментальной зоне
после территориально-частотного планирования

Результаты вычисления координат мобильного объекта в эталонных точках, полученные до и после корректировки размещения точек доступа в помещениях экспериментальной зоны, приведены на рис. 3–5. Рисунки демонстрируют погрешности определения местоположения, создаваемые разными моделями распространения радиоволн при применении метода латерации [5, 6].

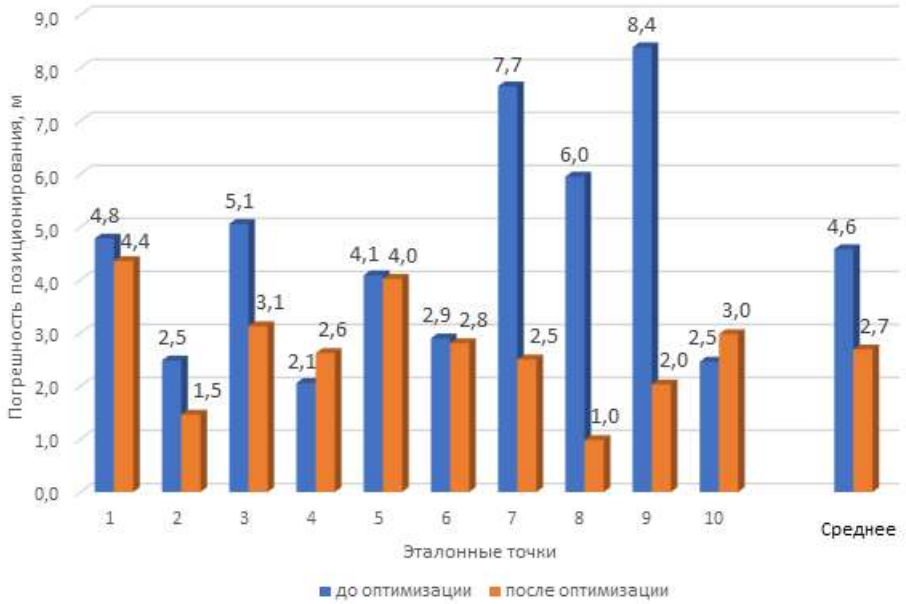


Рис. 3. Сравнительная характеристика погрешности определения местоположения в эталонных точках до и после корректировки размещения точек доступа:
модель с одним наклоном

Рис. 3 показывает значительное улучшение характеристик метода латерации для модели с одним наклоном в большинстве точек при правильном размещении АР. Средняя погрешность вычислений до планирования составляла 4,58 м, после планирования – 2,69 м.

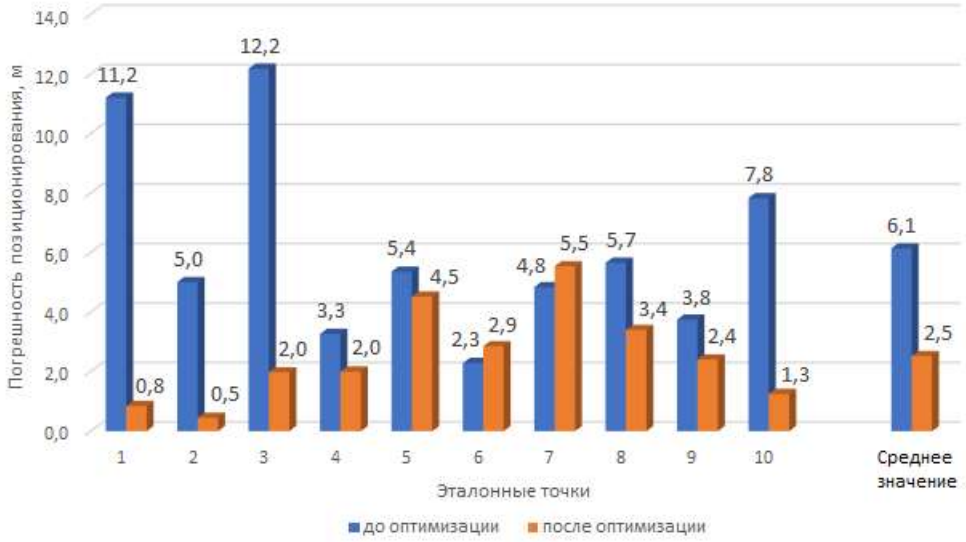


Рис. 4. Сравнительная характеристика погрешности определения местоположения в эталонных точках до и после корректировки размещения точек доступа: модель со многими стенами

Рис. 4, как и предыдущий, показывает значительное улучшение характеристик метода латерации для модели со многими стенами в большинстве точек при правильном размещении АР. Средняя погрешность вычислений, которая до планирования составляла 6,14 м, после планирования – 2,53 м.

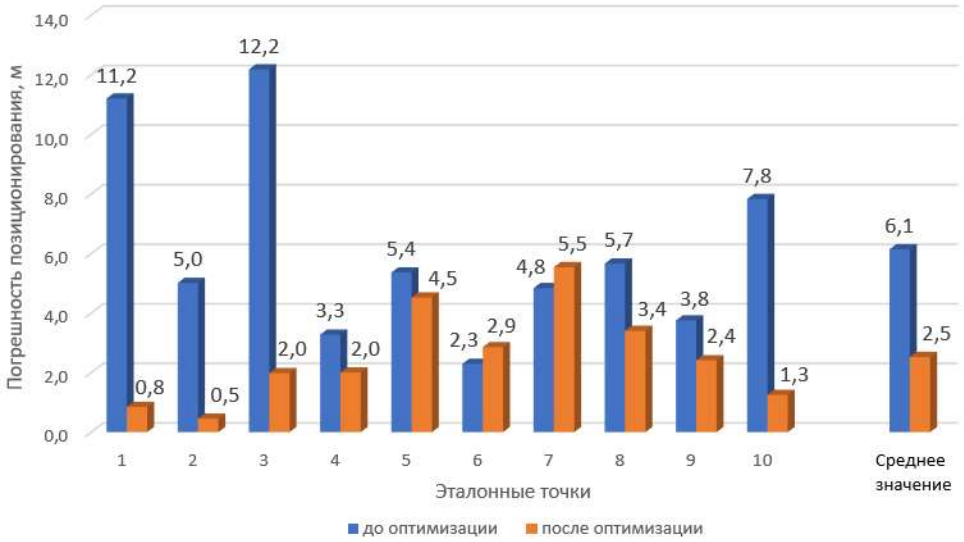


Рис. 5. Сравнительная характеристика погрешности определения местоположения в эталонных точках до и после корректировки размещения точек доступа: модель, рекомендованная МСЭ

Для модели, рекомендованной Международным Союзом Электросвязи изменения погрешности вычислений не так заметны (рис. 5), но все-таки их значения ниже, чем до оптимизации. Средняя погрешность вычислений до планирования составляла 3,52 м, а после планирования – 2,56 м.

Таким образом, оптимизация размещения точек доступа в сети Wi-Fi привела к повышению точности определения местоположения при измерении параметра уровня сигнала на входе приёмного устройства RSSI от средних значений погрешности вычислений 4 м до средних значений 2,5 м. Полученные результаты подтверждают предположение о том, что правильное размещение точек доступа в сети Wi-Fi приводит к улучшению радиопокрытия помещений до уровня RSSI не менее -65 дБм в любой точке, что позволяет обеспечить необходимую точность позиционирования.

Список используемых источников

1. Отчет о НИР № 084-00003-19-00 от 27.12.2018 (Федеральное агентство связи). Исследование и разработка системы определения местоположения в централизованной Wi-Fi сети / Костюкович А. Е., Кокорева Е. В., Якушев И. Ю., Зубкова Н. О., Дощинский И. В. Новосибирск : СибГУТИ, 2019. 109 с.

2. Kokoreva E., Kostyukovich A., Shurygina K., Doshchinsky I. Experimental Study of the Positioning System in the Centralized Wi-Fi Network // Advances in Artificial Systems for Medicine and Education V. AIMEE 2021. Lecture Notes on Data Engineering and Communications Technologies. vol 107. Springer, 2022. pp. 346–357.

3. Кокорева Е.В., Костюкович А.Е. Результаты натурных испытаний системы определения местоположения в сети Wi-Fi // Экономика и качество систем связи. Москва. 2021. № 3 (21). С. 64-71.

4. D-link Wi-Fi Planner Pro. Планировщик беспроводных сетей. URL: https://www.dlink.ru/tools/wi-fi/ (дата обращения: 15.03.2022).

5. Indoor Propagation Models // COST Action 231 : Digital mobile radio towards future generation systems: Final report. 1999. pp. 175–189.

6. ITU-R P.1238-8 Propagation data and prediction methods for the planning of indoor radio communication systems and the radio local area networks in the frequency range 900 MHz to 100 GHz. Geneva: ITU-R Recommendations, 2015.

УДК 004.056
ГРНТИ 81.93.29

АНАЛИЗ ИНФОРМАТИВНОСТИ ПРИЗНАКОВ ВРЕДОНОСНЫХ БОТОВ В СОЦИАЛЬНЫХ СЕТЯХ

М. В. Коломеец

Санкт-Петербургский федеральный исследовательский центр Российской академии наук

Вредоносные боты в социальных сетях представляют собой серьезную угрозу, так как они используются злоумышленниками для накрутки репутации, шантажа, мошенничества, распространения дезинформации и прочих вредоносных действий. При этом становится крайне актуальной задача обнаружения ботов, как экспертными методами, так и методами машинного обучения. Для этого, специалистам необходимо понимать, какие источники данных могут содержать в себе отличительные признаки ботов, чтобы на их основе формировать эффективные методы принятия решения. В данном докладе представлен статистический анализ информативности признаков ботов социальной сети ВКонтакте по типам данных, генерируемых аккаунтом: профилю, текстовой информации, медиа информации, распределениям, временным распределениям и смежным аккаунтам. Результаты данного анализа могут быть использованы для создания новых более точных методов детектирования, основанных как на экспертном анализе, так и на анализе методами машинного обучения.

информационная безопасность, социальные сети, обнаружение ботов, статистический анализ, информативность признаков.

Аккаунты социальных сетей содержат большое разнообразие данных, на основе которых может производиться экспертная оценка либо обучение классификаторов в задаче обнаружения ботов [1]. Источники данных [2] в социальной сети можно разделить на следующие категории:

1) Профиль – поля анкеты пользователя, которые представлены категориями, числами и текстом;

2) Текстовую информацию – генерируемый пользователем текстовый контент;

3) Медиа информацию – генерируемый пользователем медиа контент;

4) Распределения – параметры генерируемого пользователем контента;

5) Временные распределения - временные параметры генерируемого пользователем контента;

6) Смежные аккаунты – параметры аккаунтов, с которыми пользователь осуществлял социальное взаимодействие;

7) Графы – структуры графов взаимодействий пользователей на основе смежных аккаунтов.

Для анализа информативности источников данных были собраны 100 тысяч аккаунтов случайных пользователей и 18 тысяч аккаунтов ботов из социальной сети ВКонтакте. Для каждого источника данных были применены методы генерации признаков по следующей схеме:

1) Профиль – one hot encoding для категориальных данных, методы естественной обработки языка [3] для текстовых данных;
2) Текстовая информация – методы естественной обработки языка [3];
3) Медиа информация – анализ использования изображений по умолчанию;
4) Распределения – статистические методы [2];
5) Временные распределения – статистические методы анализа временных рядов [2];
6) Смежные аккаунты – анализ графов смежных аккаунтов [4];
7) Графы – графовые алгоритмы [4].

Всего было сгенерировано 260.000 признаков. Из всех аккаунтов были выбраны 4 000 случайных равномерно распределённых аккаунтов (2 000 ботов и 2 000 пользователей), с количеством ненулевых признаков >10 % (мера наполняемости аккаунта, для того чтобы исключить незаполненные и заблокированные). На их основе была рассчитана информативность [5] как:

1) Корреляция Пирсона между векторами признака и лейблов;
2) Корреляция Спирмена между векторами признака и лейблов.

Распределение информативности признаков представлено на рис. 1 и 2 в виде ящиков с усами.

Анализ информативности признаков показал, что наиболее эффективным с точки зрения обнаружения ботов является использование признаков на основе смежных аккаунтов и построенных на их основе графов.

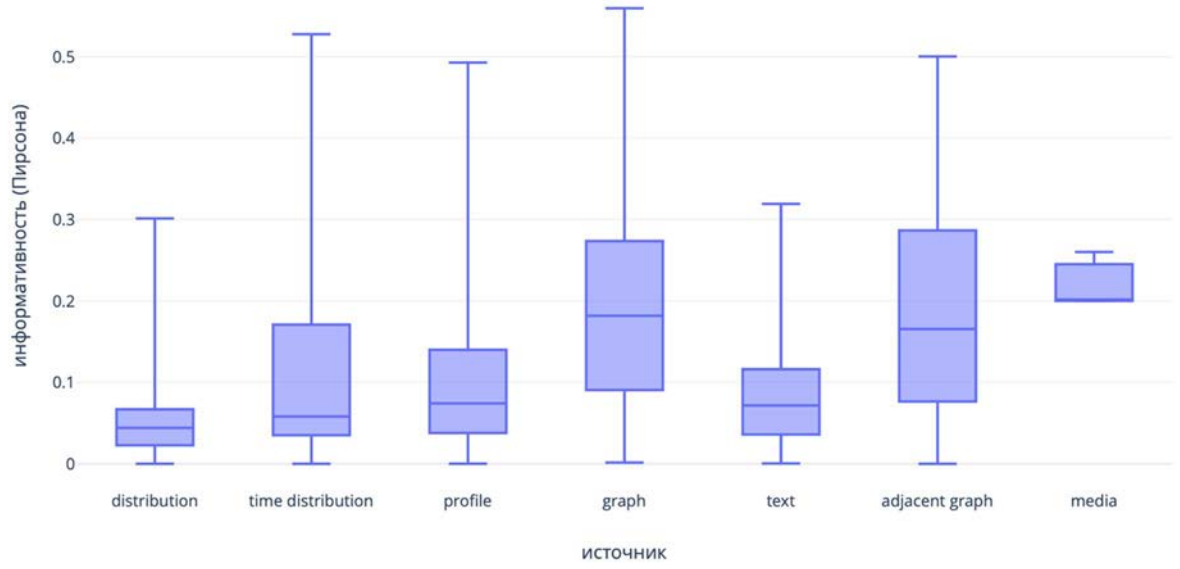


Рис. 1. Информативность признаков ботов (корреляция Пирсона)

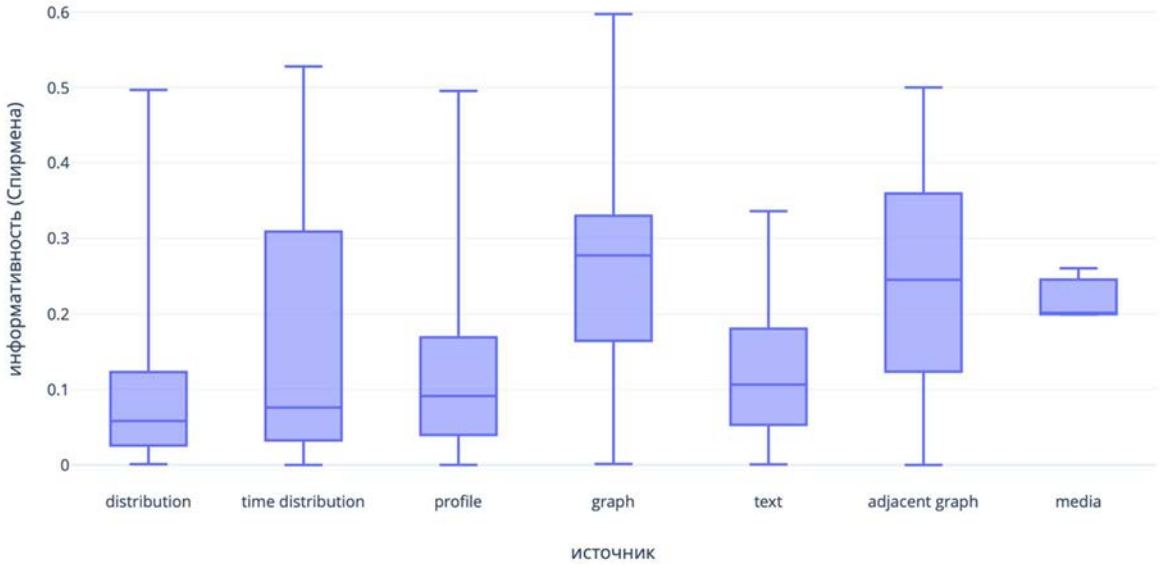


Рис. 2. Информативность признаков ботов (корреляция Спирмена)

Необходимо отметить, что использованные в данной работе методы оценки информативности отображают лишь линейную зависимость признака от лейбла. При использовании сложных моделей машинного обучения (глубокие нейронные сети и т. п.), способных находить множественные взаимосвязи между признаками, можно использовать в том числе признаки с низким значением линейной информативности.

Представленные данные могут использоваться как в задачах построения эффективных автоматизированных систем поиска ботов используя простые модели, а также при экспертной оценке.

Работа выполнена при финансовой поддержке РНФ (проект № 18-71-10094-П).

Список используемых источников

1. Karatas A., Iahin S. A review on social bot detection techniques and research directions. // In Proc. Int. Security and Cryptology Conference Turkey. October 2017. pp. 156–161.

2. Коломеец М. В. Анализ статистических признаков профилей в социальных сетях для обнаружения ботов // Актуальные проблемы инфотелекоммуникаций в науке и образовании. X Юбилейная международная научно-техническая и научно-методическая конференция: сб. науч. ст. СПб.: СПбГУТ, 2021. Т. 1. С. 509–512.

3. Dickerson J. P., Kagan V., Subrahmanian V. Using sentiment to detect bots on twitter: Are humans more opinionated than bots? // In Proc. of the 2014 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM'14), Beijing, China. IEEE, August 2014. pp. 620–627.

4. Maxim Kolomeets, Andrey Chechulin, Igor Kotenko. Bot detection by friends graph in social networks // Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA). 2, 12. 2021. pp. 141–159.

5. Biesiada J., Duch W. Feature selection for high-dimensional data—a Pearson redundancy based filter // Computer recognition systems 2. Springer, Berlin, Heidelberg, 2007. pp. 242–249.

УДК 004.056
ГРНТИ 81.93.29

ВИЗУАЛЬНАЯ МОДЕЛЬ ГРАФА АТАК КОМПЬЮТЕРНОЙ СЕТИ

М. В. Коломеец, А. А. Чечулин

Санкт-Петербургский федеральный исследовательский центр Российской академии наук

При анализе безопасности компьютерных сетей зачастую применяются автоматизированные подходы, в которых часть решений принимаются не в автоматическом режиме, а оператором. Так, при анализе графов атак компьютерной сети, оператор системы может принимать решения по определению важности хостов сети, стратегиям защиты, моделированию инцидентов и т.д. В такой ситуации возникает необходимость предоставлению оператору удобных инструментов ручной и полуавтоматической аналитики, в том числе с использованием визуальных моделей. В данной работе представлена визуальная модель графа атак, которую может использовать оператор для мониторинга состояния компьютерной сети и соответствующего принятия решений. Работа также содержит примеры графической реализации данной модели на основе данных о реальной компьютерной сети и имеющихся в ней уязвимостях.

анализ рисков, сетевая безопасность, графы атак, визуальная аналитика.

В настоящее время, в системах анализа и мониторинга компьютерных сетей все чаще применяется визуальная аналитика, как универсальный инструмент, позволяющий оператору оперативно оценить ситуацию и выбрать наиболее подходящее контрмеры. При этом, с ростом самих сетей, анализ которых необходимо производить, а также усложнением методологий анализа рисков, возникает необходимость понятного и оперативного представления сетевых рисков оператору системы.

Большинство SIEM систем [1–3] представляют данные компьютерной сети в виде линейных, столбчатых, круговых и им подобных графиков, описывающих либо метрики сети, либо метрики хоста. При таком подходе оператор не может детально анализировать зависимости между хостами и потенциальные маршруты злоумышленника.

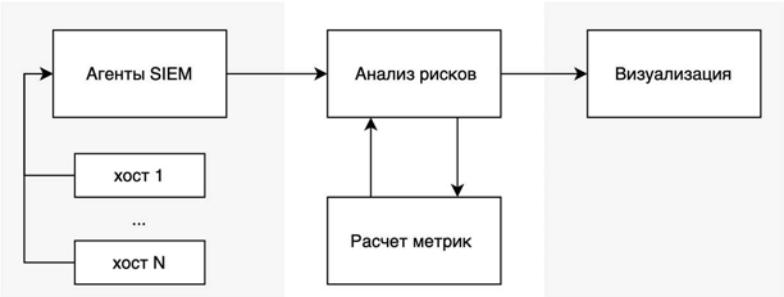


Рис. 1 Архитектура подсистемы визуализации

Для анализа потенциальных маршрутов злоумышленника была разработана модель графа атак, которая визуализирует состояние компьютерной сети на основе метрик отдельных хостов и маршрутов между ними.

Архитектура подсистемы визуализации представлена рис. 1.

На первом этапе информация о топологии сети, уязвимостях хостов и состоянии хостов поступает от агентов сбора SIEM системы (или аналогичной системы сбора информации о хостах сети и их метриках) в модуль анализа рисков. На втором этапе модуль анализа рисков рассчитывает возможные маршруты злоумышленника и метрики рисков хоста. На третьем этапе модуль визуализации отображает данные компьютерной сети в виде графа атак. Пример визуализации графа атак изображен на рис. 2.

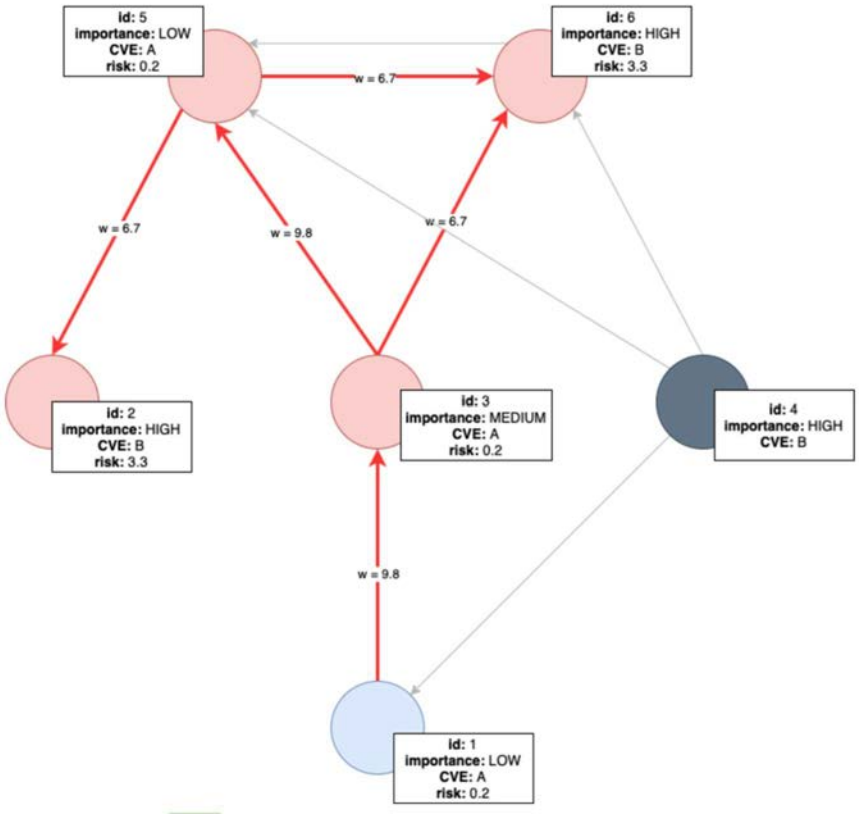


Рис. 2. Визуальная модель графа атак компьютерной сети

Визуальная модель графа атак включает в себя следующие компоненты:

1) Вершина графа представляет собой хост сети.

2) Ребро графа, представляет собой логическое соединение между хостами сети (хосты взаимно обнаруживаемы по сети).

3) Цвет вершины представляет собой тип хоста:

а. Красный – эксплуатируемые хосты, которые досягаемые для злоумышленника.

b. Серый – неэксплуатируемые хосты, которые недосягаемые для злоумышленника.

c. Синий – точки входа злоумышленника.

4) Цвет ребра представляет собой тип ребра:

a. Красный – эксплуатируемые ребра, уведомляют о возможности перехода злоумышленника между хостами.

b. Серый – неэксплуатируемые ребра, уведомляют о невозможности перехода злоумышленника между хостами.

5) Численные метрики хостов и метрики путей представлены в виде текстовых полей поверх вершин и ребер графа.

На основе данной модели графа атак оператор может производить визуальный анализ рисков компьютерной сети на предмет доступности сегментов сети для злоумышленника. Доступность, в зависимости от методологии расчета рисков [4–5], может быть выражена в виде определённой меры риска. Например, для CVSS 3.1 [6] в качестве доступности можно взять метрики Exploitability или Risk.

Работа выполнена при частичной финансовой поддержке бюджетной темы FFSU-2019-0002.

Список используемых источников

1. Kotenko I., Novikova E. Visualization of Security Metrics for Cyber Situation Awareness // Proceedings – 9th International Conference on Availability, Reliability and Security, ARES 2014, 2014. pp. 506–513.

2. Коломеец М. В., Чечулин А. А., Котенко И. В. Обзор методологических примитивов для поэтапного построения модели визуализации данных // Труды СПИИРАН. 2015. № 5 (42). С. 232–257.

3. Коломеец М. В., Котенко И. В., Косов Н. А., Агеев С. А. Иванов А. Ю. Анализ методов человеко-машинного взаимодействия в инструментах визуальной аналитики SIEM-систем // Материалы конференции «Информационные технологии в управлении» (ИТУ-2018). Санкт-Петербург. 2-4 октября 2018. СПб.: АО «Концерн «ЦНИИ «Электроприбор», 2018. С. 559–562.

4. Maxim Kolomeec, Gustavo Gonzalez-Granadillo, Elena Doynikova, Andrey Chechulin, Igor Kotenko, and Herve Debar. Choosing models for security metrics visualization // Computer Network Security. Lecture Notes in Computer Science, Springer-Verlag. The 2017 7th International Conference on Mathematical Methods, Models and Architectures for Computer Networks Security (MMM-ACNS-2017). August 28-30, 2017, Warsaw, Poland Vol. 10446. pp. 75–87. DOI: 10.1007/978-3-319-65127-9_7.

5. Doynikova Elena, Kotenko Igor. An automated graph based approach to risk assessment for computer networks with mobile components // Communications in Computer and Information Science (см. в книгах) // Mobile Internet Security. The 2016 International Symposium on Mobile Internet Security, MobiSec 2016. Taichung, Taiwan, July 14–15, 2016. Vol. 797. pp. 95–106. DOI: 10.1007/978-981-10-7850-7_9.

6. FIRST, Common Vulnerability Scoring System 3.1 (CVSS V3.1) – specification document. URL: https://www.first.org/cvss/v3-1/cvss-v31-specification_r1.pdf (дата доступа: 29.03.2021)

УДК 621.396.93
ГРНТИ 47.49.31

ИНТЕЛЛЕКТУАЛЬНАЯ СИСТЕМА УПРАВЛЕНИЯ ПАРКОВКОЙ ДЛЯ БЕСПИЛОТНЫХ АВТОМОБИЛЕЙ НА ОСНОВЕ ТЕХНОЛОГИЙ ИНТЕРНЕТА ВЕЩЕЙ

И. И. Комаров, Д. А. Лобач, А. С. А. Мутханна

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В данной работе рассматриваются основные технологии позиционирования для беспилотных автомобилей; сопоставляются и анализируются точность позиционирования, преимущества и недостатки, предложена умная система позиционирования для беспилотных автомобилей и, наконец, дается рекомендация по выбору технологии позиционирования в России. Полученные результаты могут быть использованы в рамках практических исследований и разработках позиционирования в области технологии V2X.

Интернет Вещей, Сети 2030, V2X, Искусственный интеллект.

За прошедшее десятилетие, был не только зафиксирован эксабайт данных, передаваемых по сетям, но и, что более важно, появились автономные транспортные средства, что положило начало эре транспортных систем с алгоритмами искусственного интеллекта (ИИ) [1, 2]. Возможность создания интеллектуальных систем появилась благодаря развитию концепции Интернета Вещей. В совокупности это привело к созданию миллиардов новых подключенных конечных точек с различной чувствительностью к различным видам потребностей в ресурсах. Это выявило несколько недостатков в текущей сети технологии, особенно в проводных сетях.

Роль Сети 2030 заключается в том, чтобы определить правильный набор сетевых технологий, необходимых для предоставления требуемых критериев качества для данных сервисов [3]. Если быть точным, то оно предназначено для удовлетворения коммуникационных потребностей нашего общества и направлено, как и сети IMT-2020 к переходу на информационное общество [4]. На 2030 год цель по-прежнему будет заключается в решении вопросов, связанных с новыми возможностями как государственных, так и частных провайдеров сетевых и сервисных услуг и обеспечения не только нового уровня качества, но и поддержки его с помощью алгоритмов Искусственного интеллекта.

Состояние безопасности дорожного движения в мире становится все более серьезной социально-экономической проблемой. Уровень аварийно-

сти на дорогах остается до настоящего момента высоким. Каждый год в дорожных авариях во всем мире гибнет 1,25 млн человек [5]. За счет появления Интернета и современных технологий, возникло решение данной проблемы – создание «умного» автомобиля, который сможет через сеть взаимодействовать как с окружающей средой, так и с другими автомобилями и объектами. Технология системы обмена данными между транспортными средствами, элементами дорожной инфраструктуры и другими участниками движения называется V2X (*Vehicle to Everything Communications*) [6–8] и как следует из ее названия, технология позволяет транспортному средству взаимодействовать со всеми объектами, которые могут повлиять на него и на которые он можем сам повлиять, что дает возможность водителю либо автопилоту в режиме реального времени через различные технологии позиционирования получать и отправлять координаты местоположения, скорость, дорожные условия, сигналы трафика и поведение водителя, такие как экстренное торможение, а также данные о других типах объектов дорожного движения: пешеходы, дроны, велосипедисты и другие. Для достижения информационной полноты о дорожном движении предлагается разрабатывать и использовать цифровую модель дороги. Данная модель будет не только передавать запрашиваемую информацию транспортному средству или иной другой информационной системе, но и накапливать передающуюся информацию от всех объектов дорожного движения, а также информации с камер Умного города, реализующие системы машинного зрения. Цифровая модель дороги и/или ее участка предоставляет также возможности по внедрению алгоритмов Искусственного интеллекта для повышения качества предоставляемой информации для объектов, запрашивающих ее, а также возможности по прогнозированию трафика, его качественных параметров, в том числе системном прогнозировании дорожной обстановки с учетом погодных условий.

Интеллектуальная система парковки
на основе Технологий Интернета вещей

Количество частных автомобилей с каждым годом увеличивается, а подземные парковки в различных публичных местах становятся все более и более популярными. Однако, подземные парковки имеют сложный рельеф и поиск свободных парковочных мест отнимает большое количество времени. Это серьезно сказывается на удобстве пользования и эффективности парковочных мест.

Как правило, наземные стоянки интегрированы с системой глобального позиционирования. Тем не менее, в закрытых помещениях, GPS сигналы не могут быть получены достаточно эффективно, и GPS не может быть использована. Существующие основные технологии внутреннего позиционирования, такие как инфракрасное позиционирование, Bluetooth, Wi-Fi и UWB

имеют свои недостатки как интерференция. В связи с тем, что для создания системы позиционирования в подземных парковках требуется точность в сантиметровом формате, для системы позиционирования транспортного средства будет использоваться технология NB-IoT благодаря низкому потреблению энергии и низкой стоимости.

NB-IoT относится к узкополосной части технологии 5G. Он построен на сотовой сети и потребляет около 180 кГц полосы пропускания. Его можно напрямую развернуть в сетях GSM, UMTS или сети LTE из-за их низкой мощности.

Для реализации системы отслеживания машин необходимы будут следующие компоненты и модули:

– геомагнитный модуль (встроенный модуль связи NB-IoT),

– мобильное приложение, используемое диспетчером парковки.

Геомагнитный детектор парковочного места используется для сбора информации о занятости парковочного места, а платформа управления парковкой автоматически генерирует данные о начислении платы в соответствии со временем стоянки и правилами начисления платы и передает их в приложение. Состояние работы оборудования системы, статус занятости парковочного места, сведения о записи зарядки и другая информация загружаются на платформу управления парковкой, и данные отправляются на экран наружной информации в режиме реального времени, чтобы сообщить владельцу об оставшихся парковочных местах на каждом этаже парковки.

При подъезде машины к парковке, система сама находит место для парковки с помощью информации на экране навигации. Когда транспортное средство подъезжает к шлагбауму, камера, установленная на перекрестке, фиксирует информацию о номерном знаке транспортного средства, въезжающего на парковку, а затем отправляет эту информацию в систему управления парковкой (рис.).

Стоит также отметить возможность имплементирования алгоритмов Искусственного Интеллекта для разращения следующих задач:

- Оптимизация парковочных мест;
- Прогнозирование нагрузки (плотность автомобилей) на парковку, учитывая временные параметры (день, вечер), а также географическое положение парковки;
- Прогнозирование нагрузки на зарядные станции для электро-автомобилей;
- Прогнозирование и формирование рекомендаций по распределению площадей на парковке, учитывая тип и размер автомобиля, водителя (его опыт и предпочтения) и т. д.

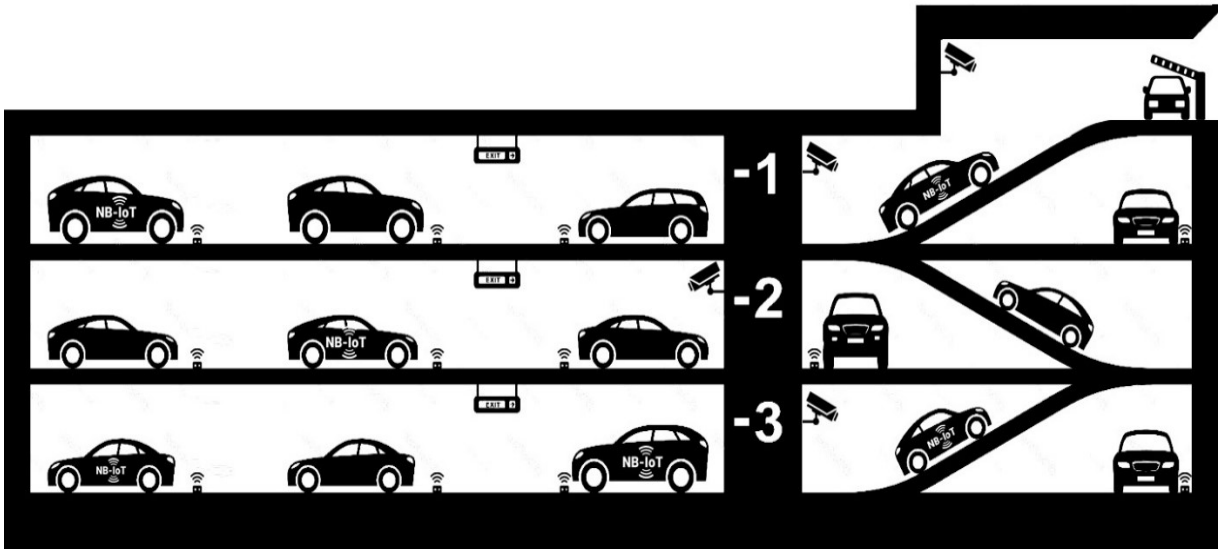


Рисунок. Интеллектуальная система управления парковки на основе Интернета Вещей

Данные алгоритмы могут быть реализованы в виде аналитических модулей к информационной платформе управления парковками для V2X, агрегировать и получать данные более высшего порядка и передавать их в информационную систему Умного города. С целью модульности, независимости и возможности масштабирования, а также простоты развертывания, данные аналитические модули с алгоритмами ИИ могут быть представлены в виде микросервисов распределенного ИИ. Данные микросервисы могут быть масштабированы путем живой миграции при необходимости произведения большего количества аналитических расчетов, например, при росте пользователей, а также являться взаимозаменяемыми.

Выводы

В данной статье представлены концепция, ключевые технологии, применимые сценарии и значения V2X, а также системные решения. Можно заметить, что Подводя итог, можно сказать, что техническое решение V2X для совместной работы автомобиля и дороги может вполне удовлетворить текущие потребности в вспомогательном вождении для обеспечения эффективности движения и повышения безопасности движения, а также может заложить очень хорошую основу для будущей эволюции автономного вождения. Отраслевая практика соответствующих демонстрационных площадок полностью подтвердила большую ценность и потенциал V2X в обеспечении эффективности и повышении безопасности. В то же время существует еще много проблем в области стандартизации технологии V2X.

Исследование выполнено в рамках выполнения ПНИ по государственному заданию СПбГУТ на 2021 год.

Список используемых источников

1. Бородин А. С., Кучерявый А. Е. Сети связи пятого поколения как основа цифровой экономики // Электросвязь. 2017. № 5. С. 45–49.
2. Khayyat M., Elgendy I.A., Muthanna A., Alshahrani A.S., Alharbi S., Koucheryavy A. E. Advanced deep learning-based computational offloading for multilevel vehicular edge-cloud computing networks // IEEE Access. 2020. Т. 8. pp. 137052–137062.
3. Кучерявый А. Е. Сети связи с ультра малыми задержками // Труды НИИР. 2020. № 1. С. 69.
4. Атея А. А., Мутханна А. С., Кучерявый А. Е. Интеллектуальное ядро для сетей связи 5G и тактильного интернета на базе программно-конфигурируемых сетей // Электросвязь. 2019. № 3. С. 34–40.
5. Global status report on road safety: time for action. Geneva, World Health Organization, 2009. URL: www.who.int/violence_injury_prevention/road_safety_status/2009
6. Фокин Г. А., Владыко А. Г. Позиционирование транспортных средств в сверхплотных сетях радиодоступа V2X/5G с использованием расширенного фильтра Калмана // Труды учебных заведений связи. 2020. Т. 6. № 4. С. 45–59. DOI: 10.31854/1813-324X-2020-6-4-45-59
7. Владыко А. Г., Мутханна А. С., Кучерявый А. Е. Метод выгрузки трафика в V2X/5G сетях на основе системы граничных вычислений // Электросвязь. 2020. № 8. С. 24–30.
8. Мутханна А. С. Интеллектуальная распределенная архитектура сети связи для поддержки беспилотных автомобилей // Электросвязь. 2020. № 7. С. 29–34.

УДК 004.056
ГРНТИ 81.93.29

ВЫЯВЛЕНИЕ ПРЕИМУЩЕСТВ И НЕДОСТАТКОВ ПРИМЕНЕНИЯ ТОРГОВЫХ БОТОВ СРЕДИ ОСОБЕННОСТЕЙ ИХ ФУНКЦИОНИРОВАНИЯ

В. А. Коптелова, Н. А. Косов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Настоящая работа посвящена определению необходимости и целесообразности использования торговых ботов в сфере электронной торговли путём определения преимуществ и недостатков таких ботов.

торговые боты, электронная торговля, автомазированная программа, преимущества торговых ботов, недостатки торговых ботов.

В настоящее время существует множество программных решений, которые автоматизируют любую работу, в том числе упрощают процессы в торговой системе. Алгоритмизация торговли представляет собой результат применения специализированных компьютерных систем, работающих по заданному алгоритму – торговых ботов. Всего 12–14 лет назад на российском рынке практически не использовались боты и процесс действий не был автоматизирован [1]. Благодаря торговым ботам появилась возможность отслеживать различные необходимые показатели и применять любую торговую стратегию с разным уровнем сложности на программном уровне.

Чтобы действительно понять потенциал ботов, необходимо понять, что такое боты, а также их сильные и слабые стороны по сравнению с другими способами ведения дел. Анализ преимуществ и недостатков таких ботов позволит определить, целесообразность использования торгового бота при том или ином сценарии или действия могут быть выполнены без использования автоматизированного средства [2]. В соответствии с этим, среди особенностей функционирования торговых ботов предлагается отметить следующие преимущества:

1. Скорость. Торговый бот может проделывать множество операций практически одновременно. При применении современных технологий с наилучшим оборудованием скорость выполнения операций может измеряться в миллисекундах.

2. Точность. Боты в отличии от человека не ошибутся при анализе данных, не перепутают требуемые действия (например, операцию купли и операцию продажи), безошибочно заполнят окна форм.

3. Отсутствие усталости. Автоматизированная программа может работать без перерывов и без выходных. Ни один человек физически не сможет просидеть такое количество времени перед монитором в силу физической усталости. Но важно отметить, что бот будет требовать регулярного контроля и повышения эффективности действий для оптимизации работы.

4. Безэмоциональность. Отсутствие эмоциональной составляющей автоматизированного бота реализовывает заданную стратегию без задержек. Боты будут действовать по заданному алгоритму, за вычетом человеческих эмоции, которые способствуют ошибкам.

5. Помощь в повторяющейся работе. В повседневной работе человек должен выполнять множество повторяющихся действий, таких как отправка писем, проверка определенных документов на наличие ошибок и многое другое. Используя ботов, человек может продуктивно автоматизировать эти рутинные задачи и даже убрать монотонные задачи для людей.

Имея перечисленные преимущества, предлагается выделить следующие недостатки торговых ботов:

1. Финансовые затраты на бота. Покупка или создание торгового бота должна предусматривать финансовые расходы. Существуют готовые программные обеспечения, которые реализованы с помощью простых алгоритмов и стоят относительно недорого. Индивидуально разработанный торговый робот включает в себя создание частного торгового алгоритма заказчика и будет стоить существенно дороже.

2. Возможность компьютерного сбоя. При возникновении программной ошибки торговый бот может продолжить работу неправильно, выполняя некорректные действия. К данному пункту относятся риск разрыва Интернет-соединения, отключение электроэнергии и так далее.

3. Отсутствие вариативности ситуации. Бот изначально ориентирован на выполнение своих действий в определенных условиях. Непредвиденные критерии приведут к «дезориентации» бота, что может повлечь за собой убыточные действия.

4. Безэмоциональность. Является как преимуществом, так и недостатком. Бот, ориентирующийся на заложенный в него алгоритм, может привести к излишним убыткам, которые человек мог бы предотвратить [3].

5. Безработица и лень. Наличие бота может сделать человека более ленивым, поскольку они автоматизируют большую часть работы. Люди, как правило, становятся зависимыми от этих изобретений, которые могут создать проблемы для будущих поколений. Каждая организация стремится заменить людей с минимальной квалификацией роботами, которые могут выполнять аналогичную работу с большей эффективностью.

Выявленные недостатки позволяют сделать вывод, что торговые боты не в состоянии полностью заменить или исключить действия человека, однако они вполне могут применяться в качестве дополнительного инструмента для повышения эффективности процессов.

Список используемых источников

1. Федотова Г. В., Ботнарь С. Ю. Особенности алгоритмической торговли на фондовом рынке // Теория и практика сервиса: экономика, социальная сфера, технологии. 2016. №. 3 (29).

2. Иванов М. А. Использование торговых роботов на рынке Форекс: преимущества и недостатки // European science. 2018. №. 6 (38).

3. Горшков М. А., Сыромятников В. Н. Торговые роботы // Новое слово в науке: перспективы развития. 2016. №. 1-2. С. 227–230.

Статья представлена заведующим кафедрой ЗСС СПбГУТ, кандидатом технических наук, доцентом А. В. Красовым.

УДК 003.26.09
ГРНТИ 81.96

СИСТЕМА ДИСТАНЦИОННОГО ЭЛЕКТРОННОГО ГОЛОСОВАНИЯ В ДИССЕРТАЦИОННОМ СОВЕТЕ ВУЗА

В. И. Коржик, А. Е. Кучерявый, В. А. Яковлев

Санкт-Петербургский государственный университете телекоммуникаций им. проф. М. А. Бонч-Бруевича

Предлагается системы дистанционно электронного голосования в диссертационном совете университета, обеспечивающая выполнение требований ВАК к процедуре голосования по присуждению ученых степеней с сохранением конфиденциальности и анонимности голосов членов диссовета, что является актуальным в период пандемии. Определены состав системы голосования, ее параметры и алгоритм функционирования. В основе криптографического ядра системы голосования предлагается использовать криптографическую систему гомоморфного шифрования Пэйе.

система дистанционного электронного голосования, диссертационный совет, гомоморфное шифрование.

Системы дистанционного электронного взаимодействия между людьми все шире входят в нашу жизнь (предоставление различных информационных услуг, интернет магазины, дистанционное обучение и многое другое. Актуальность такого взаимодействия особенно остро проявилась в условиях пандемии новой короновирусной инфекции, которая продолжается уже два года и перспективы ее спада пока остаются неопределенными. Многие задачи дистанционного взаимодействия удается решать на основе разработанных и проверенных платформ: Zoom, Google meet, Discord и пр. Однако для некоторых видов взаимодействия необходимо выполнение требований информационной безопасности, в частности, обеспечения конфиденциальности и аутентификации передаваемых сообщений. К таким системам, например относятся системы дистанционного электронного голосования (ДЭГ). В сентябре 2021 года система ДЭГ применялась в шести субьектах РФ при проведении парламентских выборов. Основным подходом к обеспечению информационно безопасности в этой и подобной системах голосования является применение криптографических методов защиты информации.

В данном докладе предлагается система дистанционного электронного голосования в диссертационном совете университета, обеспечивающая выполнение требований ВАК к процедуре голосования по присуждению ученых степеней на основе. криптографических методов.

Предполагается, что защита диссертации (доклад соискателя, вопросы по теме диссертации, выступления оппонентов и членов ДС), а также процедурные вопросы (выборы счетной комиссии, утверждение протокола голосования) осуществляется публично в режиме видеоконференции с использованием платформ для видеоконференций Zoom или Google meet.

Предлагаемая система относится только к процедуре голосования членов ДС по присуждению ученой степени соискателю. По требованиям ВАК голосование по присуждению ученых степеней кандидатов и докторов наук должно быть тайным [1]. При ручном голосовании тайна голоса обеспечивается тем, что член ДС имеет возможность заполнения бюллетеня скрытно от кого-либо. Заполненный бюллетень опускается в урну для голосования. после чего счетная комиссия посчитывает число голосов, поданных ЗА (НЕТ) присуждение ученой степени кандидату ученой степени. При этом обеспечивается анонимность голосования, так как после опускания бюллетеня в урну разрывается связь между бюллетенем и лицом его заполнившим. Выполнение этих двух требований: тайны голоса и анонимности голосующего составляют главную проблему всех систем электронного голосования.

В основе системы ДЭГ ДС мы предполагаем использовать криптографическую систему гомоморфного шифрования [2, 3]. Обеспечение тайны голосования и анонимности в такой системе основываются на том, что выполняется следующее условие

$$D_{\hat{K}}(E_K(m_1)\cdot E_K(m_2)\cdot\ldots E_K(m_N)) = m_1 + m_2 + \ldots + m_N, \qquad (1)$$

где $E_K(m_i)$ – зашифрованный голос m_i i-го члена ДС, $D_{\hat{K}}(E)$ – результат дешифрования криптограммы, составленной из произведения криптограмм членов ДС. Суть выражения (1) заключается в том, что результат дешифрования произведения зашифрованных голосов равен сумме этих голосов. За счет шифрования обеспечивается тайна голоса при его передаче по каналам системы ДЭГ, а за счет того, что при расшифровании получается сумма всех голосов сразу, обеспечивается анонимность индивидуальных голосов. Шифрование каждый член ДС осуществляет на едином для всех открытом ключе K, дешифрование осуществляет счетная комиссия на закрытом ключе – $\hat{K}$.

Такая криптосистема в наибольшей степени подходит к решению задачи голосования в ДС, так как голосование является маломасштабным и не требуется много пересылок между участниками процесса голосования.

Предлагаема система (ДЭГ ДС) представлена на рисунке.

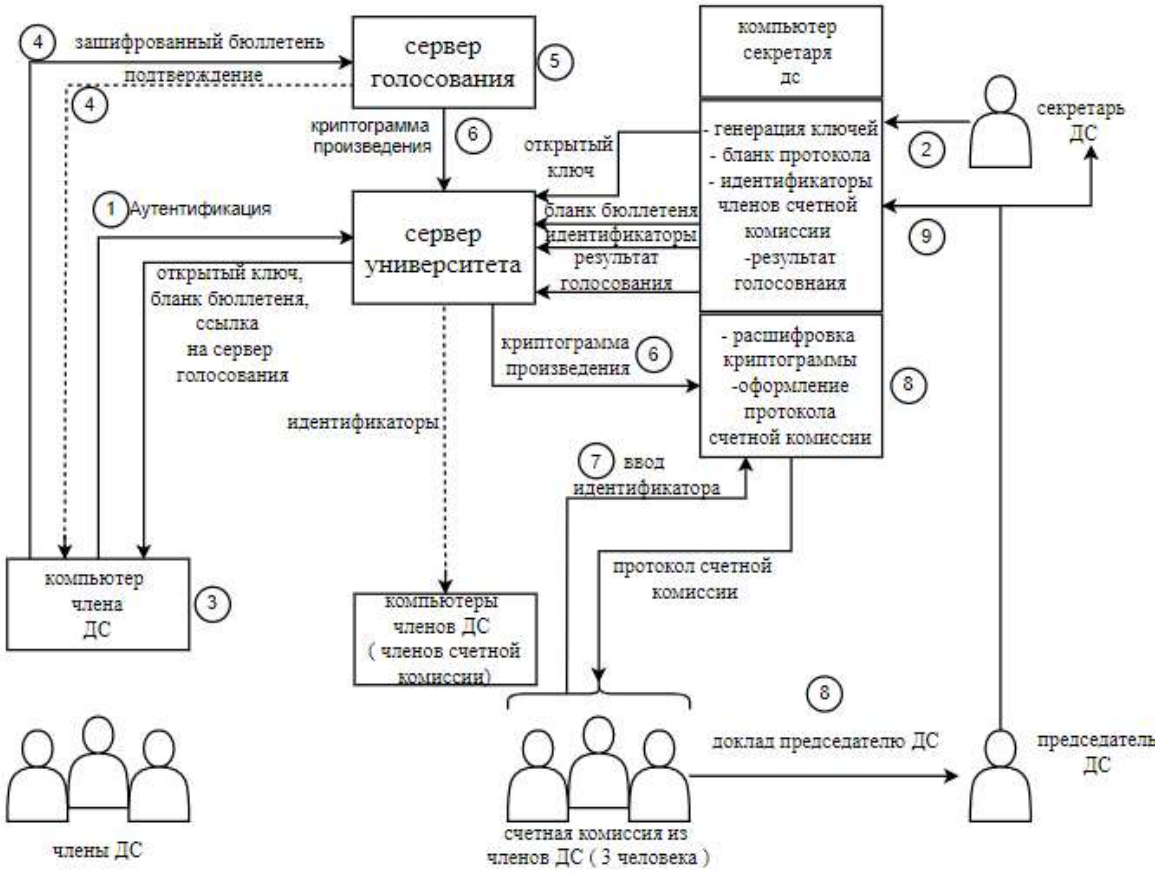


Рисунок. Структурная схема ДЭГ ДС

Мы предлагаем дистанционную схему электронного голосования, которая предполагает, что все члены диссовета голосуют в электронном виде. Председатель, секретарь диссовета и несколько членов диссовета, из которых выбирается счетная комиссия, присутствуют на защите очно, остальные члены диссовета могут участвовать в заседании диссовета дистанционно.
В состав системы голосования входят:

- члены диссертационного совета – физические лица, имеющее право голоса в диссовете. Решение члена диссертационного совета – положительный или отрицательный результат по присуждению ученой степени. (соискатель ученой степени, получает положительный результат, если за присуждение степени проголосовало 2/3 членов диссовета, принявших участие в голосовании). Предполагается, что каждый член ДС имеет компьютер, с помощью которого осуществляется голосование и шифрование бюллетеня. Каждый член ДС имеет доступ к личному кабинету университета и доступ к серверу голосования.
- сервер сбора и преобразования зашифрованных бюллетеней (сервер голосования) – выполняет функцию обработки криптограмм, полученных от членов диссовета и хранения зашифрованных голосов.

• сервер университета выполняет функции аутентификации членов ДС, рассылку открытых ключей и взаимодействие с компьютером секретаря ДС;

• компьютер секретаря ДС. На нем генерируются ключ шифрования бюллетеней, ключ расшифрования и осуществляется расшифрование итоговой криптограммы, полученной от сервера голосования.

• счетная комиссия – осуществляет расшифрование криптограммы, определяет сколько членов ДС приняло участие в голосовании, подсчет голосов поданных ЗА и НЕТ и объявляет результаты голосования.

Функционирование системы осуществляется следующим образом.

1. Вход в систему голосования осуществляется через личный кабинет члена диссертационного совета (необходимо нажать на отдельную вкладку «Диссертационный совет» на главной странице личного кабинета).

Принимающий участие в голосовании член ДС после ввода фамилии и пароля в соответствующие графы, аутентифицируется, и тем самым подтверждает участие в голосовании.

2. Во время входа участников в систему голосования, секретарь диссовета, используя компьютер диссовета, генерирует открытый ключ и закрытый ключи для схемы шифрования по схеме Пэйе. Отправляет открытый ключ членам диссовета. Закрытый ключ хранится на компьютере в защищенной области памяти.

3. Члены диссертационного совета получают открытый ключ, бюллетень, и ссылку на сервер голосования. Члены ДС голосуют и зашифровывают свои бюллетени открытым ключом. Повторное голосование исключено, за счет блокировки доступа сервером при попытке повторного голосования.

4. Проголосовавшие члены диссертационного совета отправляют свои зашифрованные бюллетени на сервер голосования (выделенный ресурс сервера университета или, как вариант, сервер аутсортинга) и получают ответ «ваш голос учтен».

5. Сервер голосования получает зашифрованные криптограммы и выполняет операцию их перемножения, как действительных чисел.

6. Сервер голосования в установленное время отправляет результат перемножения на сервер университета, передающий данные на компьютер секретаря диссовета.

7. Члены счетной комиссии (3 человека), выбранные заранее, получают сообщение от сервера университета в личном кабинете с личными идентификационными номерами для входа на страницу счетной комиссии и получения доступа к закрытому ключу расшифрования. Используя этот ключ, расшифровывают криптограмму-произведение и получают сумму голосов,

поданных ЗА и ПРОТИВ соискателя. После происходит автоматическое заполнение и печать протокола счетной комиссии. Члены счетной комиссии подписывают протокол.

8. Председатель счетной комиссии докладывает о результатах голосования председателю диссовета.

9. Председатель диссовета, через секретаря диссовета доводит результат голосования до всех членов диссовета. Протокол счетной комиссии утверждается открытым голосованием.

10. Секретарь делает запись результата голосования в Журнале диссовета.

В представленной системе голосования выполняются следующие требования:

– легитимность членов ДС обеспечивается аутентификацией члена ДС в личном кабинете.

– тайна голосования обеспечивается за счет шифрования бюллетеня членом ДС.

– анонимность члена ДС обеспечивается специальными свойствами криптографических преобразований;

– оповещение о приеме бюллетеня обеспечивается отправкой сообщения сервером в личный кабинет члену ДС.

– исключение повторного голосования членом ДС обеспечивается путем блокировки доступа к серверу, после приема криптограммы от него.

Предлагаемая система позволит осуществить переход на дистанционную систему голосования в ДС университета и имеет следующие достоинства:

– система проста в своем построении и функционировании, использует ресурс личного кабинета сотрудника ГУТ;

– реализация системы не требует больших вложений средств по созданию дополнительной инфраструктуры и в основном сводится к разработке программного обеспечения ее компонент.

Список используемых источников

1. О порядке присуждения ученых степеней: Постановление Правительства РФ от 24.09.2013 N 842 (ред. от 01.10.2018, с изм. от 26.05.2020).

2. Paillier P. Public key cryptosystems based on composite degree residue classes // In Proc. EUROCRYPT 1999, pp. 223–238.

3. Коржик В. И., Яковлев В. А. Основы криптографии: учебное пособие. СПб.: ИЦ Интермедиа, 2016. 296 с.

УДК 004.056(075.8)
ГРНТИ 81.96

ПРОТОКОЛ РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ ПО ПОСТОЯННЫМ КАНАЛАМ НА ОСНОВЕ СОВМЕСТНОГО ПРИМЕНЕНИЯ ИНТЕРАКТИВНЫХ ПРОТОКОЛОВ ОБМЕНА ДАННЫМИ

В. И. Коржик, В. А. Яковлев

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Исследуется система распределения ключей, включающая три последовательно выполняемых протокола. Первый протокол – числовой протокол распределения бит сырого ключа (ЧПРК) по постоянным бесшумным каналам (типа Интернет), в котором легальные пользователи A и B обмениваются числами $(p+n_A)$ и $(g+n_B)$ соответственно, где p,q – гауссовские случайные величины с параметрами (0,1), а n_A, n_B – гауссовские случайные величины с параметрами (0,σ). Биты «сырого» ключа вычисляется пользователем A, как $K_A = rec[p(g+n_B)]$, пользователем B как $K_B = rec[q(p+n_A)]$, а нарушителем E, контролирующим обмен сообщениями между A и B, как $K_E = rec[(p+n_A)(g+n_B)]$, где $rec[u]$ – операция квантования и на два уровня по знаку. Второй протокол – протокол преимущественного улучшения основного канала легальных пользователей (ПУОК), выполняется путем передачи пользователем A блока, состоящего из s раз повторяющегося случайного числа V = (0,1). Легальный пользователь B принимает блок $V^s \oplus K_B^s$, если все биты в нем одинаковые, в противном случае блок стирается. Нарушитель принимает этот блок и декодирует его по мажоритарному правилу. ПУОК может применяться t раз. Третий протокол – протокол ухудшения двух каналов (УДК) выполняется путем разбиения последовательности бит ключа после выполнения ПУОК на блоки и побитного сложения v блоков. Получены аналитические соотношения, для вычисления вероятности несовпадения бит ключей у легальных пользователей и вероятности несовпадения бит ключа у легального пользователя и нарушителя после выполнения каждого протокола.

криптография, распределение ключей, бесшумные каналы.

Решается задача распределения ключа по бесшумным каналам типа Интернет в присутствии пассивного злоумышленника. Известно, что такая задача в принципе может быть решена, если вероятность ошибки p_m при передаче бита ключа от корреспондента A к корреспонденту B (по основному каналуr) меньше, чем вероятность ошибки p_e в принятом бите нарушителем E (по отводному каналу).

$$p_m \ll p_e. \qquad (1)$$

Эта задача решается на основе комбинированного протокола обмена данными между легальными корреспондентами, включающего три субпротокола. Первый протокол – числовой протокол распределения бит сырого ключа (ЧПРК) по постоянным бесшумным каналам (типа Интернет), в котором легальные пользователи А и В обмениваются числами $(p+n_A)$ и $(g+n_B)$ соответственно, где p,q – гауссовские случайные величины с параметрами (0,1), а n_A, n_B – гауссовские случайные величины с параметрами (0,б). Биты «сырого» ключа вычисляется пользователем А, как $K_A = rec[p(g+n_B)]$, пользователем В как $K_B = rec[q(p+n_A)]$, а нарушителем Е, контролирующим обмен сообщениями между А и В, как $K_E = rec[(p+n_A)(g+n_B)]$, где $rec[u]$ – операция квантования u на два уровня по знаку.

В [1] были получены выражения для вероятности несовпадения бит ключа у корреспондентов А и В $P(K_A \neq K_B) = p_m$ и у нарушителя и корреспондента А $P(K_A \neq K_E) = p_e$ для данного протокола. Значения вероятностей в зависимости от параметра $б^2$ приведены в таблице 1.

Из таблицы следует, что с увеличением $б^2$ вероятность правильного выделения бита ключа уменьшается как у легального пользователя, так и у нарушителя. Причем вероятность правильного приема бита ключа у нарушителя несколько больше чем у легального пользователя, то есть условие (1) не выполняется.

В этой связи мы используем второй протокол – протокол передачи случайного бита с использованием помехоустойчивого кода, который назовем *протоколом преимущественного улучшения основного канала (ПУОК)* [2].

Сначала рассмотрим следующий способ передачи бита ключа от А к В (рис.) А генерирует случайный и равновероятный символ V = 0,1, суммирует его с битом сырого ключа K_A и предает В, который суммирует принятый бит с битом сырого ключа K_B и получает бит U. $U = V \oplus K_A \oplus K_B$. Несложно увидеть, что $V \oplus U = K_A \oplus K_B$. Тогда можно записать выражение для вероятности ошибки в основном канале $P(V \oplus U = 1) = P(K_A \oplus K_B = 1) = P(K_A \neq K_B) = p_m$.

Аналогично можно записать выражение для вероятности ошибки в приеме бита ключа нарушителем в отводном канале (рис.).

$$P(V \oplus W = 1) = P(K_A \oplus K_E = 1) = P(K_A \neq K_E) = p_e .$$

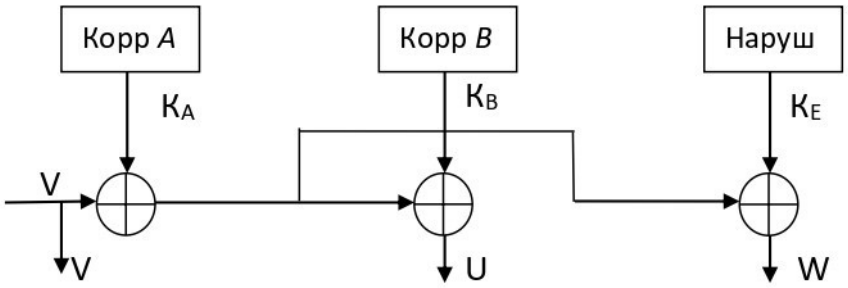


Рисунок. Модель передачи бита ключа

Рассмотрим протокол *преимущественного улучшения основного канала (ПУОК)* [2].

Случайный бит *V*, преобразуется в кодовое слово длиной s бит путем повторения бита *V* s раз. Корреспондент B декодирует принятый двоичный блок следующим образом:

– если все *s* бит в блоке одинаковые (нули или единицы) блок считается принятым;

– если блок содержит и нули и единицы блок стирается, об этом сообщается корр, A по *каналу обсуждения* и он стирает этот бит из буфера памяти.

Нарушитель E контролирует обмен информацией в отводном канале и канале обсуждения и, если корреспонденты стерли блок, он тоже его стирает, если они приняли блок, он его декодирует по мажоритарному правилу. Протокол ПУОК может быть выполнен несколько раз подряд.

После выполнения очередной итерации протокола ПУОК пользователей A, B и нарушителя E формируются новые последовательности, обозначим их как *Vi, Ui* и *Wi* соответственно, где *i* – номер итерации, То есть последовательности на выходе первой итерации являются входными последовательностями для второй итерации и так далее.

Выражение для вероятностей ошибки легального пользователя B после первой итерации

$$p_{mПУОК} = \frac{p_m{}^s}{P_{accept}}, \tag{2}$$

где $P_{accept} = (1-p_m)^s + p_m{}^s$ – вероятность приема кодового блока пользователем B. Для вероятности ошибки декодирования блока нарушителем запишем следующеее выражение (при четном s)

$$p_{eПУОК} = \frac{1}{P_{accept}} \left[\begin{array}{l} \sum\limits_{i:t(\overline{w}_i)>s/2} p(\overline{w}_i, \overline{u} = 0^s) + 1/2 \sum\limits_{i:t(\overline{w}_i)=s/2} p(\overline{w}_i, \overline{u} = 0^s) + \\ + \sum\limits_{i:t(\overline{w}_i)<s/2} p(\overline{w}_i, \overline{u} = 1^s) + 1/2 \sum\limits_{i:t(\overline{w}_i)=s/2} p(\overline{w}_i, \overline{u} = 1^s) \end{array} \right], \tag{3}$$

где $\bar{u}, \bar{w}$ кодовые блоки на входе декодеров у В и Е соответственно, $t(\bar{w}_i)$ – вес Хэмминга блока $\bar{w}_i$. В этом выражении учтена зависимость в приеме блока $\bar{w}$ от того, что принял В: $\bar{u} = 0^s$ или $\bar{u} = 1^s$. Вероятность любой пары блоков находится из соотношения $p(\bar{w}_i, \bar{u}_j) = \prod_{k=0}^{s-1} p(w_{ik}, u_{jk})$ [1].

В таблице 2 приведены вероятности ошибок на выходе декодеров В и Е после выполнения протокола ПУОК при s = 4 для разных значений дисперсии шумов $\sigma_{n_A}^2 = \sigma_{n_B}^2 = \sigma^2$ для двух итераций.

ТАБЛИЦА 1. Вероятности ошибки в основном и отводном каналах для протоколов ЧПРК и ПУОК

σ^2	Протокол ЧПРК		ПУОК 1-я итерация		ПУОК 2-я итерация	
	p_m	p_e	$p_{mПУОК}$	$p_{eПУОК}$	$p_{mПУОК}$	$p_{eПУОК}$
0.1	$1.760 \cdot 10^{-1}$	$9.749 \cdot 10^{-2}$	$2.075 \cdot 10^{-3}$	$1.433 \cdot 10^{-3}$	$1.656 \cdot 10^{-11}$	$4.704 \cdot 10^{-7}$
0.2	$2.319 \cdot 10^{-1}$	$1.339 \cdot 10^{-1}$	$8.237 \cdot 10^{-3}$	$5.713 \cdot 10^{-3}$	$4.604 \cdot 10^{-9}$	$7.773 \cdot 10^{-6}$
0.3	$2.681 \cdot 10^{-1}$	$1.595 \cdot 10^{-1}$	$1.769 \cdot 10^{-2}$	$1.233 \cdot 10^{-2}$	$9.803 \cdot 10^{-8}$	$3.758 \cdot 10^{-5}$
0.4	$2.946 \cdot 10^{-1}$	1.79510^{-1}	$2.951 \cdot 10^{-2}$	$2.064 \cdot 10^{-2}$	$7.581 \cdot 10^{-7}$	$1.105 \cdot 10^{-4}$
0.5	$3.151 \cdot 10^{-1}$	$1.959 \cdot 10^{-1}$	$4.285 \cdot 10^{-2}$	$3.011 \cdot 10^{-2}$	$3.372 \cdot 10^{-6}$	$2.472 \cdot 10^{-4}$
0.6	$3.316 \cdot 10^{-1}$	$2.098 \cdot 10^{-1}$	$5.707 \cdot 10^{-2}$	$4.026 \cdot 10^{-2}$	$1.061 \cdot 10^{-5}$	$4.666 \cdot 10^{-4}$
0.7	$3.452 \cdot 10^{-1}$	$2.218 \cdot 10^{-1}$	$7.167 \cdot 10^{-2}$	$5.076 \cdot 10^{-2}$	$2.639 \cdot 10^{-5}$	$7.846 \cdot 10^{-4}$
0.8	$3.567 \cdot 10^{-1}$	$2.323 \cdot 10^{-1}$	$8.630 \cdot 10^{-2}$	$6.135 \cdot 10^{-2}$	$5.547 \cdot 10^{-5}$	$1.214 \cdot 10^{-3}$
0.9	$3.665 \cdot 10^{-1}$	$2.416 \cdot 10^{-1}$	$1.007 \cdot 10^{-1}$	$7.176 \cdot 10^{-2}$	$1.029 \cdot 10^{-4}$	$1.766 \cdot 10^{-3}$
1	$3.750 \cdot 10^{-1}$	$2.5 \cdot 10^{-1}$	$1.147 \cdot 10^{-1}$	$8.216 \cdot 10^{-2}$	$1.734 \cdot 10^{-4}$	$2.448 \cdot 10^{-3}$

После первой итерации вероятность ошибки в основном канале по-прежнему больше, чем в отводном, но это различие стало меньше (ср. с 1-м столбцом табл. 1). После второй итерации ПУОК в обоих каналах вероятность ошибки значительно уменьшилась и вероятность ошибки в основном канале стала значительно меньше, чем отводном $p_m \ll p_e$. Третья итерация ПУОк в этих условиях не имеет смысла. Преимущество в основном канале над отводным каналом (1) достигнуто. Однако обе вероятности малы, что затрудняет применение процедуры усиления секретности [2]. Поэтому далее применяется третий протокол, протокол преобразования последовательностей бит $\bar{v}, \bar{u}, \bar{w}$, полученных после *i*-й итерации протокола ПУОК, который назовем протоколом ухудшения двух (основного и отводного) каналов (УДК).

Корреспонденты А, В и нарушитель Е формируют новые последовательности, суммируя, соседние четные и нечетные биты исходных последовательностей:

$$\tilde{v}_i = v_{2i} \oplus v_{2i+1},\ \tilde{u}_i = \tilde{u}_{2i} \oplus \tilde{u}_{2i+1},\ \tilde{w}_i = \tilde{w}_{2i} \oplus \tilde{w}_{2i+1},\ i=0,1,2\ldots.$$

Над полученными последовательностями можно еще раз применить протокол ухудшения двух каналов, после этого еще раз и так далее. Обозначим последовательности у A, B и E при v – кратном применении протокола УДК $\tilde{\tilde{v}}^v, \tilde{\tilde{u}}^v, \tilde{\tilde{w}}^v$.

Получены следующие рекуррентные соотношения для вычисления вероятностей ошибок в основном и отводном каналах при v- кратном применении протокола УДК.

$$\tilde{p}^{(v)}_{mУДК} = 2\tilde{p}^{(v-1)}_{mУДК}(1-\tilde{p}^{(v-1)}_{mУДК}),\ \tilde{p}^{(v)}_{eУДК} = 2\tilde{p}^{(v-1)}_{eУДК}(1-\tilde{p}^{(v-1)}_{eУДК}).$$

В таблице 2 показаны значения $\tilde{p}^{(16)}_{mУДК}$ и $\tilde{p}^{(16)}_{eУДК}$ от СКО σ n_A, n_B при 16-и кратном применении протокола УДК.

ТАБЛИЦА 2. Вероятности ошибок в основном и отводном каналах после 16-ти кратного применения протокола УДК

σ	$\tilde{p}^{(16)}_{mУДК}$	$\tilde{p}^{(16)}_{eУДК}$	σ	$\tilde{p}^{(16)}_{mУДК}$	$\tilde{p}^{(16)}_{eУДК}$
0.1	$9.01\cdot10^{-15}$	$2.57\cdot10^{-6}$	0.6	0.026	0.5
0.2	$6.64\cdot10^{-10}$	$7.05\cdot10^{-4}$	0.7	0.184	0.5
0.3	$5.20\cdot10^{-7}$	0.02	0.8	0.465	0.5
0.4	$5.38\cdot10^{-5}$	0.17	0.9	0.5	0.5
0.5	$1.54\cdot10^{-3}$	0.456	1	0.5	0.5

Как видно из таблицы при определенных значениях σ могут быть созданы условия выполнения неравенства (1). Например, при σ = 0.4 имеем $p_m = 5.38\cdot10^{-5}$ и $p_e = 0.456$ ($p_m \ll p_e$.).

Список используемых источников

1. Яковлев В. А, Коржик В. И., Вероятности ошибок при распределении ключей по бесшумным постоянным каналам с использованием добавления искусственного шума // Актуальные проблемы инфотелекоммуникаций в науке и образовании. X Международная научно-техн. и научно-метод. конференция: сб. научн. ст. СПб.: СПбГУТ, 2021. Т. 1. С. 802–807.

2. Maurer U., Secret key agreement by public discussion from common information // IEEE Transactions on Information Theory. 1993. 39:3. pp. 733–742.

УДК 004.056
ГРНТИ 49.33.35

ГРАФОВЫЕ АЛГОРИТМЫ И ПЛАТФОРМЫ УПРАВЛЕНИЯ ГРАФОВЫМИ БАЗАМИ ДАННЫХ ДЛЯ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ

И. В. Котенко, В. В. Пучков

Санкт-Петербургский Федеральный исследовательский центр Российской академии наук

В работе рассматриваются современные платформы управления графовыми базами данных. Определяется возможность использования их как инструмента при анализе графов данных для обеспечения кибербезопасности, в том числе при оценивании защищенности киберфизических систем. Приводятся достоинства и недостатки графовых баз данных по сравнению с традиционными реляционными базами данных. Основное внимание уделяется методикам оценивания защищенности на основе анализа графов атак.

системы управления графовыми базами данных, киберфизические системы, оценивание защищенности, графы атак.

В последние годы использование графов в системах управления базами данных (СУБД) стало активно внедряться в различных сферах. В частности, одним из примеров, где использование графовых СУБД довольно перспективно, является обработка массивов данных для оценивания защищенности при обеспечении кибербезопасности. Это обусловлено тем, что анализируемые данные имеют множественные взаимосвязи, а рассматриваемые системы являются довольно сложными объектами. Поэтому работа с графовыми базами наиболее актуальна, так как математический аппарат этих баз данных был специально создан для работы с отношениями и связями [1–3].

Упрощенно процесс оценивания защищенности на основе графов атак можно представить в виде следующей последовательности действий [4–8]. На первом этапе происходит анализ рассматриваемой (возможно проектируемой) сетевой структуры: определяется состав системы, определяются используемые программные продукты и протоколы связи, т. е. выполняется аудит системы. На втором этапе происходит сбор данных по угрозам и уязвимостям, на основе библиотек и баз данных общеизвестных уязвимостей. На третьем этапе производится обработка данных об обнаруженных угрозах. Итогом этой работы являются входные данные четвертого этапа, на котором происходит построение графа атак. Пятым этапом является анализ графа атак. Конечными результатами являются показатели защищенности, максимально привязанные к рассматриваемой системе.

В таблице 1 приведены наиболее часто употребляемые показатели защищенности, связанные с анализом путей реализации графа атак.

ТАБЛИЦА 1. Показатели защищенности на основе графов атак

Наименование	Описание
Показатель кратчайшего пути	Определяет длину наименьшего пути атаки
Показатель количества путей	Определяет количество путей атаки в пределах данного графа
Показатель средней длины пути	Представляет собой длину пути атаки как среднего арифметического для всех длин путей
Наиболее частая длина пути	Длина пути атаки, встречаемой чаще всего

Именно на заключительном этапе (анализ графа атак и расчет параметров защищенности) предполагается использование графовых баз данных.

В настоящее время в литературе встречаются различные работы, посвященные работе с СУБД и графовым алгоритмам.

Например, в [2] описывается возможность использования графовых баз данных для решения прикладных задач, например, при анализе сложных сетей. В [1, 3] рассматриваются практические вопросы работы с графовыми базами данных на платформе Neo4j и Apache Spark. Основными задачами применения графовых алгоритмов в целях обеспечения кибербезопасности являются: анализ защищенности сети, определение шаблона атаки, определение структуры графа атаки. В [4–8] предлагаются методики анализа защищенности с применением байесовских графов, которые дают возможность учесть влияние текущих событий на рассматриваемую систему и соответственно предположить развитие возможных путей будущих атак. В [9] для анализа защищенности сети используется граф атак с гибридной зависимостью. Уязвимости здесь представляют собой предварительные условия и постусловия. Ребра этого графа отражают взаимосвязь между условиями и уязвимостями. Ребро, идущее от узла состояния к узлу уязвимости, показывает, что это условие является предусловием уязвимости. Ребро, идущее от узла уязвимости к узлу условия, показывает, что узел условия является постусловием уязвимости. Несколько узлов постусловий для уязвимости следует интерпретировать как дизъюнкцию постусловий. Узлы множественных предварительных условий для уязвимости следует интерпретировать как совокупность предварительных условий.

Показатели, указанные в таблице 1 пригодны при анализе защищенности. Однако, авторы в [9] считают, что в случае их изолированного использования, итоговые выводы скорее всего будут иметь большую погрешность. Только комплексный анализ приведенных данных дает возможность получить более достоверные данные.

В [10] предложен подход к оцениванию рисков безопасности на базе графов атак, позволяющий получить количественные показатели безопасности, учитывающие динамические атрибуты, связанные с уязвимостями, которые могут изменяться с течением времени.

В [11] представлен метод использования известных субъектов угроз для обогащения графов атак, что дает возможность аналитикам принимать упреждающие меры и усиливать защиту своих информационных систем.

Выделим преимущества использования графовых баз данных по сравнению с реляционными и NoSQL базами при проведении анализа защищенности.

Скорость обработки запросов. В связи с тем, что запросы при работе базы локализуются в определенной части графа, наблюдается достаточно большой прирост производительности в случае работы с данными, имеющими множественные связи.

Гибкость и вариативность при проектировании. При работе с графовыми СУБД имеется возможность своевременно наращивать при необходимости новые узлы, взаимосвязи и зависимости. Подобная гибкость графовых баз дает возможность моделировать процесс, постепенно добавляя необходимые данные.

Оперативный контроль данных при разработке. Современные графовые базы имеют все необходимое для разработки и дальнейшего обслуживания созданных приложений. Интегрированный язык запросов и встроенный программный интерфейс дает возможность проводить эффективную разработку. В отличие от реляционных баз, где применяются механизмы контроля данных, основанные на схемах, в графовых базах контроль проводится на основе программной модели с помощью запросов и тестов для моделей данных, что позволяет своевременно реагировать на происходящие изменения.

Рассмотрим **основные алгоритмы**, применяемые для анализа данных с помощью графовых СУБД:

– алгоритмы поиска пути – с помощью этих алгоритмов решается наиболее частая задача теории графов по поиску кратчайших путей;

– алгоритмы определения центральности – помогают ответить на вопрос о том, какие узлы наиболее важны в рассматриваемой сети;

– алгоритмы кластеризации вершин – данные алгоритмы позволяют проводить анализ сложных сетей.

В таблице 2 приведена классификация графовых алгоритмов по трем условных группам [1].

Следует отметить, что графовую базу данных следует использовать при проведении анализа данных сложной сетевой структуры. Это, например, логистическая, информационная, киберфизическая модель.

ТАБЛИЦА 2. Классификация графовых алгоритмов

Поиск пути	Определение центральности	Алгоритмы кластеризации
Поиск в ширину (BFS)	Алгоритм PageRank	Алгоритм Гирвана Ньюмана
Поиск в глубину (DFS)	Степень центральности	Модульность Лувена
Кратчайший путь из одного источника (SSSP)	Центральность собственного вектора	Сильно связанные компоненты (SCC)
Все пары кратчайшего пути (APSP)	Близость как центральность	Слабосвязанные компоненты (Union Find)

Рассмотрим особенности некоторых графовых баз данных.

Neo4J. Разработана компанией Neo Technology в 2009 г. Доступна в трех видах: Community, Advanced и Enterprise. Версия Community распространяется по лицензии AGPL v3, для коммерческих же проектов необходимо приобретать версию Advanced. Версия Enterprise также позволяет осуществлять резервное копирование и масштабируема. Для достижения максимальной производительности в Neo4J существует два типа кэширования: файловый (file buffer cache) и объектный (object cache). Первый кэширует данные с жесткого диска. Второй кэш хранит в себе различные объекты графа для увеличения производительности обходов графа. Также в Neo4J поддерживаются алгоритмы обхода графов, что необходимо для решения задачи поиска соседних вершин [3].

Apache Spark. Главной особенностью Spark являются кластерные вычисления в памяти, которые многократно увеличивают скорость обработки приложения. Spark работает в широком диапазоне нагрузок: пакетные приложения, итерационные алгоритмы и др. Помимо поддержки этих задач в соответствующей системе, это снижает нагрузку на управление обслуживанием отдельных инструментов. Скорость - Spark помогает запускать приложения в кластере Hadoop до 100 раз быстрее в памяти и в 10 раз быстрее при работе на диске. Spark хранит промежуточные данные обработки в памяти и поддерживает несколько языков (Java, Scala, Python).

Amazon Neptune. Это полностью управляемый сервис графовой БД, который упрощает создание и запуск приложений, работающих с наборами тесно связанных данных [1]. Он поддерживает популярные свойства графовых моделей и модели W3C и RDF, и соответствующие им языки запросов Apache, TinkerPop, Gremlin и SPARQL. Neptune используется в сервисах рекомендаций, системах выявления мошенничества, графах знаний и сетевой безопасности.

Применение графовых СУБД, на данный момент является привлекательным инструментом для хранения и анализа данных имеющих сложную иерархическую структуру и множественные взаимосвязи. Данные условия полностью соответствуют требованиям, к задачам, которые требуется ре-

шить при работе системы кибербезопасности по оцениванию защищенности. Значительный рост скорости обработки запросов при анализе графов с использованием графовых СУБД позволяет эффективнее реагировать на возможные угрозы при проведении анализа возможных угроз информационной или киберфизической системы.

Работа выполнена при финансовой поддержке Гранта РНФ № 21-71-20078 в СПб ФИЦ РАН.

Список используемых источников

1. Нидхем М., Ходлер Э. Графовые алгоритмы. Практическая реализация на платформах Apache Spark и Neo4j. М.: ДМК Пресс, 2020. 258 с.

2. Гуральник Р. И. Некоторые задачи на графовых базах данных // Труды ИСП РАН. 2016. Т. 28, вып. 4. С. 193–216.

3. Робинсон Я., Вебер Д., Эифрем Э. Графовые базы данных: новые возможности для работы со связанными данными. М.: ДМК Пресс, 2016. 256 с.

4. Дойникова Е. В., Котенко И. В. Совершенствование графов атак для мониторинга кибербезопасности: оперирование неточностями, обработка циклов, отображение инцидентов и автоматический выбор защитных мер // Труды СПИИРАН. 2018. Вып. 2 (57). С. 211–240. DOI: 10.15622/sp.57.9.

5. Kotenko I., Stepashkin M. Network Security Evaluation based on Simulation of Malefactor's Behavior // Proceedings. International Conference on Security and Cryptography, SECRYPT 2006. Polytechnic Institute of Setubal. Setubal, 2006. pp. 339–344.

6. Kotenko I., Stepashkin M., Doynikova E. Security Analysis of Information Systems taking into account Social Engineering Attacks // Proceedings of the 19th Euromicro International Conference on Parallel, Distributed and network-based Processing (PDP 2011). Ayia Napa, Cyprus, 9-11 February 2011. Los Alamitos, California. IEEE Computer Society. 2011. pp. 611–618.

7. Kotenko I., Doynikova E. Security Assessment of Computer Networks based on Attack Graphs and Security Events // Lecture Notes in Computer Science. 2014. Vol. 8407. pp. 462–471.

8. Kotenko I., Chechulin A. Computer Attack Modeling and Security Evaluation based on Attack Graphs // Proceedings of the 2013 IEEE 7th International Conference on Intelligent Data Acquisition and Advanced Computing Systems, IDAACS 2013. 2013. pp. 614–619.

9. Noel S., Jajodia S. Managing Attack Graph Complexity through Visual Hierarchical Aggregation // Proceedings of ACM Workshop Visualization and Data Mining for Computer Security, 2004. pp. 109–118. DOI: 10.1145/1029208.1029225.

10. Tantawy A., Abdelwahed S., Erradi A., Shabanb K. Model-based risk assessment for cyber physical systems security // Computers & Security, Volume 96, September 2020, 101864.

11. Gylling A., Ekstedt M., Afzal Z., Eliasson P. Mapping Cyber Threat Intelligence to Probabilistic Attack Graphs // 2021 IEEE International Conference on Cyber Security and Resilience (CSR) Workshops. 2021.

УДК 004.056
ГРНТИ 49.33.35

МОДЕЛЬ КОМПРОМЕТАЦИИ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

И. В. Котенко, С. С. Хмыров

Санкт-Петербургский Федеральный исследовательский центр Российской академии наук

Объекты критической информационной инфраструктуры (КИИ) находятся под защитой государства, а требования к обеспечению безопасности регламентированы на законодательном уровне. В работе рассмотрены нестандартные методики и векторы атак на объекты КИИ. Характеристика нарушителя подразумевает его высокий потенциал и широкие возможности ведения кибероперациий над инфраструктурой жертвы, а также высокую мотивацию по достижению поставленной цели. Основное содержание статьи составляет предлагаемая модель компрометации объектов КИИ, построенная на основе существующих методик компрометации и векторов атак на объекты КИИ.

целевые атаки, критическая инфраструктура, атрибуция кибернарушителя, кибербезопасность.

Целевые кибератаки (таргетированные, APT) на объекты критической информационной инфраструктуры (КИИ) обладают многомерностью и скрытностью [1]. К объектам КИИ относятся информационные системы (ИС), информационно-телекоммуникационные сети (ИТС), автоматизированные системы управления (АСУ) [2]. Целевые кибератаки сопровождаются компьютерным инцидентом (КИ), т. е. фактом нарушения и (или) прекращения функционирования объекта КИИ, сети электросвязи, используемой для организации взаимодействия таких объектов, и (или) нарушения безопасности обрабатываемой таким объектом информации, в том числе произошедший в результате компьютерной атаки [2]. В большинстве случаев, таргетированные атаки на объекты КИИ выполняются правительственными кибергруппировками или кибернаемниками [3–6].

Кибератаки на критическую информационную инфраструктуру

Для анализа целевых атак на объекты КИИ выборочно взяты следующие наиболее разрушительные кибератаки: атака APT33, атака APT «Энергетический медведь», атака на SolarWinds (APT 29), атака на Colonial Pipeline (APT DarkSide). В отмеченных выше кибератаках применялись раз-

посторонние векторы компрометации целевой системы. С учетом жизненного цикла атаки [7], можно выделить следующий сценарий действий APT: на этапе «Доставки (Delivery)», в большинстве случаев, проникновения за периметр целевой сети осуществлялось с помощью фишинга или специализированного ПО [8-10]. В отдельных случаях, доступ к целевой среде был получен через атаку на цепочки поставок [11]. Действия APT внутри скомпрометированной инфраструктуры имеют схожие тактики, техники (подтехники) и процедуры (ТТП) с целевыми атаками на корпоративный сегмент [12]. После запуска вредоносного кода (инструментария) на подконтрольном узле или системе, обеспечивалось «Постоянство (Persistance)», «Уклонение от защиты (Defense Evasion)», «Командование и контроль (Command & Control)», «Повышение привилегий (Privilege Escalation)», «Доступ к учетным данным» (Credential Access), «Боковое смещение (Lateral Movement)», «Сбор (Collection)», «Эксфильтрация (Exfiltration)», «Причинение ущерба (Impact)» [7,13]. Однако в ряде случаев [14] APT воздействовали непосредственно на системы промышленного управления (АСУ ТП, ICS), применяя характерные для таких систем ТТП. Например, «Подавление функции отклика (Inhibit Response Function)», «Нарушение управления процессами (Impair Process Control)». Схематически процесс компрометации (проявления атаки) представлен на рис. 1.

Модель компрометации объектов КИИ

Как показано на рис. 1, для проникновения в целевую среду злоумышленники оказывают деструктивное воздействие на инфраструктуру жертвы по определенным векторам. Инфраструктура жертвы включает в себя персонал, информационные системы (ИС), сервисы, оборудование, промышленные системы (АСУ ТП, ICS). Также злоумышленники могут скомпрометировать поставщиков услуг (цепочку поставок). Предлагаемая модель компрометации объектов КИИ (модель) предполагает следующие составные элементы:

– Векторы целевой кибератаки. По назначению их можно разделить на «Общие» и «Технологические». «Общие» включают в себя традиционные для кибератак на корпоративную инфраструктуру - фишинг, недостатки конфигурации инфраструктуры, эксплуатацию известных уязвимостей, использование уязвимостей нулевого дня, цепочку поставок. «Технологические» учитывают специфику организации промышленных сетей (автономность), особенности эксплуатации АСУ ТП (например, атака на промышленные беспроводные сети, ПЛК контролеры), имеет узкую направленность [15] в случаях недостатка конфигурации, эксплуатации известных уязвимостей, использование уязвимостей нулевого дня и цепочки поставок [11].

– Инфраструктура. Подразделяется на два типа, включающая (1) персонал, ИС, сервисы, оборудование и (2) промышленные системы. Типы инфраструктуры имеют различные атрибуты (характеристики), которые будут уточняться в будущих исследованиях (работах).

– Этапы компрометации объекта КИИ. Данный элемент в модели, позволяет проводить классификацию в зависимости от типа инфраструктуры, применяемых тактик, техник (подтехник) и процедур.

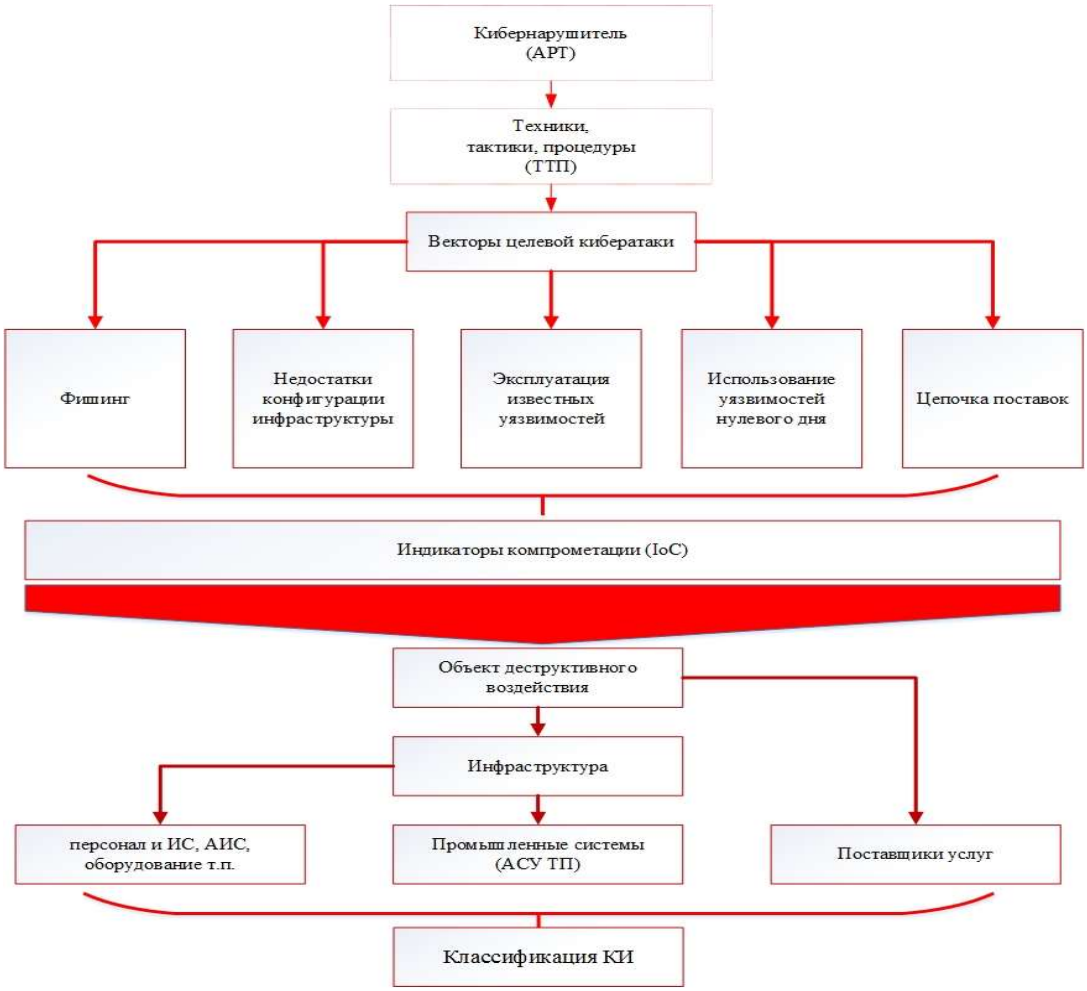


Рис. 1. Схематическое представление процесса проявления атаки

Для инфраструктуры первого типа, включено пять фаз (этапов, шагов) [16]. Этап 3 «Доставка», этап 4 «Заражение», этап 5 «Установка», этап 6 «Получение управления», этап 7 «Выполнение действий». Этапы 1 «Разведка» и 2 «Вооружение» отсутствуют, так как будут включены в другие модели (нарушителя и атрибуции). Инфраструктура второго типа содержит Этап 2 «Разработка и выполнение атаки». Также можно проанализировать перемещение злоумышленников от одного типа инфраструктуры к другому.

– Степень компрометации целевой системы. Продвигаясь по цепочке вредоносных процессов, злоумышленники совершают набор заготовленных

действий. Необходимо выполнить классификацию сценария развития кибератаки, определить степень распространения, площади покрытия и характерный почерк. Агрегируя количественно такие показатели как скорость распространения/заражения, число скомпрометированных объектов (узлов), характер кибератаки, можно формировать поведенческие признаки и т. п.

– Предполагаемый тип кибернарушителя. Имея представление о действиях злоумышленника, можно сравнивать входящие данные и характерные признаки определенных APT. Сигнатуры вредоносных событий (компаний) можно использовать для выявления сходства с вредоносными компаниями известных APT. На данном этапе также устанавливается возможность профилирования кибератакующего [16].

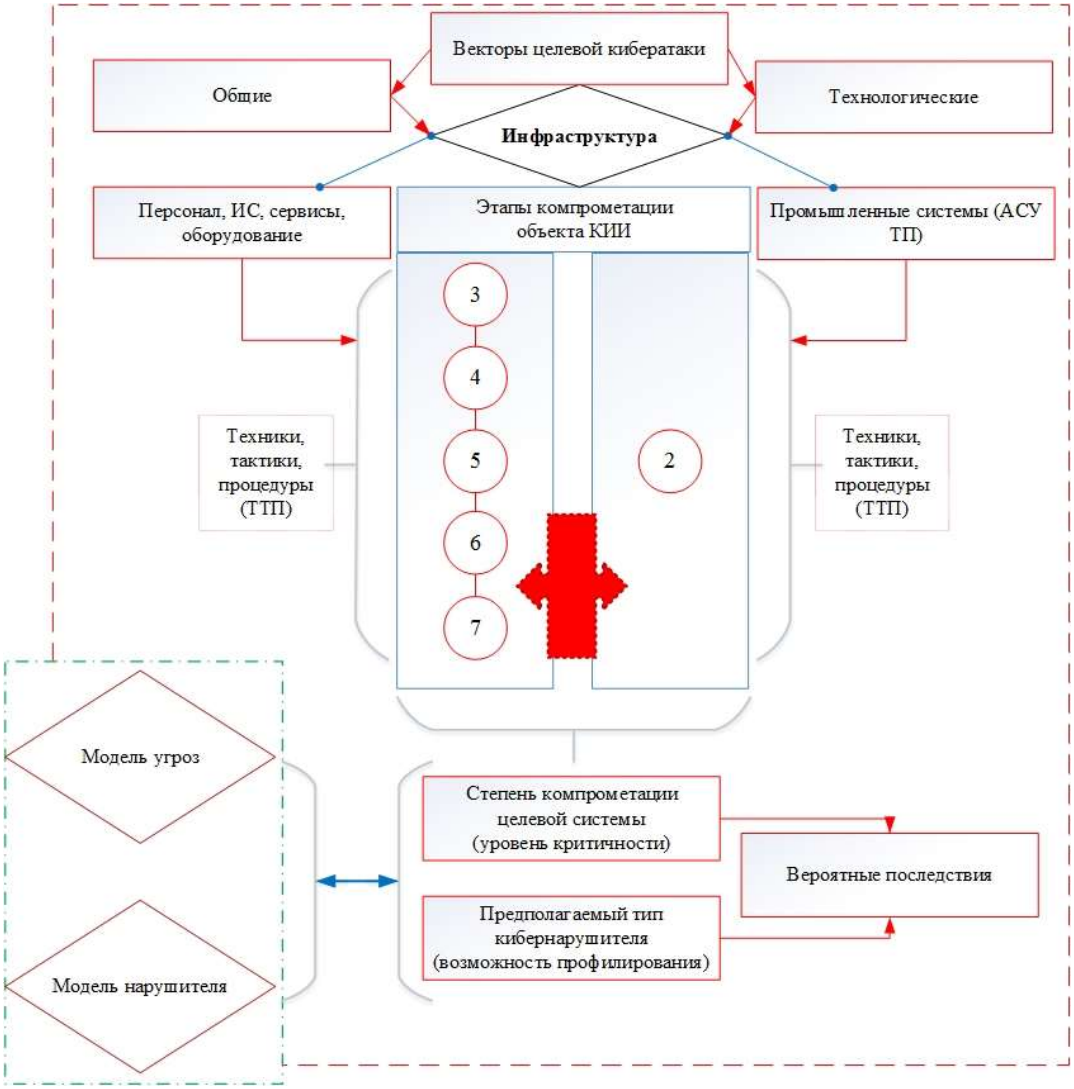


Рис. 2. Схематическое представление модели компрометации объекта КИИ

– Вероятные последствия. В зависимости от степени атрибуции кибернарушителя, можно спрогнозировать вероятные последствия для целевого

объекта. Интеграция знаний в данную модель о совершенных кибератаках и типах атакованных объектов, позволяет обозначить потенциальные или традиционные последствия относительно атакованного целевого объекта. Схематически модель имеет следующий вид (рис. 2).

Выводы

Задача предлагаемой модели - выявление схожих сценариев развития вторжения на объекты КИИ. Отличие модели компрометации от модели угроз, заключается в более конкретной направленности на атрибуцию нарушителя. Модель выступает вспомогательным элементом в процессе обогащения данных по результатам анализа целевых кибератак на объекты КИИ и является составной частью методики поэтапной атрибуции. В последующих работах планируется данную модель конкретизировать, применить на практике и при необходимости внести корректировки для улучшения итоговых показателей.

Работа выполнена при финансовой поддержке РНФ (проект № 21-71-20078).

Список используемых источников

1. The Global State of Industrial Cybersecurity. New York, USA, 2020. 10 p.
2. Федеральный закон «О безопасности критической информационной инфраструктуры РФ» от 26.07.2017 N 187-ФЗ. URL: https://fstec.ru/component/attachments/download/1906 (дата обращения: 24.02.2022).
3. Scott J. ICIT «Carbanak Threatens Critical Infrastructure» – Cybercriminal APTs Merit Significant Investigation and Discussion, October 2017, 15 p.
4. Научно-технический центр ФГУП «ГРЧЦ». URL: https://rdc.grfc.ru/2021/07/kiberataki_na_kii (дата обращения: 12.02.2022).
5. Crouching Yeti: Атаки на серверы. URL: https://ics-cert.kaspersky.ru/publications/reports/2018/04/23/energetic-bear-crouching-yeti-attacks-on-servers/ (дата обращения: 12.02.2022).
6. Hemsley K., Fisher E. History of Industrial Control System Cyber Incidents. 2018.
7. The Cyber Kill Chain. URL: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html (дата обращения: 11.02.2022).
8. O'Leary J., et al. Insights into Iranian Cyber Espionage: APT33 Targets Aerospace and Energy Sectors and has Ties to Destructive Malware. URL: https://www.mandiant.com/resources/apt33-insights-into-iranian-cyber-espionage (дата обращения: 24.02.2022).
9. Davis S., Carr N. APT33: New Insights into Iranian Cyber Espionage Group. Retrieved. URL: https://hack2interesting.com/iranian-cyber-espionage-apt33/ (дата обращения: 24.02.2022).
10. CrowdStrike Intelligence Team. SUNSPOT: An Implant in the Build Process. 2021. 61 p.
11. Supply Chain Compromise. URL: https://attack.mitre.org/techniques/T1195/ (дата обращения: 24.02.2022).
12. Enterprise Matrix. URL: https://attack.mitre.org/matrices/enterprise/ (дата обращения: 24.02.2022).

13. Marshall A., Weiss J. Malicious Control System Cyber Security Attack Case Study – Maroochy Water Services, Australia, MITRE, 2018. 16 p.

14. Ahmed Y., Asyhari A., Rahman M. A. A cyber kill chain approach for detecting advanced persistent threats // Computers, Materials & Continua. 2021. vol. 67, no. 2.

15. Хмыров С. С., Котенко И. В. Анализ расширенной модели «cyber kill chain» для атрибуции нарушителей кибербезопасности при реализации целевых атак на объекты критической инфраструктуры // XII Санкт-Петербургская межрегиональная конференция ИБРР-2021. 2021. С. 103-105.

16. Caltagirone S., Pendergast A., Betz C. The diamond model of intrusion analysis // Threat Connect. 2013. vol. 298, no. 0704. pp. 1–61.

УДК 621.391
ГРНТИ 49.31.29

ИЗУЧЕНИЕ ТЕХНОЛОГИИ МНОГОКАНАЛЬНЫХ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ НА ПРИМЕРЕ ОБОРУДОВАНИЯ СИСТЕМ КАБЕЛЬНОГО ТЕЛЕВИЗИОННОГО ВЕЩАНИЯ

К. А. Кропотова, В. Л. Можгинский

Казанский национальный исследовательский технический университет имени А. Н. Туполева - КАИ

Основным принципом построения многоканальных телекоммуникационных систем на протяжении многих десятилетий было частотное разделение каналов. Сейчас изучение технологии аналоговых многоканальных систем с частотным разделением каналов осталось лишь на теоретическом уровне, хотя на наш взгляд она заслуживает более основательного практического освоения, поскольку принципы этой технологии чрезвычайно широко и повсеместно используются.

многоканальные телекоммуникационные системы, частотное разделение каналов.

Многоканальные телекоммуникационные системы являются основой первичной сети связи в России. Основным принципом построения многоканальных телекоммуникационных систем на протяжении многих десятилетий было частотное разделение каналов. В конце прошлого века многоканальные системы перестали быть аналоговыми, поэтому оборудование для формирования группового сигнала в низкочастотной области на принципе частотного разделения каналов перестали выпускать. Изучение технологии аналоговых многоканальных систем с частотным разделением каналов осталось лишь на теоретическом уровне, хотя на наш взгляд она заслуживает

более основательного практического освоения, поскольку принципы этой технологии чрезвычайно широко и повсеместно используются.

Возможность такого практического изучения имеется, как нам представляется, на примере широко распространённых до настоящего времени систем кабельного телевидения. Система кабельного телевизионного вещания представляет собой специфическую разновидность многоканальной телекоммуникационной системы, которая у большинства операторов имеет аналоговую составляющую из 60–70 каналов. На основе аналогового оборудования одного из операторов кабельного телевидения, великодушно подаренного кафедре РТС КНИТУ-КАИ, создан лабораторный комплекс, позволяющий практически исследовать основные элементы многоканальной системы с частотным разделением каналов.

Для обучения студентов технологии формирования группового сигнала с частотным разделением каналов можно наглядно использовать модуляторы головной стации системы кабельного телевидения. Основа оборудования головной станции – модули одного из самых дорогих брендов “Blankom”. Все модули имеют идентичный конструктив (рис.).

Модульный состав оборудования Blankom в составе лабораторного комплекса:

1. Шкаф настенный Blankom
2. Blankom SNT 601, блок питания – 4 шт.
3. Blankom SDD 800, демодулятор – 14 шт.
4. Blankom GKM 800, модулятор – 23 шт.
5. Blankom SDM 800, трансмодулятор – 2 шт.
6. Blankom GKM 012, модулятор – 1 шт.
7. Blankom GSF 001, сумматор – 3 шт.
8. Blankom SEV 108, сплиттер – 6 шт.
9. Blankom GSF 101, активный сумматор – 1 шт.

ТВ-модуляторы серии GKM 800 имеют полный охват диапазона частот 47 ... 862 МГц (устройства разделены на восемь вариантов). Варианты аппаратов:

GKM 86x – 45...75 МГц
GKM 87x – 75... 100 МГц
GKM 83x – 110... 174 МГц
GKM 82x – 174...230 МГц
GKM 84x – 230...302 МГц
GKM 85x – 302...470 МГц
GKM 80x – 470...606 МГц
GKM 81x – 606...862 МГц

Часть схемы соединения модулей при создании лабораторного комплекса оставлена без изменения (как работала у оператора), частично использованы оригинальные наработки коллег по кафедре [1, 2].

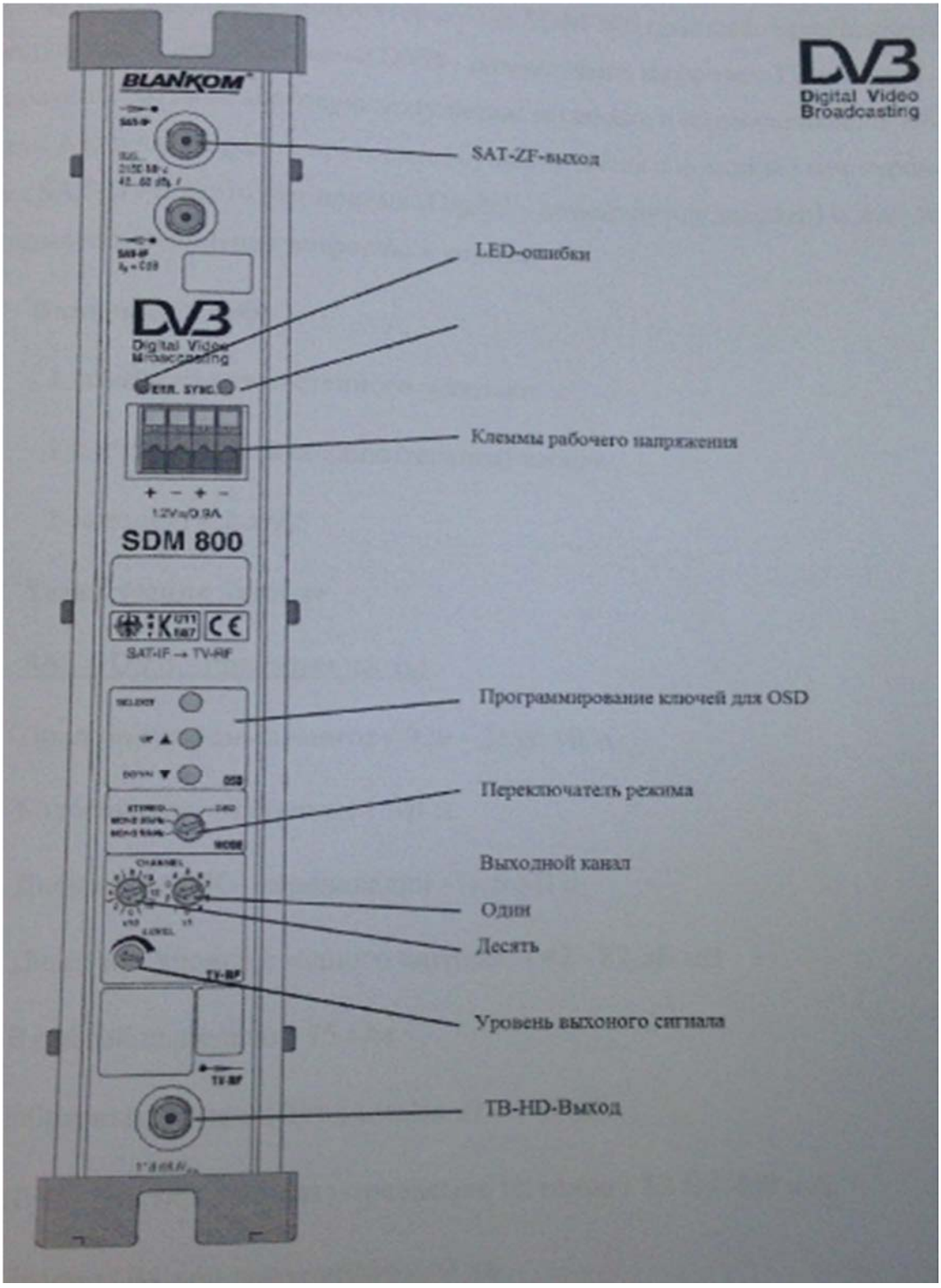


Рисунок. Фото модуля Blankom SDM 800 из документации

Полную схему соединения всех модулей здесь не приводим из-за её большого размера, и как следствие нечитаемости на формате А4, в методических рекомендациях для студентов она представлена на формате А1.

Список используемых источников

1. Урецкий Я. С., Карловский А. П., и др. Способ определения передаточных характеристик элементов конструкции многоканальной виброзащитной системы // Патент на изобретение RU 2168162 C1, 27.05.2001. Заявка № 2000102516/28 от 01.02.2000.

2. Урецкий Я. С., Карловский А. П., и др. Система передачи информации на подвижные объекты // Патент на полезную модель RU 19630 U1, 10.09.2001. Заявка №2001107545/20 от 23.03.2001.

УДК 004.75
ГРНТИ 49.33.35

МЕТРИКА ЗАЩИЩЕННОСТИ ИНТЕРНЕТ ВЕЩЕЙ

А. В. Крылов, И. А. Ушаков

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Интернет вещей (IoT) - это сеть устройств, имеющих уникальную идентификацию и встроенное программное обеспечение, необходимое для передачи информации. Конечные сетевые устройства и протоколы используются для связи с облачным сервером, который обрабатывает и агрегирует большие данные, поступающие от различных устройств, выполняет аналитику и помогает в принятии бизнес-решений. IoT является значимой частью современной революции в промышленности, сельском хозяйстве, здравоохранении и «умных» городах. Обеспечение безопасности всех субъектов, вовлеченных в сеть IoT, является особенно важным, поскольку она предполагает повсеместный сбор и распространение данных.

умные города, Интернет вещей (IoT), безопасность IoT, оценка рисков безопасности, протоколы IoT, угрозы IoT.

Риск информационной безопасности в классическом виде определяется как функция трех переменных:

– вероятности существования угрозы;

– вероятности существования уязвимости (незащищенности);

– потенциального воздействия.

Если любая из этих переменных приближается к нулю, то полный риск стремится к нулю.

Классические методы оценки рисков основываться на таких параметрах как [1]:

- $P(t)$ – вероятность реализации угрозы информационной безопасности;
- S – степень влияния угрозы на актив (экономически);
- $P(v)$ – вероятность наличия уязвимости;

- $L(t)$ – уровень угрозы;
- $L(v)$ – уровень (степень уязвимости).

В подобных методах оценки расчет риска производится с использованием значения угроз и ценности актива. Значительным недостатком является оценка в виде условных значений и то, что не учитываются реальные факторы безопасности на элементах сети, описанные ниже [2].

Физическая защищенность устройств в сети. Данный фактор отражает физическую доступность устройств для злоумышленников. Значения фактора представлены коэффициентом в численном значение от 1 до 5.

Наличие устройств, предназначенных для защиты сети. Фактор, отражающий наличие в сегменте сети специализированных устройств для фильтрации сетевого трафика и разграничения доступности сети, таких как межсетевые экраны [3]. Значения фактора представлены коэффициентом в численном значение от 0 до 2.

Уровень доступа к администрированию устройств. Этот показатель информирует о внедрении инструментов разграничения административного доступа к устройствам, который может быть использован злоумышленниками для полного контроля над сетью.

Службы и протоколы используемые в работе сети. Сетевые службы необходимое для работы сети могут как повышать уровень безопасности, так и являться местом уязвимости устройств IoT. Фактор отражает корректность работы сетевых служб и протоколов таких как dhcp, ntp, snmp, syslog.

Наличие шифрования сетевого траффика. Шифрование сетевого трафика значительно повышает сложность перехвата конфиденциальной информации. Однако использование шифрования и сетей VPN в частности повышает инфокоммуникационные затраты на создание и поддержание работоспособности сети [4].

Актуальность версий ПО. Использование актуальных версий ПО крайне важно при обеспечении информационной безопасности сети. Обнаруженные сетевые уязвимости CVE устраняются разработчиками в новых версиях ПО или малых обновлениях – патчах.

Количество устройств в сети IoT. Стоит учитывать количество устройств в сети, как конечных, так и коммутационных. Каждый узел может являться потенциальной точкой входа злоумышленника и угрозой для всей сети, следовательно, угроза безопасности прямо пропорциональна с количеством устройств. Уровень защищенности конечных устройств и коммутационных различается, так конечные устройства, в основном, более уязвимы к атакам и взлому [5]. Поэтому учитывать количество оконечных и коммутационных устройств стоит отдельно, суммируя их с разными коэффициентами, где:

*N*оконеч. – кол-во оконечных устройств в сети, таких как датчики IoT, видеокамеры, отдельные серверы и т. д., численное значение определяется в соответствии с диапазонами, таблица 3;

*N*коммут. – кол-во коммутационных устройств, таких как маршрутизаторы, межсетевые экраны, крипто шлюзы и т. д., численное значение определяется в соответствии с диапазонами, таблица 1.

Таблица 1. Диапазон численного значения кол-во устройств в сети IoT

Диапазон кол-во устройств	Численное значение $N_{оконеч}$	Численное значение $N_{коммут}$
$N > 1\,000$	-5	-4
$500 < N \leq 1000$	-4	-3
$250 < N \leq 500$	-3	-2
$100 < N \leq 250$	-2	-1
$75 < N \leq 100$	-1	0
$50 < N \leq 75$	0	1
$25 < N \leq 50$	1	2
$10 < N \leq 25$	2	3
$N \leq 10$	3	4

Каждый из вышеперечисленных критериев защищённости сегмента сети IoT оценён по степени важности, в процентном соотношении. Процентный множитель важности показывает, как сильно влияет определенный критерий на итоговую оценку всего сегмента сети. Оценка важности критериев представлена в таблице 2.

ТАБЛИЦА 2. Оценка важности критериев безопасности сегмента сети IoT

Критерий безопасности сегмента сети IoT	Процентный множитель
Физическая защищенность устройств в сети, *F*	10 %
Наличие устройств, предназначенных для защиты сети, *M*	20 %
Уровень доступа к администрированию устройств, *A*	15 %
Наличие шифрования сетевого траффика, *K*	30 %
Службы и протоколы используемые в работе сети, *S*	10 %
Актуальность версий ПО, *P*	10 %
Количество устройств в сети IoT, *N*	5 %

На основе исследованных критериев безопасности сегмента сети IoT была разработанная формула для оценки защищённости сегмента сети Интернет вещей.

Формула расчета коэффициента безопасности сегмента сети IoT:

$$D = 0,1F + 0,2M + 0,15A + 0,3K + 0,1P + 0,1S + 0,05N,$$

где F – Среднее значение показателя «Физическая защищенность устройств в сети», полученное в результате соотношения суммы показателя Fу для каждого устройства в сегменте сети к количеству всех устройств n: $F = (\sum F\text{у})/n$;

M – Показатель «Наличие устройств, предназначенных для защиты сети»;

A – Среднее значение показателя «Уровень доступа к администрированию устройств», полученное в результате соотношения суммы показателя Aу для каждого устройства в сегменте сети к количеству всех устройств n: $A = (\sum A\text{у})/n$;

K – Показатель «Наличие шифрования сетевого траффика»;

P – Среднее значение показателя «Актуальность версий ПО», полученное в результате соотношения суммы показателя Pу для каждого устройства в сегменте сети к количеству всех устройств n: $P = (\sum P\text{у})/n$;

S – Среднее значение показателя «Службы и протоколы используемые в работе сети», полученное в результате соотношения суммы показателя Sу для каждого устройства в сегменте сети к количеству всех устройств n: $S = (\sum S\text{у})/n$;

N – Показатель «Количество устройств в сети IoT», сумма коэффициентов количества устройств: $N = N\text{оконеч.} + N\text{коммут.}$;

Критерий безопасности сегмента сети IoT (D) позволяет провести аудит сегмента сети и определить уровень защищенности сети в целом. В расчёте критерия D не учитываться такие сегменты сети как: Центр обработки данных, канальные магистрали провайдеров, демилитаризованные зоны ДМЗ, облачный серверы (cloud server). В таблице 3 представлена шкала уровней защищенности сегмента сети IoT для аудита с использованием Критерия безопасности сегмента сети IoT (D):

ТАБЛИЦА 3. Шкала уровней защищенности сегмента сети IoT

Критерий безопасности сегмента сети IoT (D)	Уровень защищенности сегмента сети IoT	Уязвимость сегмента сети IoT
$D < -1$	0	Критично низкий уровень, необходимо срочное принятие мер по повышению уровня безопасности.
$-1 \le D < 0$	1	Очень низкий уровень, необходимо запланированное принятие мер по повышению уровня безопасности.
$0 \le D < 1$	2	Низкий уровень, необходимо запланированное принятие мер по повышению уровня безопасности.

Критерий безопасности сегмента сети IoT (D)	Уровень защищенности сегмента сети IoT	Уязвимость сегмента сети IoT
$1 \le D < 1{,}25$	3	Средний уровень, рекомендовано запланированное принятие мер по повышению уровня безопасности.
$1{,}25 \le D < 1{,}5$	4	Оптимальный уровень, рекомендовано запланированное принятие мер по повышению уровня безопасности.
$1{,}5 \le D < 2$	5	Высокий уровень, возможны запланированные меры по повышению уровня безопасности.
$D \ge 2$	6	Очень высокий уровень, принятие мер по повышению уровня безопасности не требуется.

Список используемых источников

1. King, J.; Awad, A.I. A Distributed Security Mechanism for Resource-Constrained IoT Devices // Informatica (Slovenia). 2016, 40, 133–143.

2. Ning, H. Unit and Ubiquitous Internet of Things; CRC Press, Inc.: Boca Raton, FL, USA, 2013.

3. Miller, M. The Internet of Things: How Smart TVs, Smart Cars, Smart Homes, and Smart Cities are Changing the World; Que Publishing: Indianapolis, Indiana, 2015.

4. Al-Fuqaha, A.; Guizani, M.; Mohammadi, M.; Aledhari, M.; Ayyash, M. Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. IEEE Commun. Surv. Tutor. 2015, 17, 2347–2376.

5. Suryadevara, N. K.; Mukhopadhyay, S. C. Smart Homes: Design, Implementation and Issues; Springer: Cham, Switzerland, 2015.

6. Савинов Н. В., Токарева К. А., Ушаков И. А., Красов А. В., Сахаров Д. В. Исследование модели сети цод на основе политик *Cisco Aci* // Защита информации. Инсайд. 2019. № 4 (88). С. 32–43.

7. Absolute security. URL: https://www.absolutesecurity.co.uk/

8. Prevent enterprise IoT security challenges with preparation. URL: http://internetofthingsagenda.techtarget.com/essentialguide/Prevent-enterprise-IoT-security-challenges-with-preparation

9. Applications and Key Challenges. In Proceedings of the 10th International Conference on Frontiers of Information Technology, Islamabad, India, 17–19 December 2012; pp. 257–260.

10. Сахаров Д. В., Красов А. В., Ушаков И. А., Орлов Г. А. Защищенная модель программно-определяемой сети в среде виртуализации *Kvm* // Электросвязь. 2020. № 3. С. 26–32.

11. Сахаров Д. В., Красов А. В., Ушаков И. А., Бирих Э. В. Моделирование защищенной масштабируемой сети предприятия с динамической маршрутизацией на основе Ipv6 // Защита информации. Инсайд. 2020. № 1 (91). С. 51–57.

12. Khan, R.; Khan, S.U.; Zaheer, R.; Khan, S. Future Internet: The Internet of Things Architecture, Possible.

УДК 621.391
ГРНТИ 49.33.29

МЕТОДЫ РЕАЛИЗАЦИИ ИММЕРСИВНЫХ ТЕХНОЛОГИЙ В СЕТЯХ СВЯЗИ ПЯТОГО ПОКОЛЕНИЯ

К. А. Кузнецов, А. С. А. Мутханна

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

С каждым годом возрастает потребность в скоростной, надежной системе передачи данных, для задач диктуемых потребителями повсеместно начинается внедрение сетей мобильной связи пятого поколения. Одна из основных проблем таких сетей - обеспечение, заявленной в IMT-2020, задержки на уровне не более 1 мс. Благодаря концепции Тактильного Интернета появился спрос на свех низкие задержки для обеспечения которых требуется превзойти скорость света при передачи информации между конечными устройствами. Для достижения таких показателей планируют применять различные технологии, позволяющие переносить сервисы ближе к абоненту (MEC), виртуаилизорать и адаптивно перемещать сетевые функции (NFV), а также предиктивно анализировать трафик и дискретные действия человека.

5G, Тактильны Интернет, MEC, NFV.

Введение

Иммерсивные технологии – это набор различных методов и средств, позволяющих воздействовать на спектр человеческих ощущений или на его часть. В последнее время такие технологии набирают все большую популярность и стремительно входят в обыденную жизнь, так, например, виртуальная реальность (VR) давно знакома многим, дополненная реальность (AR) уже активно применятся в строительстве, машиностроении и других отраслях промышленности [1]. Говоря на языке цифр, человеческое зрение не сильно чувствительно к изменениям, что позволяет с легкостью реализовывать вышеописанные технологии в сетях связи предыдущих поколений, но, переходя к другим органам чувств, картина резко меняется – реакция на тактильные ощущения достигает 1 мс, что накладывает весомые требования к круговой задержке в целях передачи таких ощущений. Сети пятого поколения, а именно сегмент URLLC (*Ultra-Reliable Low Latency Communication*), создается в целях достижения минимально возможных показателей задержки, сохраняя высокую надежность передачи. Для реализации поставленных задач далее будет рассмотрен ряд технологий, позволяющих «преодолеть» предел скорости света и существенно увеличить

возможность применения концепции Тактильного Интернета. Исследование выполняется в рамках выполнения ПНИ по государственному заданию СПбГУТ на 2021 год.

Пограничные вычисления с множественным доступом

Пограничные вычисление с множественным доступом (MEC, *Multi-access Edge Computing*) это архитектурная модель сети передачи данных, позволяющая приблизить вычислительные ресурсы и системы к абоненту, или его устройству доступа или иному устройству генерации трафика, чувствительного к задержкам. Это децентрализованное облачно-вычислительное расширение, в котором данные обрабатываются и хранятся на границе, и только те рабочие задачи, которые устойчивы к задержкам, и другие массовые или пакетные процессы передаются обратно в централизованное облако для поддержки внутренних служб (Рис. 1). Пограничные вычисления не заменяют облако, они просто размещают те части приложений, которые должны быть ближе к конечным точкам там, где они и должны находиться [2]. В публичном развертывании это означает размещение вычислительных и сопутствующих ресурсов на границе беспроводной сети общего пользования, обеспечивая доступ практически любым устройством, косвенно или напрямую поддерживающим сотовую связь, и обеспечивая покрытие на больших географических территориях. В частном развертывании, частная беспроводная сеть создается на территории предприятия и интегрируется с вычислительными ресурсами в помещении и предназначена для использования только данным клиентом, поддерживает определенные устройства и обеспечивая минимально возможную задержку. Оба варианта представляют собой комбинацию облачной вычислительной и сетевой среды, в которой всем данным не нужно курсировать между удаленными друг от друга серверами, пользователями или устройствами. За счет сокращения расстояния, которое должны преодолеть данные, уменьшается количество хопов, которые они совершают проходя через сетевое оборудование. Граничные вычисления могут уменьшить задержку при передаче данных, ускорить обработку и сохранить пропускную способность существующей сети.

Вычисления на границе также позволяют локализовать данные для организаций, которым требуется локальное хранение информации для обеспечения безопасности или конфиденциальности. Кроме того, они могут поддерживать непрерывность бизнеса позволяя региональным офисам или сайтам продолжать работать при сбоях в работе основного узла. Частные развертывания обеспечивают высочайшую производительность и низкую задержку, еще больше сокращая «последнюю милю», размещая сеть, вычислительные системы и системы хранения данных в помещениях, где генерируются данные. Это обеспечивает еще большую безопасность и суверенитет

данных по сравнению с публичным развертыванием, когда потребности клиента или приложения диктуют такие уровни производительности и безопасности.

Граничные вычисления могут обеспечить более быструю локализованную обработку данных, что совместно с сетями пятого поколения может приблизить тактильные взаимодействия к режиму реального времени.

Рис. 1. Архитектура MEC

Архитектура NFV

Архитектура NFV (*Network function virtualization*), предложенная Европейским институтом телекоммуникационных стандартов (ETSI), каждый компонент которой основан на стандартах организации для обеспечения лучшей стабильности и совместимости. NFV - виртуализация сетевых функций, которая позволит пересмотреть подходы к созданию архитектуры сети и позволит перенести сетевые функции в виртуальное пространство на базе стандартных серверов [3].

Архитектура NFV (рис. 2) состоит из:

1. Виртуализированных сетевых функции (VNFs) – это программные приложения, обеспечивающие сетевые функции, такие как совместное использование файлов, службы каталогов и конфигураций.

2. Инфраструктуры виртуализации сетевых функций (NFVi), которая состоит из компонентов инфраструктуры – вычислительных систем, систем хранения данных, сетей – на платформе для поддержки программного обеспечения, такого как гипервизор KVM или платформа управления контейнерами, необходимого для запуска сетевых приложений.

3. Управления, автоматизации и сетевой оркестрации (MANO), обеспечивает основу для управления инфраструктурой NFV и предоставления новых VNF.

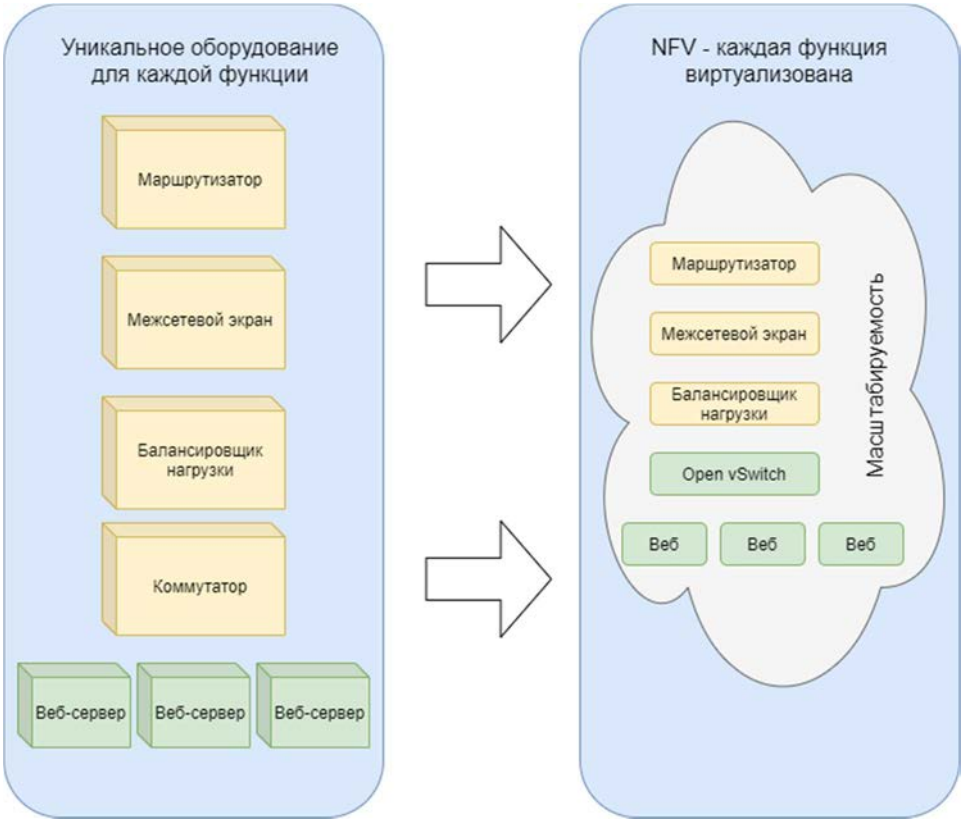


Рис. 2. Сравнение SDN и NFV

Переход к NFV можно сравнить только с переходом от аналоговых телефонных станций к цифровым в начале 70-х годов, когда производителям оборудования понадобилось такая же переориентация и переоснащение.

Предикативный анализ

Группа исследователей под руководством Элейна Вонга из Университета Мельбурна (Австралия) разработала метод усиления тактильной обратной связи в приложениях H2M, характерных для тактильного интернета. Метод может быть использован для прогнозирования правильной обратной связи в самых разных приложениях - от электронного здравоохранения до игр виртуальной реальности. Модуль, использует искусственную нейронную сеть для прогнозирования свойств материала, к которому прикасается человек. Алгоритм обучения с подкреплением позволяет угадывать подходящую тактильную обратную связь в системе H2M до того, как будет известна правильная обратная связь. Модуль, названный Event-based HAptic SAmple Forecast (EHASAF) [4], ускоряет процесс, предоставляя реакцию на прикосновение на основе вероятностного прогноза материала, с которым

взаимодействует пользователь. Чтобы облегчить работу приложений в сетях большой протяженности, модуль основываясь на данных искусственного интеллекта позволяет преодолеть эффект длительной задержки распространения информации. После определения фактического материала устройство адаптирует и обновляет свое распределение вероятности, чтобы помочь выбрать правильную обратную связь в будущем.

Заключение

Всеобщая информатизация и новые технологии в ИТ сфере, значительно влияют на архитектуру сетей связи нового поколения. Применение иммерсивных технологий за пределами одного предприятия все еще остается лишь целью исследований, но совместное применение описанных технологий позволит расширить радиус работы сети с сохранением требуемого QoS. Таким образом, решения по устранению зависимости между расстоянием и временем отклика сети имеют решающее значение для реализации передачи иммерсивных технологий, и Тактильного Интернета в частности, в сетях пятого поколения.

Исследование выполнено в рамках выполнения ПНИ по государственному заданию СПбГУТ на 2021 год.

Список используемых источников

1. Muthanna, A., Ateya, A. A., Amelyanovich, A., Shpakov, M., Darya, P., & Makolkina, M. (2018). AR Enabled System for Cultural Heritage Monitoring and Preservation. In Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) (Vol. 11118 LNCS, pp. 560–571). Springer Verlag. https://doi.org/10.1007/978-3-030-01168-0_50

2. Muthanna A. et al. Framework of QoS management for time constraint services with requested network parameters based on SDN/NFV infrastructure // 2018 10th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT). IEEE, 2018. pp. 1–6.

3. A Al-Ansi, AM Al-Ansi, A Muthanna, IA Elgendy, A Koucheryavy Survey on Intelligence Edge Computing in 6G: Characteristics, Challenges, Potential Use Cases, and Market Drivers Future Internet 13 (5), 118.

4. Wong E. Predictive touch response mechanism is a step toward a tactile internet, 2020.

УДК 004.912
ГРНТИ 20.19.27

СОВРЕМЕННЫЕ ПОДХОДЫ К ФОРМАЛИЗАЦИИ И МОДЕЛИРОВАНИЮ СЦЕНАРИЕВ ИСПОЛЬЗОВАНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ

М. Д. Кузнецов

Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)

Сбор и использование персональных данных для удовлетворения цифровых потребностей пользователей сегодня являются крайне распространенными сценариями. Пользователи активно предоставляют свои персональные данные для улучшения качества цифровых сервисов, не всегда отдавая себе отчет, какие данные они передают и как они будут обрабатываться. В то же время пользовательские соглашения – единственный способ информирования о том, какие персональные данные и как используются. Существуют различные подходы к повышению прозрачности пользовательских соглашений, в частности метод на основе онтологического моделирования. В данной работе рассматриваются результаты применения онтологий в сфере регулирования сбора и использования персональных данных, полученные в актуальных трудах по теме.

пользовательские соглашения, формальное представление, онтология, персональные данные.

Рынок Интернета и, в частности, интернета вещей являются самыми быстрорастущими областями. Такие темпы развития образуют непокрытые законодательством средства и способы обработки персональных данных, и пользовательские соглашения на использование и обработку персональных данных по сути являются единственными документами, которые регулируют законность оборота персональных данных. В связи с рядом больших утечек персональных данных, внимание сообщества было обращено на способы регулирования их оборота, в результате чего были приняты меры по улучшению законного регулирования сбора и обработки персональных данных. Одним из таких документов является General Data Protection Regulation (GDPR) [1]. Эти законодательные меры обязали поставщиков цифровых услуг четко прописывать правила оборота персональных данных. Однако пользовательские соглашения на обработку данных, призванные прояснить ситуацию с персональными данными, зачастую написаны крайне сложно, так что конечные пользователи не всегда могут понять с какими правилами они соглашаются. Поэтому проблема прозрачности пользовательских соглашений стоит как никогда остро.

По указанной проблеме ведутся исследования специалистами со всего мира. Одними из самых важных работ являются работы проекта Usable Privacy Policy [2]. В них исследователи применяют различные методы текстового анализа, но самыми точными из них пока остаются методы, основанные на моделях глубокого обучения. Не смотря на их точность, они все же обладают рядом важных особенностей, затрудняющих и замедляющих исследования. Например, такие модели нуждаются в качественных экспериментальных данных и обучающих выборках, разработка и формирование, которых крайне трудоемкая и рутинная задача.

Консорциум W3C занимается разработкой единых принципов и стандартов, называемых «рекомендациями» для Интернета, которые затем внедряются производителями программ и оборудования. Это обеспечивает совместимость между программными продуктами и аппаратурой различных компаний, что делает Всемирную сеть более совершенной, универсальной и удобной. В ряд разработок консорциума входит формат онтологии owl. На данный момент это один из популярнейших форматов для онтологического моделирования, соответственно значительная часть работ использует именно их стандарты.

В рамках проекта Usable Privacy Policy [2] авторы провели большую работу по сбору пользовательских соглашений, а также провели аннотирование при поддержке квалифицированных юристов. Важным моментом здесь является то, что исследования велись до принятия законов, регулирующих обработку и хранение персональных данных, и то, что исследуемые ими пользовательские соглашения были предназначены для веб-сайтов. Семантический фреймворк, представленный теми же авторами в работе [3], призван формализовать политики безопасности в виде онтологий. Разработчики сформулировали 57 SPARQL запросов, позволяющих извлекать данные из онтологического представления для ответа на вопросы по политикам безопасности. Работа была представлена в 2016 году и с тех пор индустрия предложила новые кейсы и проблемы для решения. В частности, не покрыты аспекты, посвященные уведомлениям для пользователей и мер, принимающихся в случае кражи или повреждения данных. Данная работа является одной из самых важных по проблемам формализации пользовательских соглашений с применением онтологических моделей. Онтология наполнялась с применением датасета OPP-115, который был сформирован в рамках проекта Usable Privacy Policy (UPP) [2]. Он содержит 115 пользовательских соглашений веб-сайтов, выбранных с помощью сервиса Amazon Alexa. К достоинствам данного датасета следует отнести разработанную его составителями схему для аннотирования, которая включает различные сценарии использования персональных данных, а также информацию об экспертах,

выполнявших разметку текстов. Каждая из политик была аннотирована несколько раз, что позволило создать более 20000 аннотаций с различными аспектами использования персональных данных.

В серии работ A Core Ontology for Privacy Requirements [4, 5, 6] авторы предлагают и поэтапно совершенствуют онтологию, призванную помочь инженерам и разработчикам информационных систем и IoT-устройств, полагаясь на 5 принципов: ясность, согласованность, расширяемость, минимальное смещение кодирования и минимальное онтологическое обязательство. Онтология разрабатывалась пошагово – на первом шаге авторы выделили четкие цели, на которых они фокусируются – помощь инженерам в разработке систем важной частью которых является безопасность. Далее авторы сфокусировались на получении актуальных знаний о предметной области и ее ключевых концептов на основе предыдущих работ, в результате чего были выделены ключевые четыре группы знаний:

– организационные концепции охватывают социальные и технические аспекты будущей системы;

– концепции для выявления рисков, которые могут поставить под угрозу требования конфиденциальности;

– концепции восстановления включают методы противодействия для снижения рисков для конфиденциальности;

– концепции конфиденциальности отражают требования/потребности заинтересованных сторон в отношении конфиденциальности.

На следующем шаге авторы провели концептуализацию – воплотили результаты исследований в онтологическую модель. Данная модель подвергалась ревизии от специалистов и исследователей в области безопасности, чтобы понять, насколько хорошо она отражает действительность. На четвертом шаге авторы реализовали спроектированную ранее модель с использованием формального языкового представления. На последнем этапе авторы произвели валидацию результатов – проверку, отвечает ли разработанная онтологическая модель требованиям специалистов и инженеров, а также проверку корректности результатов по запросам к онтологии. В ходе разработки авторы сформировали вопросы, на основе которых валидация и производилась.

Концептуальная модель включает четыре основных направления:

– organizational dimension – отражает охват социальных и технических частей системы по возможностям, целям и зависимостям;

– risk dimension – отражает риски для организационных и социальных сфер системы (например, для персональных данных);

– treatment dimension – отражает методы противодействия угрозам;

– privacy dimension – отражает охват акторов, то есть заинтересованных лиц.

В работе так же представлены осязаемые результаты – ряд SPARQL запросов и выводы по ним.

В работе Judicial Support Systems: Ideas for a Privacy Ontology-Based Case Analyzer [7] авторы полагают, что формализация юридических документов и документов, посвященных конфиденциальности в виде онтологий это очень удачное применение онтологического моделирования для поддержки принятия решений и выделяют их применение в данной области как наиболее удачное и интересное. Авторы показывают структуру разработанной ими онтологии использования персональных данных, основанную на взаимосвязи между принципами, директивами, фактами и случаями, характеризующими предметную область. Ее предназначение – помощь юридическим сотрудникам, внедрение в приложения поддержки принятия решений, связанных с юридическими аспектами использования приложений и сервисов. Ядром разработки является фреймворк DOGMA. Авторы считают, что подобное онтологическое представление юридических правил использования приложения и сервисов в последствии может быть интегрировано непосредственно в эти сервисы и приложения.

В работе MyMemory: an Ontology for Privacy Protection in External Digital Memories [8] авторы предложили онтологию применимую для обеспечения защиты данных, хранящихся на внешних носителях, в частности в облачных хранилищах, на серверах социальных сетей. В контексте работы под воспоминаниями подразумевается контент, генерируемый пользователями – их реакция на тот или иной контент, фото, видео, сообщения и т.д. Кроме того, предлагаемая онтология включает в себя тринадцать правил, которые более точно определяют семантику онтологии. Правила составляют ядро представленной онтологии в отношении ее предполагаемого использования, т. е. описывают ситуации, в которых память должна автоматически оставаться закрытой для третьих акторов, которые пытаются получить к ней доступ. Каждое правило представлено как в текстовом описании, так и на языке правил семантической паутины (SWRL). Среди упомянутых правил авторы выделяют следующие:

– определение человека как контекстного элемента;

– определение местоположения как контекстного элемента;

– владелец может получить доступ к своей памяти;

– определение человека как не владельца памяти;

– определение человека как части ситуации;

– определение местоположения как части ситуации;

– определение эмоционального состояния как части ситуации;

– определение эмоционального состояния как контекстного элемента, определение его чувств и определение его отношений с человеком и с воспоминаниями;

– классификация эмоционального состояния как стрессового;

– классификация эмоционального состояния как расслабленного;

– доступ к памяти можно получить, если владелец чувствует себя расслабленным;

– невозможно получить доступ к памяти, если владелец чувствует стресс и, если кто-то другой просит об этом.

Таким образом, в MyMemory заложены функции регулирования персонального контента, производимого пользователями. Авторы заключают, что результат их работы может быть применен к информационным системам, в частности к социальным сетям.

По результатам анализа связанных работ было выяснено, что все работы так или иначе направлены на один результат – обеспечение безопасности данных с применением онтологического моделирования. Это делается немного по-разному, причем в своих онтологиях авторы не уделяют должного внимания механизмам уведомления о тех или иных событиях и нарушениях политики или требований безопасности, хотя это тоже является частью безопасности. Такое положение дел свидетельствует о необходимости рассмотрения данного вопроса в дальнейшем.

Актуальность задачи формализации пользовательских соглашений обусловлена тем фактом, что политики безопасности являются официальным и единственным способом информировать пользователей о том, какие персональные данные собираются, и каким образом они обрабатываются.

Будущие исследования автора связаны с дальнейшей детализацией предметной области – юридических документов, регулирующих обработку распространение и удержание персональных данных пользователей, развитие в сторону автоматизированной формализации для выявления различных аспектов использования персональных данных и расчета рисков, связанных с использованием устройства или сервиса.

Список используемых источников

1. General Data Protection Regulation // gdpr.eu. URL: https://gdpr.eu (дата обращения: 23.12.2021).

2. Usable privacy policy project // usableprivacy.org. URL: https://usableprivacy.org (дата обращения: 21.12.2021).

3. Oltramari, A., et al. PrivOnto: a semantic framework for the analysis of privacy policies // Semantic Web, vol. 9. 2018. pp. 185–203.

4. Gharib Mohamad, Giorgini, Paolo, Mylopoulos John. COPri v.2 – A core ontology for privacy requirements // Data & Knowledge Engineering. 2021. doi: 133.101888.10.1016/j.datak.2021.101888.

5. Gharib Mohamad, Mylopoulos John. A Core Ontology for Privacy Requirements Engineering. 2018. Available: https://arxiv.org/pdf/1811.12621.pdf

6. Gharib Mohamad, Mylopoulos John, Giorgini Paolo. COPri - A Core Ontology for Privacy Requirements Engineering. 2020. doi: 10.1007/978-3-030-50316-1_28.

7. Tang Yan, Meersman Robert. Judicial Support Systems: Ideas for a Privacy Ontology-Based Case Analyzer // Lecture Notes in Computer Science. 2005. doi: 3762.800-807. 10.1007/11575863_100.

8. Santoro Flávia, Baião Fernanda, Rodrigues Teixeira Bianca. MyMemory: an ontology for privacy protection in external digital memories. 2018. Available: https://www.researchgate.net/publication/328579389_MyMemory_an_ontology_for_privacy_protection_in_external_digital_memories

Статья представлена доцентом кафедры информационных систем СПбГЭТУ ЛЭТИ, кандидатом технических наук, доцентом Е. С. Новиковой.

УДК 004.056
ГРНТИ 81.93.29

АЛГОРИТМЫ КОНСЕНСУСА И ПОДХОДЫ К ИХ РЕАЛИЗАЦИИ В BLOCKCHAIN СИСТЕМАХ

Д. В. Кушнир, Е. Р. Никонов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье проводится исследование алгоритмов консенсуса технологии blockchain, особенности их программной реализации на языке программирования Python. В работе затрагиваются вопросы формирования блоков, последующего анализа текущего состояния распределенного реестра и применение гибридных консенсусов.

blockchain, распределенный реестр, алгоритм консенсуса, хеширование, транзакции.

Технология *blockchain* [1], образующая последовательную связь блоков данных, была предложена еще в начале 90-х годов двадцатого века [2], но популярной и востребована стала лишь недавно, благодаря использованию совместно с криптовалютой *bitcoin*. Однако технология интересна не столько своим использованием в криптовалюте, сколько применением в других сферах и взаимосвязью рассматриваемой технологии с информационной безопасностью.

На данный момент на рынке известно множество идей, проектов, криптовалют, которые базируются на различных системах распределенного реестра и имеют разные алгоритмы обработки информации. Одни из самых важных алгоритмов, на которых базируется *blockchain*, это алгоритмы консенсуса. Споры по поводу лучших ведутся до сих пор, ведь именно от них зависят главные идеи системы – доверие и равноправие.

При создании системы *blockchain* рано или поздно встает вопрос о выборе алгоритма консенсуса [3]. Ключевая идея консенсусов заключается в

безопасном помещении данных в блок таким образом, чтобы позволить участникам сети согласовать состояние самой сети.

На данный момент самыми известными алгоритмами являются: *Proof of Work* (*PoW*) - алгоритм доказательства работы, *Proof of Stake (PoS)* - алгоритм доказательство доли владения.

Алгоритм *Proof of Work* похож на алгоритм из реальной жизни: необходимо работать и работать усердно, чтобы получить награду для поддержания своей жизни. В *blockchain* сети, основанной на *PoW,* некоторые участники с ролью *miner* работают, чтобы поддерживать сеть, добавляя в нее новые блоки и получая за это вознаграждение.

Работа заключается в решении определенной сложной и длительной задачи, результат которой быстро и легко проверить. Проверкой обычно занимаются другие участники сети. После всех процедур блоки добавляются в «цепь».

Функции хеширования широко используются для проверки целостности данных. Работа подразумевает из себя нахождение хеша для блока, отвечающего определенным требованиям. Именно данный хеш служит доказательством, а поиск доказательства – работой.

Алгоритм:

- Получение данных;
- Добавление счетчика к данным. Счетчик начинается с 0;
- Взятие хеш функции от данных и счетчика;
- Проверка, удовлетворяет ли хеш определенным условиям / требованию. Если да, то работа завершена. Если нет, то счетчик увеличивается на 1 и работа продолжается с шага 3 пока хеш не будет удовлетворять определенным условиям / требованию.

В *blockchain* системах каждое найденное значение счетчика, удовлетворяющее условиям, называется *nonce*. Чем сложнее условие (сложность), тем сложнее и требует больше времени процесс подбора *nonce*. В *bitcoin* сети требование периодически корректируется, так как по замыслу блок должен генерироваться каждые 10 минут (рис. 1).

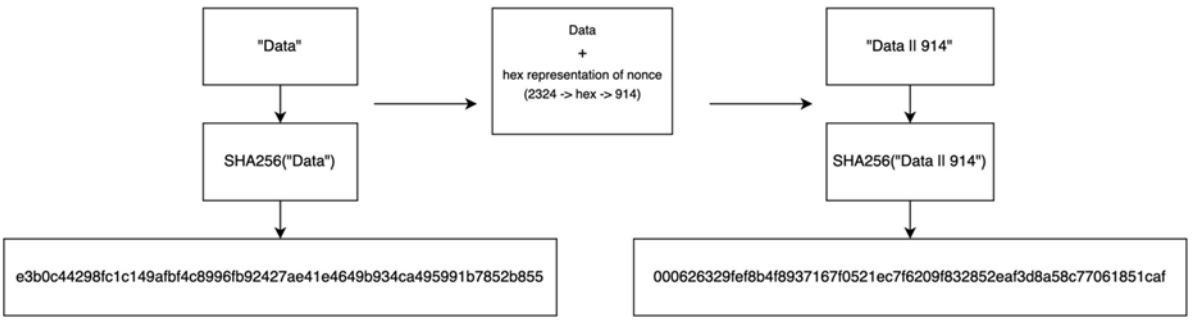


Рис. 1. Схема нахождения хеша для *PoW системы* со сложностью – 12 бит, где 914 – шестнадцатеричное представление nonce

В рамках исследования были смоделированы отдельные процессы *blockchain* систем на языке программирования Python: формирование основы *blockchain* системы; работа алгоритмов консенсуса; работа с транзакциями; работа с открытыми и закрытыми ключами.

Каждый блок в цепи представляет из себя набор определенных данных: время создания блока, транзакции; хеш предыдущего блока; хеш блока; значение счетчика – *nonce*.

Используя алгоритм *PoW,* нам необходимо назначить условие – сложность. Например, сложность равна 12 бит. Цель означает, что нам нужно найти такой хеш, который будет занимать меньше 256−12 = 244 бит (256 – длина хеша SHA-256 в битах, 64 – длина хеша SHA-256 в 16 системе), при сложности в 12 бит хеш будет иметь 3 нулевых значения вначале, как показано на рис. 1.

Реализация консенсуса *PoW*, на описанных ранее положениях, представлена на рис. 2.

```
class Block(object):
    def __init__(self, timeStamp, transactions, prevHash, hash, nonce):
        self.timeStamp = timeStamp
        self.transactions = transactions
        self.prevHash = prevHash
        self.hash = hash
        self.nonce = nonce

class Chain(object):
    def __init__(self):
        ...

    def proofOfWork(self, block):
        target = int(str(int(10**round((256 - self.targetBits)/4))), 16) # target bits -> target instance
        maxInt64 = int(9223372036854775807) # 64 bits (8 bytes). To prevent overflow
        nonce = 0
        allIdsTxsInOne = ''
        for tx in block.transactions:
            allIdsTxsInOne += tx.id
        txHash = hashlib.sha256(allIdsTxsInOne.encode('utf-8')).hexdigest()
        while nonce < maxInt64:
            allInOne = str(block.timeStamp) + str(txHash) + str(block.prevHash) + '{:x}'.format(int(nonce))
            dataHash = hashlib.sha256(allInOne.encode('utf-8')).hexdigest()
            # cmp
            if ((int(dataHash, 16) > target) - (int(dataHash, 16) < target)) == -1:
                break
            else:
                nonce += 1
        return dataHash, nonce
```

Рис. 2. Реализация консенсуса *PoW*

К достоинствам алгоритма *PoW* можно отнести: высокий уровень безопасности, децентрализованный метод проверки транзакций, вознаграждение за сформированный блок данных.

Основными недостатками являются: большое энергопотребление в ходе работы сети и большие затраты на оборудование, что может поставить под сомнение равноправие в распределенной сети.

Создавая различные системы на основе *blockchain* по алгоритму *PoW,* необходимо учитывать и возможные угрозы. К наиболее известным относят угрозы [4]: Атака 51 %, *DOS*, Атака *Sybil*.

Алгоритм консенсуса *Proof of Stake* является прямой альтернативой алгоритму *Proof of Work.* Данный алгоритм позволяет выбирать создателя нового блока данных заранее на основании его доли средств в общем количестве доли системы. Если *PoW* использует большие вычислительные мощности и запасы энергии, то *PoS* не нуждается в этом и отталкивается только от ограничения процента возможных проверок транзакций участником сети. Ограничение соответствует количеству криптовалюты (или же некоторых данных, в зависимости от системы) и времени их хранения у претендента.

Роль *miner* с данным алгоритмом теряет смысл, на её замену приходит *validator*. Криптографические вычисления сводятся к тому, чтобы подтвердить владение определенным процентом всех монет системы.

Чтобы найти все неиспользованные средства определенного пользователя, необходимо найти все его неиспользованные транзакции. На рис. 3–4 представлена реализация нахождения транзакций определенных пользователей.

```
def unspentTxs(self, pubKeyHash):
    unspentTxs = []
    unlockingInputs = []
    unspentValidTxs = []
    for block in self.blocks:
        for tx in block.transactions:
            for index, vOut in enumerate(tx.vOut):
                move = True
                for vIn in tx.vIn:
                    # if an input have any reference to the output -> tx was spent
                    if (index == vIn.vOut) and (vIn.id == tx.id):
                        move = False
                        break
                if move == False: continue
                # check if provided public key hash was used to lock the output
                if vOut.isLockedWithKey(pubKeyHash):
                    # set tx itself, index of the vOut and vOut itself
                    unspentTxs.append([tx, index, vOut])
            for vIn in tx.vIn:
                if vIn.vOut == -1: break # first transaction
                if vIn.usesKey(self.pubKeyHash(vIn.pubKey), pubKeyHash):
                    unlockingInputs.append(vIn)
```

Рис. 3. Поиск неиспользованных транзакций (1)

```
    # we have unlocking inputs and unspent transactions -> get valid unspent transactions
    if len(unlockingInputs) == 0:
        unspentValidTxs = unspentTxs
    else:
        for vOutput in unspentTxs:
            for vInput in unlockingInputs:
                equals = False
                for vInput in unlockingInputs:
                    if (vInput.id == vOutput[0].id) and (vInput.vOut == vOutput[1]):
                        equals = True
                        break
                if equals == False:
                    unspentValidTxs.append(vOutput)
                    break
    return unspentValidTxs
```

Рис. 4. Поиск неиспользованных транзакций (2)

Пользователь с ролью *validator* воспринимается «накопительным счетом» и участвует в жизни системы. Алгоритм «замораживает» средства участника на время подтверждения им транзакций (залог) и после возвращает их обратно с определенной наградой. Любой вред сети или попытки «нечестной игры» могут привести к потере репутации и средств подтверждающего.

Достоинства консенсуса *PoS*: низкие затраты на электропотребление системы в ходе работы, противодействие атакам злоумышленников из-за зависимости от доли.

Недостатки: зависимость от “жизнеспособности” крупных валидаторов, “заморозка средств”, влияние срока хранения монет на выбор подтверждающего.

Угрозы [4]: «Ничего на кону», начальное распределение, накопление возраста монет, предвычисление.

Помимо рассмотренных существуют и другие алгоритмы консенсуса, основывающиеся на них или же предлагающие другие идеи для обеспечения доверия в системе. Такие технологии пытаются устранить недостатки в существующих алгоритмах, но часто порождают новые. Однако отдельный интерес заслуживают гибридные системы, основанные на *Proof of Work* и *Proof of Stake* [5].

Помимо отдельных гибридов *PoW* и отдельных гибридов *PoS,* существуют гибриды, объединяющие обе технологии, также старающиеся нивелировать недостатки технологий по отдельности. Пример использования: криптовалюта *Decred* [6].

В рамках данной статьи были рассмотрены самые известные алгоритмы консенсуса: *Proof of Work*, *Proof of Stake*, гибриды на основе *PoW* и *PoS*. Оценены достоинства и недостатки алгоритмов, проведено моделирование отдельных процессов *blockchain* систем, включающих консенсусы, и представлены результаты.

Каждый из алгоритмов является уникальным, решает определенную задачу, но имеет недостатки, порой даже критические, что ставит под сомнение их использование в тех или иных областях. На помощь приходит альтернатива в виде гибридов, пытающихся сгладить или вовсе убрать имеющиеся помехи в использовании.

В перспективе создания *blockchain* системы продолжается разработка реализации алгоритма совместного консенсуса, использующего технологии *PoW* и *PoS*.

Список используемых источников

1. Nakamoto S. Bitcoin: A peer-to-peer electronic cash system // Decentralized Business Review. 2008. P. 21260.

2. Haber, S., Stornetta, W. S. How to time-stamp a digital document. J. Cryptology 3, 99–111 (1991).

3. Никонов Е. Р., Горбань С. А. Анализ веб-инструментов для создания системы блокчейн // Молодежная научная школа кафедры "Защищенные системы связи". 2020. Т. 1. № 1 (1). С. 57–59.

4. White Paper: Proof of Stake vs. Proof of Work // BitFury Group. URL: https://bitfury.com/content/downloads/pos-vs-pow-1.0.2.pdf (дата обращения: 02.01.2022).

5. White PaperY Xiao, N Zhang, W Lou, YT Hou: A Survey of Distributed Consensus Protocols for Blockchain Networks // BitFury Group. URL: https://arxiv.org/pdf/1904.04098.pdf (дата обращения: 02.01.2022).

6. Md Sadek Ferdous, Member, IEEE, Mohammad Jabed Morshed Chowdhury, Mohammad A. Hoque, Member, IEEE, and Alan Colman: Blockchain Consensus Algorithms: A Survey // BitFury Group. URL: https://arxiv.org/pdf/2001.07091.pdf (дата обращения: 02.01.2022).

УДК 004.056
ГРНТИ 81.93.29

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ В ТЕХНОЛОГИИ БЛОКЧЕЙН

Д. В. Кушнир, Д. В. Скробов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

С расширением возможностей подключения, популяризацией облачных сервисов и развитием Интернета вещей (IoT) децентрализованные подходы к доверительному управлению набирают обороты. Поскольку технологии блокчейн обеспечивают распределенный реестр, они привлекают огромное внимание со стороны исследовательского сообщества в различных областях применения. Целью данного исследования является общий анализ технологии блокчейн и изучение вопроса обеспечения безопасности в таких технологиях.

блокчейн, безопасность, защита информации, интернет вещей, технология распределенного реестра.

Введение

Человечество уже много веков продолжает развивать и совершенствовать средства коммуникации. Современные информационные технологии позволяют не только соединять людей и знания со всего мира, но и помогают во всех сферах современной жизни. Но, к сожалению, как и любые другие технологии, информационные технологии имеют как ряд преимуществ, так и недостатков. К таковым можно отнести участившиеся хакерские атаки, которым подвержены даже самые защищенные системы. Человечество активно пытается бороться со всеми проблемами, которые им преподносит цифровой век. Одним

из результатов такой борьбы являются технологии распределенного реестра. Одна из самых известных реализаций такого реестра является блокчейн.

Следует отметить, что распределенный реестр – это широкое понятие, описывающее разделяемые базы данных. Таким образом, алгоритмы, лежащие в основе блокчейна вписываются в более общее понятие распределенных реестров или разделяемых баз данных. Необходимо отметить, что в этом случае справедливо утверждение, что хотя все блокчейны являются распределенными реестрами, но не существуют распределенные реестры, не использующие блокчейн.

Также с появлением новых технологий постоянно возникает вопрос, как же обеспечивается безопасность в таких технологиях. В данной статье мы изучим подробнее вопрос обеспечения безопасности информации в технологии блокчейн.

Общие сведения о технологии

Для формулировки подходов к обеспечению безопасности данной технологии рассмотрим основы методов построения блокчейна и лежащие в его основе закономерности и представим его структуру. Технологии блокчейна позволяют построить распределенный реестр, в который могут добавляться данные. Одним из важных моментов является то, что нет необходимости в единой централизованной доверенной стороне — доверие распределяется между всеми узлами. Поэтому для добавления данных в регистр обычно необходимо достичь консенсуса между всеми (или квалифицированной частью) задействованных узлов.

Рассмотрим, как технологии, основанные на технологии блокчейн поддерживаются и используются. На рис. 1 показана структура блокчейна и ее основные элементы. Существует набор узлов (называемых узлами блокчейна, BCN), которые отвечают за хранение самой информации о блокчейне, которая может быть как в открытом, так и в зашифрованном виде. Затем они взаимодействуют для обновления данных блокчейна на основе алгоритма консенсуса. Консенсус обычно достигается среди подмножества BCN. Действительно, данные, которые будут включены в блокчейн, предложены одним из BCN. Такой узел либо выбирается детерминированным способом, либо случайным образом проверяется на основе некоторого установленного механизма. Таким образом, так называемые майнеры (которые присутствуют не во всех типах блокчейнов) являются подмножеством BCN.

Помимо BCN, в структуре также присутствуют еще одни участники – пользователи блокчейна (BCU). BCU готовы вставлять информацию в блокчейн. Более того, поскольку хранение информации в блокчейне обычно дорого и связано с проблемами масштабируемости, для этой цели можно было бы использовать, например, некоторое дополнительное хранилище (AS) в виде облачного хранилища или распределенных хэш-таблиц (DHT). В этом случае

блокчейн гарантирует целостность и проверяемость данных, выполняя привязку данных, т. е. сохраняя в регистре указатели на данные и соответствующую отметку времени.

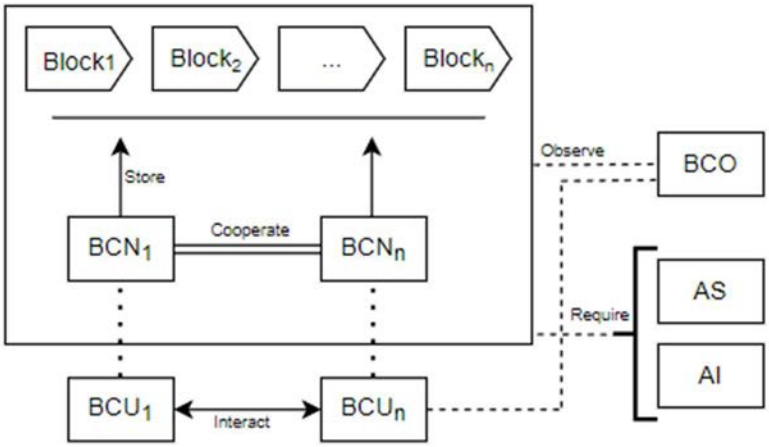


Рис. 1. Структура блокчейна и его основные элементы

Наблюдатели за блокчейном (BCO) – это те пользователи блокчейна, которые что-то получают, только извлекая данные, присутствующие в блокчейне, или наблюдая за ними. Они не вносят свой вклад в блокчейн, добавляя данные сами. Однако извлечение данных может быть записано в блокчейне посредством транзакции или взаимодействия со смарт-контрактом.

Кроме того, в некоторых блокчейн-системах имеются другие программные и аппаратные элементы для обеспечения всех необходимых возможностей. Это относится к дополнительному оборудованию или автономным программным компонентам. Эти элементы называются дополнительной инфраструктурой (AI) [1].

Консенсус. Механизмы консенсуса

Консенсус представляет собой процесс согласования финального состояния данных между узлами, которые не доверяют друг другу.

Для обеспечения функционирования инфраструктуры блокчейна, выделяются отдельные участники сети – майнеры. Роль, выполняемая ими, заключается в сборе транзакций и формирование из них блока. Блок будет включен в блокчейн при достижении консенсуса в сети. Конкретный момент времени формирования блока у каждого майнера случайны, кроме того, сами майнеры географически разнесены. Это может привести к появлению альтернативных цепочек блоков. В результате блокчейн из линейной структуры преобразовывается в древовидную. Целью консенсуса является обеспечение согласованного принятия каждым узлом сети только одной цепочки, соответствующей правилам самого консенсуса.

Если рассматривать консенсус в общем понимании, то его можно считать способом прийти к единому мнению (соглашению). Легко достичь консенсуса между двумя узлами, но в блокчейн сети принимают участие множество узлов.

Более того, участники сети могут свободно присоединяться или отсоединяться от сети, и при этом все они остаются анонимными.

В блокчейн сети не важно на сколько участники сети доверяют друг другу, или не доверяют вовсе. Они должны договориться об определенных правилах работы, которые будут затрагивать всех. И это является прямой функцией механизма консенсуса [2].

Механизм консенсуса состоит из ряда шагов, предпринимаемых всеми или почти всеми узлами в блокчейн сети для достижения планируемого состояния или значения. Механизм консенсуса в блокчейне выражается в качестве набора определенных математических правил и функций, которые дают возможность достичь соглашения между всеми участниками и обеспечить работоспособность сети.

Безопасность в блокчейне. Хеширование

Блокчейны способны достигать высокого уровня безопасности распределенных систем благодаря комбинированному использованию криптографии и механизмам консенсуса.

Так как механизмы консенсуса уже были рассмотрены выше, то рассмотрим используемые в блокчейне криптографические преобразования.

Одна из наиболее важных криптографических операций в блокчейне это хеширование. Хеширование – это преобразование массива входных данных произвольной длины в выходную битовую строку фиксированной длины, выполняемое по определённому алгоритму. Функция, реализующая алгоритм и выполняющая преобразование, называется «хеш-функцией». Итоговый результат работы называется «хешем».

Хеш каждого блока генерируется как функция от хеша предыдущего блока, что и связывает блоки друг с другом, образуя цепочку. Более того, хеш блока зависит от данных, содержащихся в этом блоке, означая, что любое изменение данных потребует изменения хеша этого блока, тем самым гарантируется неизменность данных.

Хеширование также используется в механизмах консенсуса. Существует множество хеш-функций или их семейств, например MD-5, SHA-1, SHA-2, SHA-3, ГОСТ 34.11-2018. В значительном числе реализаций блокчейна используется алгоритм SHA-256, однако есть решения и на основе других криптографических преобразованиях, например, таких как Ethash, Hex, Scrypt, NeoScrypt или даже сочетание нескольких алгоритмов.

SHA-256 (Secure Hash Algorithm) начал применяться как хеш-алгоритм первой криптовалюты Биткоин, в связи с чем успешно перешел и в другие решения, построенные по подобию Биткоина. По сути, SHA-256 представляет собой криптографическую хеш-функцию, которая призвана преобразовывать произвольный набор данных в набор фиксированной длины. При этом полученное значение будет выступать в роли дайджеста исходных данных, но восстановить сами данные из хеша уже не получится. SHA-256 относится к семейству SHA-2, которые построены на основе структуры Меркла – Дамгора. Длина

входного сообщения в SHA-256 должна быть меньше 2^{64}-1 бит. Размер блока – 512 бит, а размер слова – 32 бит. Выходное сообщение имеет длину 256 бит. Функция сжатия обрабатывает 512-битный блок сообщения и 256-битное промежуточное значение хеша. Эта функция состоит из двух основных компонентов: функции сжатия и распорядка сообщения. Алгоритм состоит из восьми шагов и делится на два этапа.

Первый этап подготовка:

1. Сообщение дополняется, чтобы добиться длины кратной 512 бит.

2. Дополненное сообщение разделяется на блоки.

3. Устанавливается изначальное значение хеш-функции, состоящее из восьми 32-битных слов, полученных путем взятия первых 32 бит дробных частей квадратных корней первых восьми простых чисел.

Вторым этапом является расчет хеш-суммы:

1. Каждый блок обрабатывается поочередно. Расчет производится в 64 цикла. В каждом цикле используются слегка отличающиеся от других циклов константы. Таким образом, результат расчета каждого цикла уникален.

2. Создается распорядок сообщения.

3. Задаются восемь вспомогательных переменных.

4. Рассчитывается промежуточная хеш-сумма.

5. Производится обработка сообщения, в результате чего получается итоговая хеш-сумма.

Безопасность в блокчейне. Программный клиент (кошелек)

Кошелек в блокчейне – это программа, клиент сети блокчейн, позволяющая хранить средства, ключи владельца кошелька, а также получать и отправлять транзакции. Принцип действия транзакций основана на использовании пары ключей, которые создаются в криптосистемах с открытым ключом. Один ключ является открытым и позволяет обозначить кому предназначены средства и проверить созданные подписи в системе. Второй ключ закрытый и отвечает за распоряжение средствами. Если знать только открытый ключ, то можно обозначить адрес, на который могут быть отправлены средства, но без секретного ключа ими нельзя будет воспользоваться.

Для выполнения транзакций и подтверждения права переводить средства криптовалюты используют асимметричное шифрование, такой вид криптографии, в котором используются два ключа и, например, ключ шифрования отличается от ключа расшифрования или ключ создания подписи отличается от ключа проверки. Такие криптографические алгоритмы получили название систем с открытым ключом.

Системы с открытым ключом используют два парных, но разных ключа – открытый и секретный. Открытый ключ находится в свободном доступе, в то время как к секретному ключу доступ есть только у его владельца. В криптографическом преобразовании ключи такого типа работают в паре. Например, если данные шифруются открытым ключом, то расшифровать их можно только с помощью соответствующего секретного ключа, как представлено

на рис. 2, или, если данные подписываются секретным ключом, то проверить подпись можно только с помощью соответствующего открытого ключа. Использовать открытый ключ из одной пары и секретный ключ из другой пары невозможно, так как каждая пара таких ключей связана определенными математическими зависимостями.

Существует несколько криптосистем с открытым ключом, например, такие как криптосистемы RSA или Эль-Гамаля. Для подтверждения транзакций при их помещении в блокчейн обычно применяются специальные алгоритмы цифровой подписи на эллиптических кривых. Наиболее распространенным в данном применении является алгоритм ECDSA (Elliptic Curve Digital Signature Algorithm) на эллиптической кривой secp256k1 [3].

Рис. 2. Схема шифрования с открытым ключом

Уязвимые компоненты блокчейна

По мере развития различных инструментов и сервисов, основанных на блокчейне, растет количество атак, имеющих цель внести данные в реестр без наличия соответствующих прав, а также добиться блокировки системы или получения злоумышленниками контроля над системой.

В основном подобные атаки рассматривают в качестве нападения следующие объекты системы:

- Криптографические алгоритмы. Самые популярные криптовалюты Биткоин и Etherium используют алгоритм ECDSA. В случае слабой реализации генератора случайных чисел при формировании секретного ключа или при выполнении алгоритма подписи, существует возможность восстановления закрытого ключа, используемого для подписания транзакции.
- Кошельки. В случае потери пароля к кошельку нет возможности восстановить доступ. При компрометации кошелька будет потерян доступ ко всем средствам, которыми кошелек управлял. Доступ к кошельку противник может осуществить через уязвимости программного обеспечения кошелька или операционной системы, на которой он работает. Также на пароль к кошельку возможна атака по словарю. Это атака, использующая метод полного перебора предполагаемых паролей.
- Механизмы консенсуса. Больше всего подвержены атакам два наиболее часто используемых алгоритма PoW (*Proof of Work*) и PoS (*Proof of Stake*). PoW подвержен атаке 51 %. Это атака, при которой злоумышленник получает кон-

троль более чем над половиной всех вычислительных мощностей в сети и получает контроль над ее ресурсами. PoS подвержен атаке Long Range. В ходе нее злоумышленник, с незначительным количеством средств, способен создать большее альтернативное количество блоков, которые по длине превзойдут основную цепочку блоков. В связи с чем основной блок может быть подменен.

- Пиринговая сеть. В основе децентрализованных сетей лежит peer-to-peer сеть – одноранговая совокупность участников блокчейн сети. На данную сеть возможны различные типы атак, в частности атака Сивилла и затемнения.
- Смарт контракты. Некоторые системы, использующие блокчейн, предоставляют возможность реализации смарт-контрактов, автоматического выполнения определенных действий, по заранее определенному алгоритму. Вместе с тем, смарт-контракт – это компьютерная программа, которая подвержена человеческому фактору и в ней могут быть ошибки и уязвимости. Особенностью является сложность внесения исправлений после распространения «ошибочного» смарт-контракта в сети. Это может создать серьезные проблемы, особенно, если создатели контракта не предусмотрели возможность вывода средств из такого контракта [4].

Заключение

В данной статье был произведен анализ технологии распределенного реестра, в частности технологии блокчейн, и, как способов обеспечения безопасности в таких системах, так и потенциальных уязвимостей в них. Распределенные реестры способны достигать высокого уровня безопасности централизованных систем благодаря комбинированному использованию криптографии и механизмов консенсуса. У технологии распределенного реестра, существуют достаточно широкие возможности для решения целого ряда задач во всех сферах человеческой жизни. В настоящее время эта технология уже активно внедрена в финансовую сферу, по всему миру, в различные системы учета, а в некоторых странах активно применяется в сфере государственного управления. Широкая распространённость решений делает необходимым дальнейшие исследования в области обеспечения их безопасности и поиска объектов потенциальных атак злоумышленников.

Список используемых источников

1. Mar Gimenez-Aguilar, Jose Mariade Fuentes: Achieving cybersecurity in blockchain-based systems: A survey. URL: https://www.sciencedirect.com/science/article/pii/S0167739X21001576 (дата обращения: 05.01.2022).
2. Джунскалиева Д. Что такое алгоритм консенсуса в блокчейне. URL: https://coinlife.com/useful/algoritm-konsensusa-v-blokchejne/ (дата обращения: 05.01.2022).
3. Binance Academy. Что Делает Блокчейн Таким Безопасным? URL: https://academy.binance.com/ru/articles/what-makes-a-blockchain-secure (дата обращения: 05.01.2022).
4. Скляр В. Безопасность блокчейн операций. URL: https://habr.com/ru/post/557926/ (дата обращения: 05.01.2022).

УДК 621.39
ГРНТИ 45.01.75

МЕТОДИЧЕСКИЙ ПОДХОД К КОМПЛЕКСНОЙ ОЦЕНКЕ ФУНКЦИОНАЛЬНОЙ УСТОЙЧИВОСТИ СИСТЕМЫ СВЯЗИ

О. А. Остроумов[1], **О. М. Лепешкин**[2], **С. П. Лапин**[1], **И. С. Черных**[1]

[1]Военная орденов Жукова и Ленина Краснознаменная академия связи имени Маршала Советского Союза С. М. Буденного

[2]Санкт-Петербургский политехнический университет Петра Великого

Рассматривая выполнение любой системой своей целевой установки необходимо учитывать имеющиеся ресурсы. Одним из основных ресурсов является время. Современные системы связи, основной целью которых является обеспечение передачи всех видов сообщений и предоставления всех видов услуг, очень динамичны. Выполнение системой цели обеспечивается устойчивым функционирование ее элементов. В работе предлагается подход к оценке функциональной устойчивости в три этапа. Актуализируется необходимость оценки последствий воздействия дестабилизирующих факторов на критически важные объекты системы связи.

критическая информационная инфраструктура, критически важный объект, функциональная устойчивость, система управления, система связи.

Особенностью современных реалий является большая динамика жизни, потребности в быстром доступе к информации, различным услугам, что обуславливает высокие требования по надежности, живучести, помехоустойчивости и др. [1–4]. Влияние различных дестабилизирующих факторов, часто приводит (может привести) к не выполнению системами, предназначенных для обмена информацией, сообщениями, данными своих функций. Обеспечение функциональной устойчивости системы достигается обеспечением функциональной устойчивости ее элементов. Контроль функционирования системы на систему управления (подсистему мониторинга и контроля).

Под функционированием понимается способность системы выполнять возложенные на нее функции в установленные сроки с требуемым качеством [5, 6].

Под функциональной устойчивость системы связи понимается способность системы связи обеспечивать обмен любыми видами сообщений и информации в установленные сроки и с требуемым качеством на всех этапах жизнедеятельности в условиях воздействия на нее различных видов дестабилизирующих факторов.

Под функционированием системы связи будем понимать способность системы выполнять возложенные на нее функции, задачи по обеспечению обмена всеми видами информации и сообщениями и предоставления всех видов услуг в условиях воздействия на нее различных видов дестабилизирующих факторов.

При контроле (мониторинге) системы связи [1, 7, 8] необходимо выявление критически важных объектов, наущение функционирования которых приводит (может привести) к нарушению функционирования всей системы. Ключевым моментом при определении критичности элемента системы является время выполнение функций, задач системы. Элемент (объект, процесс, задача и т. д.) критичный сейчас может стать не критичным потом, и наоборот не критичный сейчас станет критичным потом.

Для оценки состояния функционирования системы связи, ее критичности в работе представлен подход комплексной оценки функциональной устойчивости системы связи (СС), включающий три основных этапа:

1. Предварительный этап проектирования и построения системы связи:

– уточнение требований, целей и задач построения СС, планирование системы связи;

– моделирование структуры системы связи;

– моделирование применения системы связи;

– оценка возможностей СС с использованием полученных моделей;

– ранжирование элементов сети связи по важности для обеспечения устойчивого функционирования всех элементов системы связи, выделение наиболее критичных для функционирования системы;

– разработка рекомендаций по построению СС;

– уточнение состава сил и средств СС с учетом выше проведенных этапов.

2. Этап функционирования СС:

– оценка организации связи, построения сетей и подсистем, уточнение их возможностей;

– оценка функционирования сетей и подсистем;

– определение прогнозной эффективности примирения СС по вариантами применения;

– оценка возможности системы управления связью;

– синтез системы связи, организации новых сетей и направлений в зависимости от складывающейся обстановки.

3. Оценка результатов функционирования, разработка рекомендаций:

– формирование отчета

– разработка рекомендаций по применению СС и развитию ее, организация планирования.

На первом этапе определяется перечень требований к системе связи, выделяется главная и дополнительные цели функционирования системы,

определяются функции, задачи, оценивается имеющийся ресурс по развертыванию, функционированию и перестроению системы. Производится оценка возможностей системы, а также наличие и работоспособность системы управления связью. Кроме этого, при оценке возможностей системы связи проводится анализ состояния узлов связи, сетей и подсистем, в первую очередь состояния укомплектованности техникой и людьми. При проверке укомплектованности людьми проверяться наличие штата подразделения, его количественный и качественный состав, уровень подготовки, наличие профильного образования и образования по смежным специальностям (в том числе с присвоением соответствующей квалификации по специальности), также необходимо учитывать стаж работы в должности, т. е. практические навыки выполнения должностных обязанностей и подбор состава дежурящих смен. В рамках проверки целесообразно проведение контрольного среза, включающего теоретическую и практическую часть. Проверка укомплектованности техникой включает проверку наличия техники, ее состояния, работоспособности, наличия запасных частей и ремонтных подразделений (подразделений обеспечения), позволяющих восстановить ее работоспособность в кратчайшие сроки, а также функциональные возможности по обеспечению выполнения целей системы. При выполнении функций обеспечения сторонними организациями анализируется договор оказания услуг, сроки выполнения ими своих обязательств по каждому элементу системы связи или ее составляющим, проверяется опыт реализации ими своих обязательств, за предыдущие периоды (практическая реализация договорных отношений), в первую очередь качество и время. Обязательно обеспечивается резерв средств, обеспечивающих критически важные объекты (элементы) системы. Перечень и категория важности объектов критической информационной инфраструктуры (КИИ) представлены в реестре значимых объектов КИИ, формируемый согласно ФЗ от 26.07.2017 года № 187. Перечень элементов объектов КИИ и других КВО имеющих важное значение для функционирования системы связи, определяется опытным путем с использованием различных подходов к ранжированию объектов, исходя из:

– структурной значимости, важность для структуры всей системы;

– функциональной значимости, выполнение объектов, возложенных на него задач, для обеспечения функционирования системы;

– топологической значимости, размещение и перемещение объектов на местности, для обеспечения выполнения функционала системы;

– организационная значимость, принадлежность объекта ведомству, органу управления, административно-территориальной единице;

– психологическая значимость, психологическая устойчивость личного состава, сопротивляться психологическому воздействию, для обеспечения устойчивого функционирования объекта, системы;

– значимость для экономики, нарушение устойчивого функционирования объекта, системы приводящая к экономическим потерям;

– значимость для престижа государства, ведомства, министерства, организации;

– социальная значимость, нарушения устойчивого функционирования объектов приводит к нарушению (не выполнению) социально значимых обязательств, услуг;

– экологическая значимость, нарушение функционирования объекта, приводящее к нанесению ущерба экологии региона, государства.

Разрабатывается план реализации целей системы связи и оценивается возможность его реализации за счет имеющегося материального, людского и временного ресурсов и с учетом требований к системе.

На втором этапе производится оценка организации связи реально функционирующей системы связи, оценка ее функционирования, выполнение предъявляемых к ней требований и целей системы. Оценка прогнозируемой эффективности применения СС производится путем анализа количества обеспечиваемых с использованием элементов СС связей, обеспечивающих выполнение целей системы, по различным вариантам применения.

Оценка системы управления связью производится путем оценки органов управления и технических возможностей системы по реализации управляющих воздействий и реагированию на воздействие дестабилизирующих факторов, нарушающих функционирование системы связи и системы управления. При оценке органов управления проверяется укомплектованность подразделений, уровень подготовки, практические навыки выполнения обязанностей. Технические возможности оцениваются по реагированию на изменения обстановки. Оценка производится исходя из времени реакции (обеспечения управляющего воздействия) системы управления связью и ее элементов на дестабилизирующие факторы, нарушающие ее функционирование, с учетом выполнения мероприятий плана связи (плана выполнения мероприятий по обеспечению связи, обмена различными видами информации) и затраченных при этом ресурсах.

На третьем этапе формируются отчет функционирования системы связи и предложения по синтезу системы и дальнейшему ее развитию.

Основной задачей данной методологии является оценка функциональной устойчивости системы связи, с целью выявления критически важных элементов, объектов, процессов, связей и т. д.

Нарушение (прекращение) функционирования системы приводит к невыполнению ее своих целей, нарушению требований, предъявляемых к ней [5, 6]. Результат воздействия на различные элементы системы различный. Часть элементов имеет ключевое (критичное) значение для обеспечения функционирования системы, выход из строя (нарушение функционирования) других не скажется на выполнении системой своих задач. Рассматривая

систему связи необходимо определить не только последствия для нее нарушения функционирования отдельных элементов, но и в процессе функционирования обеспечить минимальную критичность ее элементов, т. е. система в любой момент может быть перестроена для обеспечения выполнения, возложенных на нее задач.

Список используемых источников

1. Груздев Д. А., Закалкин П. В., Кузнецов С. И., Тесля С. П. Мониторинг информационно-телекоммуникационных сетей // Труды учебных заведений связи. 2016. Т. 2. № 4. С. 46–50.

2. Пермяков А. С., Сташко Я. С. Вопросы повышения защищенности информационно-телекоммуникационной сети на основе интеллектуализации // Нейрокомпьютеры и их применение XVIII Всероссийская научная конференция. Тезисы докладов. 2020. С. 226–227.

3. Коцыняк М. А., Карпов М. А., Лаута О. С., Дементьев В. Е. Управление системой обеспечения безопасности информационно-телекоммуникационной сети на соснове алгоритмов функционирования искусственной нейронной сети // Известия Тульского государственного университета. Технические науки. 2020. № 4. С. 3–10.

4. Стародубцев Ю. И., Закалкин П. В., Иванов С. А. Техносферная война как основной способ разрешения конфликтов в условиях глобализации // Военная мысль. 2020. № 10. С. 16–21.

5. Лепешкин О. М., Остроумов О. А., Синюк А. Д. Систематизация основ методологии синтеза критической информационной инфраструктуры Российской Федерации // Военная мысль. 2021. № 8. С. 109–114.

6. Остроумов О. А., Лепешкин О. М., Ковалев Д. С., Остроумова Е. В. К вопросу о понятии критической информационной инфраструктуры системы управления // I-Methods. 2021. № 3. С. 10–15.

7. Лепешкин О. М., Харечкин П. В. Анализ моделей разграничения доступа, реализованных в современных социотехнических системах // Инфокоммуникационные технологии. 2008. Т. 6. № 2. С. 91–93.

8. Burlov V., Lepeshkin O., Lepeshkin M. Mathematical modeling of management of technosphere safety in the region // CEUR Workshop Proceedings. 9. Сер. "ICST 2020. Proceedings of the 9th International Conference "Information Control Systems and Technologies"" 2020. pp. 228–240.

УДК 621.391.827.4
ГРНТИ 47.05.09

ОБЩАЯ МЕТОДОЛОГИЯ СИНТЕЗА СИСТЕМ, ИНВАРИАНТНЫХ К НЕАДДИТИВНОЙ ПОМЕХЕ

В. В. Лебедянцев, И. И. Павлов

Сибирский государственный университет телекоммуникации и информатики

В статье рассматривается общая методология синтеза систем, инвариантных к неаддитивной помехе Ξ, которая приводит к изменению параметров сигнала. Для сравнения взяты инвариантная по отношению к помехе Ξ системы в классе систем с постоянными параметрами и не постоянными параметрами. Определяются методы модуляции и демодуляции.

неаддитивная помеха, инвариантные системы связи, аддитивная помеха, модуляция, демодуляция, помехоустойчивость.

Впервые систематизированное описание систем связи с инвариантными характеристиками помехоустойчивости встречается в работе Ю. Б. Окунева. Он рассмотрел проблемы инвариантности систем связи к аддитивной и неаддитивной помехе, ввел и описал идею абсолютной и относительной инвариантности [1].

Для обеспечения инвариантности к аддитивным помехам предложено несколько способов, базирующихся либо на выборе сигнала, либо на выборе демодулятора, а также на применении адаптивных методов приема. Инвариантность к неаддитивной (мультипликативной) помехе обеспечивалась применением соответствующего метода модуляции [2].

При разработке общих методов синтеза систем, инвариантных к неаддитивной помехе, трудно конструктивно представить действия такой помехи в общем виде. Можно только сказать, что неаддитивная помеха, которая определена через отрицание свойства аддитивности, воздействуя на отдельные (или на все) параметры сигнала, приводит к его искажению. Типичными неаддитивными помехами являются интерференционные замирания, приводящие к случайным изменениям амплитуды и фазы сигнала; эффект Допплера, связанный с перемещением отражающей среды или излучающего объекта и приводящий к изменению спектра сигнала, и т. п. [3].

В этой статье рассматривается общая методология синтеза систем, инвариантных к неаддитивной помехе Ξ, приводящей к изменению параметров сигнала.

Представим передаваемый сигнал в виде функции времени, зависящей от k определяющих параметров $\lambda_1, \lambda_2, \ldots, \lambda_k$,

$$S = S\left(t, \lambda_1, \lambda_2, \ldots, \lambda_k\right).$$

Пусть под влиянием помехи $\xi \in \Xi$ первые k_1 параметров исказились и стали равными:

$$\lambda_{1\xi} = F_1\left(\xi, \lambda_1\right), \ldots, \lambda_{k_1\xi} = F_{k_1}\left(\xi, \lambda_{k_1}\right).$$

В результате сигнал на входе приемного устройства при наличии аддитивной помехи $n \in N$ имеет вид

$$x = S\left(t, \lambda_{1\xi}, \ldots, \lambda_{k_1\xi}, \lambda_{k_1+1}, \ldots, \lambda_k\right) + n(t).$$

Построение инвариантной по отношению к помехе Ξ системы в классе систем с постоянными параметрами сводится к нахождению, во-первых, вида модуляции и, во-вторых, метода демодуляции, инвариантных к данной помехе.

Обратимся сначала к выбору инвариантного к помехе метода модуляции сигнала. Будем называть данный метод модуляции инвариантным к помехе Ξ, если информационный (модулируемый) параметр сигнала $\gamma_{инф}$, в качестве которого может выступить один из определяющих параметров λ_i сигнала или некоторое его преобразование $\Delta\lambda_i$ не зависит от помехи Ξ, т. е. если

$$\gamma_{инф} = \left\{ \begin{matrix} \lambda_i \\ \Delta\lambda_i \end{matrix} \right\} = invar\Xi \,. \qquad (1)$$

Очевидно, что условие (1) будет выполняться, если в качестве информационного параметра принять один из $k - k_i$ определяющих параметров сигнала, не подверженных действию помехи Ξ. В этом случае достигается абсолютная инвариантность информационного параметра. Прямое использование в качестве информационного параметра одного из подверженных влиянию помехи определяющих параметров сигнала в общем случае невозможно, так как при этом явно нарушается принцип инвариантности. Однако, в большинстве случаев можно найти такое преобразование Δ определяющего параметра λ_i $i = (1, 2, \ldots, k_I)$, которое будет абсолютно или хотя бы относительно инвариантным к помехе Ξ. Вид такого преобразования зависит от характеристик помехи.

Для широкого класса медленно меняющихся неаддитивных помех преобразования, обладающим свойством абсолютной или относительной инва-

риантности, является линейное дискретноразностное преобразование. Следующим этапом синтеза является определение метода демодуляции, инвариантного к помехе Ξ при выбранном методе модуляции. Сформулируем задачу более конкретно.

Оптимальные методы приема классифицируются, как известно, используемой априорной информацией о параметрах сигнала. Чем большее число параметров сигнала априорно известно, тем более высокой помехоустойчивости можно достичь. В рассматриваемом случае, по крайней мере, часть параметров сигнала подвержена искажениям случайного характера и, следовательно, в классе систем со стационарными алгоритмами эти параметры априорно неизвестны и не могут быть использованы при конструировании алгоритма демодуляции сигнала. С другой стороны, они и не должны быть использованы, так как только в таком случае алгоритм демодуляции будет инвариантен к действию помехи.

Задача нахождения алгоритма демодуляции формулируется следующим образом.

Необходимо найти алгоритм демодуляции сигнала по выбранному информационному параметру $\gamma_{\text{инф}}$, оптимальный по критерию минимума вероятности ошибки в условиях действия аддитивной помехи N при априорно неизвестных параметрах сигнала $\lambda_1, \lambda_2, \ldots, \lambda_{k1}$.

Эта задача является типичной для синтеза оптимального метода приема сигналов и решается хорошо известными методами теории статистических решений.

После выбора вида модуляции и метода демодуляции следует рассчитать вероятность ошибки при действии аддитивной помехи N. Из всех методов модуляции, инвариантных к данной неаддитивной помехе, и соответствующих им методов демодуляции выбираются такие, при которых имеет место минимум вероятности ошибки [4].

Таким образом, порядок синтеза инвариантной к неаддитивной помехе системы представляется следующим.

По известным характеристикам помехи Ξ и заданному сигналу $S(t, \lambda_1, \lambda_2, \ldots, \lambda_k)$ определяются изменения, которым подвергаются параметры сигнала $\lambda_1, \ldots, \lambda_k$ под воздействием помехи, т. е. находятся функции

$$\lambda_{1\xi} = F_1(\xi, \lambda_1), \ldots, \lambda_{k\xi} = F_k(\xi, \lambda_k).$$

Выбираются информационные параметры сигнала $\gamma_{1\ \text{инф}}, \ldots, \gamma_{m\ \text{инф}}$, инвариантные к действию данной помехи. В качестве информационных могут выступать определяющие параметры, не подверженные искажениям, или определенные преобразования определяющих параметров, инвариантные к действию данной помехи.

Для каждого вида модуляции по информационным параметрам $\gamma_{1\text{ инф}}, \ldots, \gamma_{m\text{ инф}}$ находится оптимальный при заданной аддитивной помехе N метод демодуляции и рассчитывается вероятность ошибки.

Из полученных абсолютно инвариантных систем выбирается система, обеспечивающая минимум вероятности ошибки. Эта система является оптимальной абсолютно инвариантной к данной неаддитивной помехе при заданном сигнале в классе систем с постоянными параметрами.

К сожалению, не всегда удается найти преобразования параметров сигнала, инвариантные к заданным искажениям. Кроме того, при искажениях энергетических параметров сигнала (например, его амплитуды) в присутствии аддитивного шума абсолютная инвариантность в классе систем с постоянными параметрами вообще недостижима.

Эти трудности являются следствием ограниченных возможностей систем с постоянными параметрами и могут быть преодолены при переходе к адаптивным системам.

Список используемых источников

1. Окунев Ю. Б. Системы связи с инвариантными характеристиками помехоустойчивости. М. : Связь, 1973. 80 с.

2. Лебедянцев В. В. Обобщенный инвариантный метод передачи сообщений и оценка его информационной защищенности // Инфокоммуникационные технологии. 2014. Т 12. № 3. С. 28–32.

3. Павлов И. И., Павлова М. С., Гусельников И. А., Тагаков С. С. Общее понятие о помехе в инвариантных системах передачи информации // Colloquium-journal польский международный журнал научных публикаций. 2017. № 11 (22), Ч. 6. С. 64–66.

4. Абрамов С. С., Абрамова Е. С., Павлов И. И., Павлова М. С. общие понятия адаптивной системы радиосвязи // Актуальные проблемы инфотелекоммуникаций в науке и образовании. IX Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2020. Т. 1. С. 29–33.

УДК 004.056
ГРНТИ 81.93.25

ИНСТРУМЕНТ ДЛЯ ЭКСПЕРТНОЙ ОЦЕНКИ ТОНАЛЬНОСТИ ТЕКСТОВЫХ ПУБЛИКАЦИЙ

Д. С. Левшун

Санкт-Петербургский Федеральный исследовательский центр Российской академии наук

Инструмент для экспертной оценки тональности текстовых публикаций представляет собой веб-приложение, разработанное на фреймворке Flask с помощью языка

программирования Python, взаимодействующее с PostgreSQL базой данных. Процесс работы пользователя с приложением можно разделить на три этапа: (1) подача заявки на регистрацию в качестве эксперта; (2) авторизация в системе; (3) оценка тональности текстовых публикаций. При этом текст публикации разделен на текст поста и текст репоста, что обусловлено функционалом социальных сетей, позволяющим размещать на собственных страницах публикации других пользователей и сообществ, дополняя их комментарием. В качестве текста репоста используется текст оригинальной публикации, а в качестве текста поста – комментарий, оставленный при размещении. При этом тональность поста и репоста оценивается как отдельно, так и совместно, а диапазон оценок сводится к следующим качественным характеристикам: (1) позитивно, (2) негативно, (3) нейтрально, (4) неприменимо. Данный инструмент планируется использовать для создания размеченного набора данных, который будет использован для обучения одного из компонентов системы мониторинга и выявления негативных личностных тенденций молодого поколения при взаимодействии с Интернет-пространством.

социальные сети, анализ психоэмоционального состояния, выявление негативных личностных тенденций, экспертная оценка, анализ тональности, разметка данных.

Современный человек проводит в социальных сетях значительную часть своего времени. Неудивительно, что помимо распространения нейтрального и позитивного контента, данные площадки также становятся местом распространения воздействий деструктивного характера. Отметим, что в качестве деструктивных выделяются воздействия, ставящие под сомнение общечеловеческие ценности, а также придающие позитивный окрас подобным процессам [1]. В то же время объемы информации, генерируемые социальными сетями ежедневно, огромны, что делает невозможным анализировать их эффективно без применения автоматизированных методов [2]. Именно поэтому для выявления негативных личностных тенденций, в том числе предлагается использовать обученные нейронные сети [3, 4].

Для проведения экспериментов была выбрана социальная сеть ВКонтакте [5]. ВКонтакте – крупнейшая социальная сеть среди европейцев с более чем 100 миллионами активных пользователей. Данная социальная сеть позволяет пользователям заводить профили, добавлять друг друга в друзья, вступать в различные сообщества, вести личные и групповые переписки, размещать публикации и комментировать их. Отметим, что хотя данная социальная сеть поддерживает много языков, основной язык социальной сети – русский.

Инструмент для экспертной оценки тональности текстовых публикаций представляет собой веб-приложение, разработанное на фреймворке Flask [6] с помощью языка программирования Python, взаимодействующее с PostgreSQL базой данных (см. рис. 1).

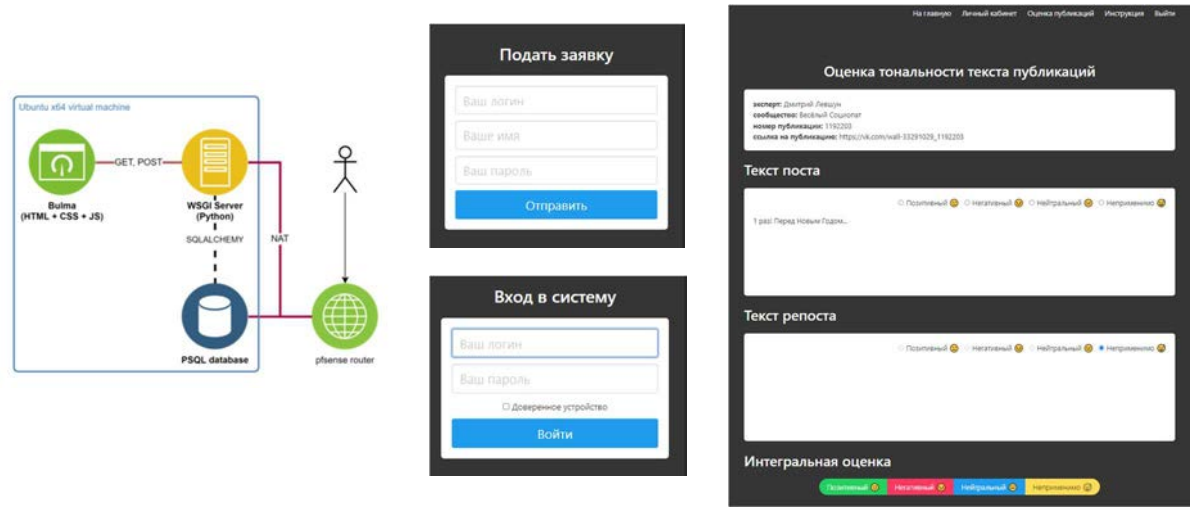


Рис. 1. Архитектура и интерфейс инструмента
для экспертной оценки тональности текстовых публикаций

Процесс работы эксперта с данным инструментом можно разделить на три основных этапа:

1. **Подача заявки на регистрацию:** пользователю предлагается ввести логин, пароль, а также свое имя, чтобы зарегистрироваться в качестве эксперта.

2. **Авторизация в системе**: после одобрения заявки, эксперту открывается возможность входа в систему. В противном случае отображается уведомление о необходимости активации учетной записи.

3. **Оценка тональности текстовых публикаций:** эксперту предлагается оценить тональность поста и репоста отдельно, а также дать интегральную оценку публикации. При этом доступны следующие оценки: (1) позитивно, (2) негативно, (3) нейтрально и (4) неприменимо. Также эксперту доступна ссылка на публикацию для уточнения контекста.

Разделение текста публикации на текст поста и текст репоста обусловлено функционалом социальных сетей, позволяющим размещать на страницах пользователей и сообществ публикации других пользователей и сообществ, дополняя их комментарием. В подобной ситуации, в качестве текста репоста используется текст оригинальной публикации, а в качестве текста поста – комментарий, оставленный при размещении (см. рис. 2).

Данный инструмент планируется использовать для создания размеченного набора данных, который будет использован для обучения одного из компонентов системы мониторинга и выявления негативных личностных тенденций молодого поколения при взаимодействии с Интернет-пространством. Для удобства экспертов, были разработаны рекомендации по оценке тональности текстовых публикаций (см. рис. 3).

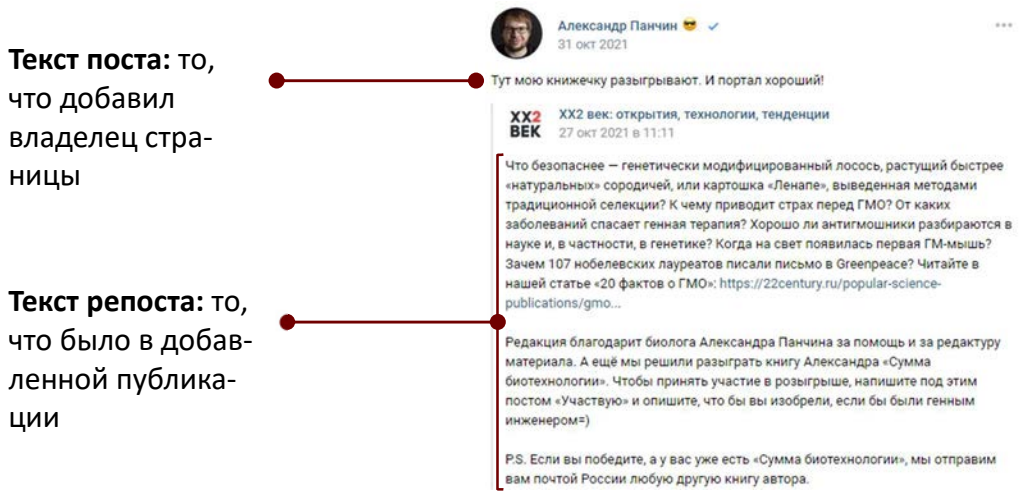


Рис. 2. Текст поста и текст репоста публикации Вконтакте

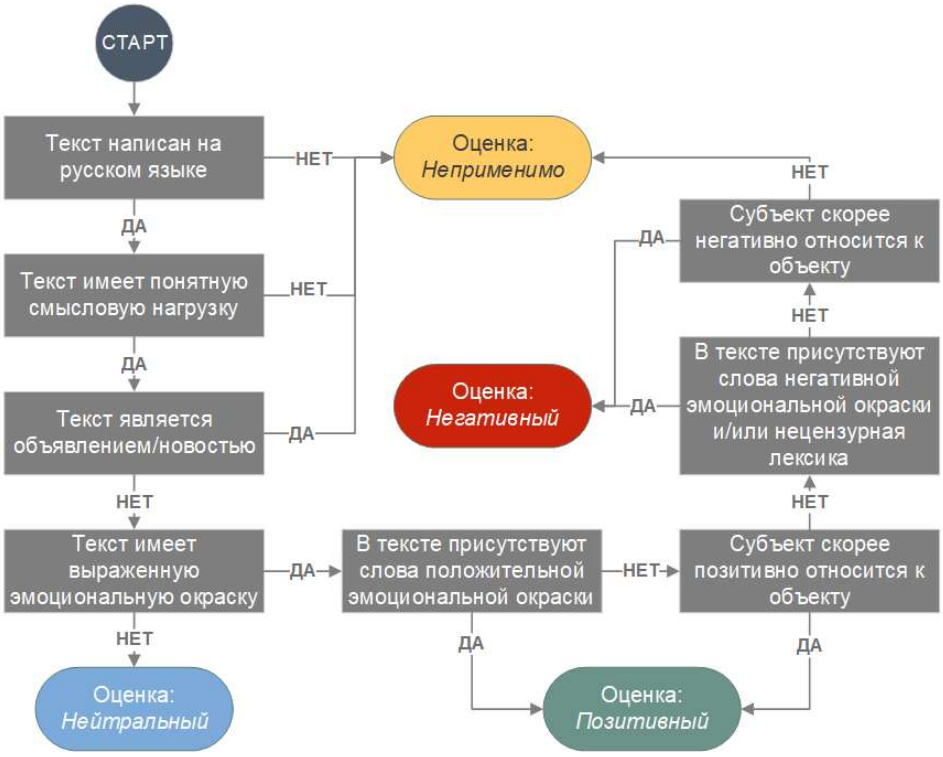


Рис. 3. Рекомендации по оценке тональности текстовых публикаций

Кроме того, данный инструмент может быть использован для решения следующих задач: (1) формирование размеченных экспертным путем наборов данных; (2) оценка тональности текстового контента сообществ; (3) анализ динамики изменения тональности контента сообществ; (4) анализ связи между тональностью и деструктивностью. А в качестве преимуществ полученного решения можно выделить следующие: (1) доступ предоставляется только авторизованным экспертам; (2) варианты оценки задаются на уровне базы данных; (3) контент может быть размечен как отдельно, так и сов-

местно; (4) контекст публикации доступен по ссылке; (5) инструмент является модульным и кросс-платформенным; (6) набор объектов оценки может быть легко расширен.

Работа выполнена при финансовой поддержке Гранта РФФИ мк 18-29-22034 в СПб ФИЦ РАН.

Список используемых источников

1. Branitskiy A., Doynikova E., Kotenko I., Krasilnikova N., Levshun D., Tishkov A., Vanchakova N. The Common Approach to Determination of the Destructive Information Impacts and Negative Personal Tendencies of Young Generation Using the Neural Network Methods for the Internet Content Processing // Proceedings of the 13th International Symposium on Intelligent Distributed Computing (IDC 2019), October 7-9, 2019, Saint-Petersburg, Russia. 2020. pp. 302–310. DOI: 10.1007/978-3-030-32258-8_36.

2. Dmitry Levshun, Olga Tushkanova, Andrey Chechulin. Active learning approach for inappropriate information classification in social networks. Proceedings of the 30th Euromicro International Conference on Parallel, Distributed and Network-Based Processing (PDP 2022). pp. 283–289. DOI: 10.1109/PDP55904.2022.00050.

3. Alexander Branitskiy, Dmitry Levshun, Natalia Krasilnikova, Elena Doynikova, Igor Kotenko, Artem Tishkov, Nina Vanchakova, and Andrey Chechulin. Determination of Young Generation's Sensitivity to the Destructive Stimuli based on the Information in Social Networks. Journal of Internet Services and Information Security (JISIS), Vol. 9, No. 3, August 2019. pp. 1–20. DOI: 10.22667/JISIS.2019.08.31.001.

4. Станкевич М. А., Игнатьев Н. А., Смирнов И. В., Кисельникова Н. В. Выявление личностных черт у пользователей социальной сети ВКонтакте // Вопросы кибербезопасности. 2019. № 4 (32). С. 80–87. DOI: 10.21681/2311-3456-2019-4-80-87

5. Социальная сеть ВКонтакте. URL: https://vk.com (дата обращения: 30.03.2022).

6. Документация фреймворка Flask. URL: https://flask.palletsprojects.com/en/2.1.x/ (дата обращения: 30.03.2022).

УДК 004.421
ГРНТИ 49.33.29

ФОРМИРОВАНИЕ ИМИТАЦИОННОЙ МОДЕЛИ ЭКВИВАЛЕТНОГО ГЕНЕРАТОРА АУДИО ТРАФИКА

М. В. Лобастова, Е. А. Лыткина, А. Ю. Матюхин

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Аудио трафик можно описать двумя процессами: процессом, описывающим поступление телефонных вызовов и процессом генерации пакетов данных, применяемым

кодеком. В статье рассмотрена модель генератора аудио трафика, который непрерывно создает пакеты, согласно заданному закону распределения. Для трафика VoIP определены его вероятностно-временные характеристики, такие как закон распределения в момент разговора, а также произведен анализ времени между вызовами и длительностью разговора. Для имитационного моделирования использовано программное обеспечение AnyLogic.

генератор аудио трафика, имитационное моделирование, закон распределения, простейший поток.

Для устройств, генерирующих аудио поток, характерен низкий объем сетевого трафика, однако на него накладываются жесткие требования к времени доставки сообщений и стандартному отклонению от среднего времени задержки. К данному типу устройств относятся все устройства речевой передачи информации, от телефонных аппаратов до систем громкоговорящей связи и оповещения, построенных на базе пакетно-ориентированных технологий передачи.

Трафик производимый, пользователем VoIP телефонии можно описать двумя процессами: процессом, описывающим поступление телефонных вызовов и процессом генерации пакетов данных, применяемым кодеком. Эти два процесса существенно отличаются масштабами времени. Если интенсивность вызовов, как правило, измеряется единицами вызовов за час, то интенсивность пакетов, производимых кодеками, определяется десятками в секунду.

Существует ряд законов распределения описывающих нагрузку сети, создаваемую одним абонентом. После получения законов необходимо обеспечить взаимосвязь параметров с целью интеграции их в имитационную модель.

Модель создана для простейшего потока вызовов. Основные параметры приведены в таблице.

ТАБЛИЦА. Параметры нагрузки, создаваемой одним абонентом

Тип генератора характеризует	Закон распределения	Параметры закона распределения
Поток во время разговора	Нормальный	$y_0 = 0{,}2$ Эрл
Продолжительность вызова	Экспоненциальный	$\lambda = 0{,}858$

Длина пакета принята постоянной, равной 200 байтам.

Структурная схема модели генератора трафика для одного VoIP абонента приведена на рис. 1. Модель содержит два источника: «callsFlow», который имитирует поток вызовов; и «pflow», который служит для имитации потока пакетов.

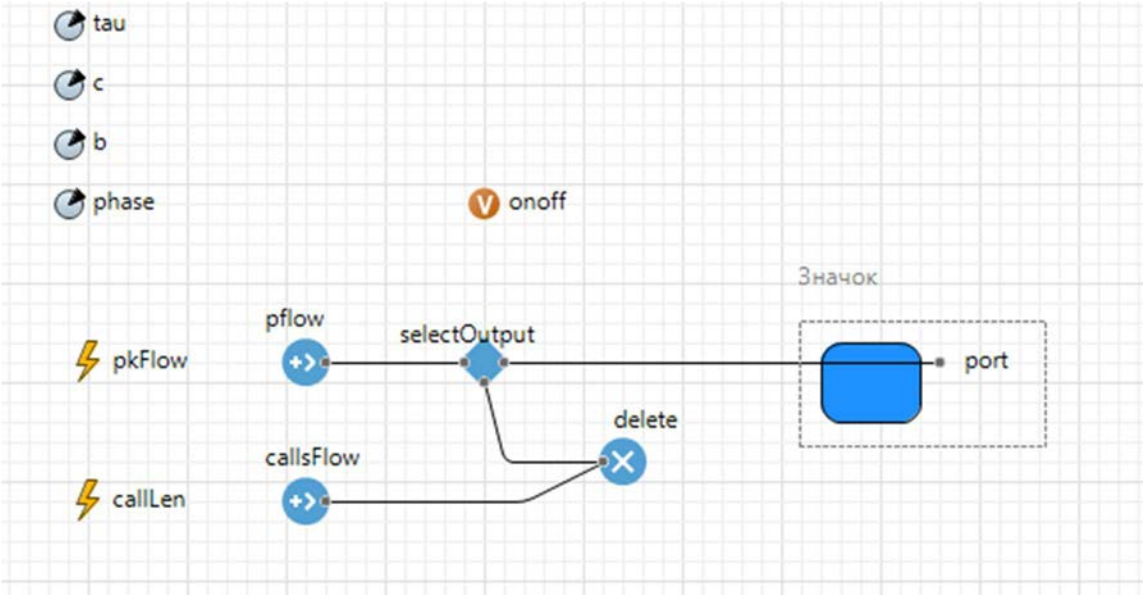


Рис. 1. Модель генератора трафика одного абонента

На рис. 2 приведена структура модели, создающей трафик группы абонентов. Главным элементом этой модели является «voIPSubs», который имеет свойства группы абонентов.

Полагая, что поток вызовов можно описать моделью простейшего потока, можно рассчитать нагрузку, создаваемую на сеть. Если количество абонентов равно n, а нагрузка одного абонента равна y_0, то интенсивность нагрузки группы абонентов рассчитывается следующим образом

$$y = ny_0 .$$

Величина интенсивности нагрузки, производимой группой абонентов равна среднему количеству активных сессий (разговоров) и может быть определена по формуле:

$$\lambda = va_0 \text{ пакетов/с},$$

где v – количество потоков, a_0 – интенсивность потока пакетов [1].

Количество потоков при известной вероятности потерь определяется из первой формулы Эрланга [2]:

$$p(y,v) = \frac{\frac{y^v}{v!}}{\sum_{i=1}^{k} \frac{y^k}{k!}}$$

Тогда с учетом размера кадра интенсивность трафика можно определить с помощью выражения

$$a = 8\lambda L \text{ бит/с},$$

где L – размер кадра в байтах.

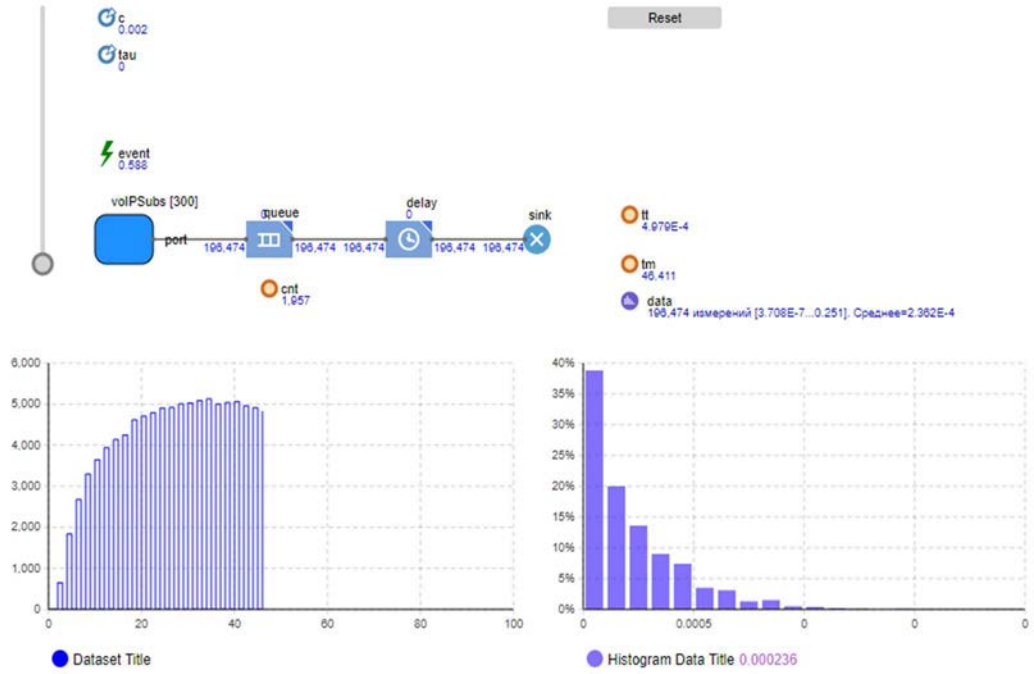


Рис. 2. Структура модели, создающей трафик группы абонентов

Таким образом, данная модель является более точным и учитывающим все аспекты создаваемой нагрузки аналогом объекта телекоммуникационной сети. Кроме того, дополнив данную модель блоками, создающими нагрузку другого типа, можно исследовать агрегированный трафик большого числа абонентов.

Список используемых источников

1. Пономарев Д. Ю. Теория телетрафика: учеб. пособие. Красноярск: СибГУ им. М. Ф. Решетнева, 2017. 160 с.

2. Зелигер Н. Б., Чугреев О. С., Яновский Г. Г. Проектирование сетей и систем передачи дискретных сообщений. М.: «Радио и связь», 1984. 177 с.

УДК 004.056
ГРНТИ 81.93.29

АНАЛИЗ УЯЗВИМОСТЕЙ ОБОРУДОВАНИЯ ПЕРЕДАЧИ ГОЛОСОВОГО ТРАФИКА

А. К. Макарова, А. В. Поляничева, К. А. Саматова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Применение Voice over IP принесло значительный вклад в развитие телефонии, оно уменьшило расходы, обеспечило качественную и эффективную коммуникацию и упростило ее использование. Технология VoIP, имеет значительные преимущества перед аналоговой телефонной связью. К сожалению, реализация этой технологии сопровождается рядом проблем, таких как проблемы совместимости, проблемы с качеством обслуживания и безопасностью. В связи с ее широким распространением актуальным является вопрос о безопасном использовании такой передачи. В рамках данной статьи будет представлен краткий обзор уязвимостей оборудования VoIP, рассмотрены самые распространённые и опасные уязвимости при передаче голосового трафика. В результате работы над докладом осуществлен критериальный анализ наиболее распространённых уязвимостей, приведены актуальные методы защиты.

телефония, безопасность IP-телефонии, уязвимости, Voice over IP.

Начавшаяся пандемия значительно ускорила внедрение технологии VoIP в связи с переходом к удаленной работе и дистанционному обучению. Организации и предприятия настолько сосредоточились на быстрой адаптации к новым условиям работы, что безопасность VoIP стала второстепенной задачей. К сожалению, многие не понимают, почему так важно безопасное использование VoIP, а также не представляют катастрофические последствия утечек данных и других кибер преступлений.

На сегодняшний день IP-телефония все больше вытесняет традиционные телефонные сети за счет следующих достоинств:

- Качество;
- Масштабируемость;
- Портативность;
- Широкий охват рынков;
- Безопасность.

Рассмотренные далее уязвимости IP-телефонии помогут увидеть основные проблемы связанные с несоблюдением обеспечения безопасности VoIP сетей и сделать выводы, необходимые для дальнейшего исследования.

Так же для каждой уязвимости предлагаются наиболее удачные методы защиты.

1. Перехват пакетов и атаки «черной дыры». Одна из наиболее распространенных атак VoIP называется перехватом пакетов, хакер крадет и регистрирует незашифрованную информацию, содержащуюся в пакетах голосовых данных, пока они находятся в пути. Так же анализ пакетов позволяет хакерам легко перехватывать имена пользователей, пароли и другие конфиденциальные данные [1].

Защита представляет собой использование VoIP VPN или виртуальных частных сетей для отправки информации. Со стороны клиентов, рекомендуется использовать сквозное шифрование всех данных и согласованный сетевой мониторинг [2].

2. Уязвимые IP-АТС и шлюзы. Злоумышленник получает удаленный доступ к шлюзу или АТС, благодаря чему имеет доступ к захвату целых сессий, узнает параметры вызова и сети, личные данные абонентов.

В целях защиты предлагается ограничить список разрешенных телефонных кодов стран, количество одновременных исходящих вызовов и реализовать строгое ограничение правилами сетевого фильтра (*Firewall*) списка IP-адресов и сетей с которых могут подключаться терминалы.

3. Атаки DoS и DDoS известны всем специалистам в области ИБ, они представляют собой отправку огромного объема данных на одно или несколько устройств, в данном случае, подключенных к VoIP. К тому же VoIP системы особенно уязвимы для таких атак, т. к. они имеют высокий приоритет в технологии обеспечения качества обслуживания QoS, и для нарушения их работы требуется меньшее количество трафика нежели для обычных сетей передачи данных.

Для минимизации ущерба и избежания последствий, следует использовать отдельное выделенное подключение к Интернету только для VoIP. VLAN специально предназначенные для VoIP-трафика, являются здесь отличным вариантом. Для пользователей VoIP, совместно использующих глобальную сеть, шифрование является лучшим способом защиты от DDoS-атак [3].

4. Утилита VOMIT (*Voice Over Misconfigured Internet Telephones*). Представляет из себя передачу голоса по неправильно настроенным IP-телефонам. VOMIT – это инструмент для взлома VoIP, который позволяет конвертировать голосовые данные, переданные посредством IP-телефонов Cisco и сжатые с помощью кодека G.711.

Защитой может служить создание частной сети АТС, так как она гораздо более безопасна, чем общедоступная сеть. Имеет место использование облачного провайдера VoIP, который шифрует вызовы перед их отправкой [4].

5. Вредоносные программы и вирусы влияют на интернет-приложения, такие как VoIP, создавая множество проблем с сетевой безопасностью. Эти вредоносные программы специально потребляют полосу пропускания сети и увеличивают перегрузку сигнала, что приводит к нарушению сигнала для VoIP вызовов.

Прежде всего, необходимо внедрить совместимые с VoIP программные и аппаратные брандмауэры, которые сканируют информацию, чтобы убедиться в ее безопасности. Некоторые маршрутизаторы активно блокируют вредоносное ПО, вплоть до блокировки опасных сайтов в сети. Уместно использование шифрования.

6. Фрикерская атака – это тип мошенничества, при котором хакеры взламывают систему VoIP, чтобы совершать междугородние звонки, менять тарифные планы, пополнять счет и совершать любые дополнительные телефонные звонки – и все это за деньги атакованной сети.

Лучшим способом предотвращения фрикинга является шифрование всех SIP-транков, приобретение программного обеспечения для защиты от программ-вымогателей, избегание сохранения платежной информации в системе и частая смена паролей учетных записей.

Для формирования случайного надёжного пароля предлагается использование следующей формулы:

$$H = \log_2 N^L = L \log_2 N = L \times \frac{\log N}{\log 2},$$

где N – кол-во возможных символов, L – кол-во символов в пароле. H измеряется в битах [5].

7. SPIT (SPAM *over Internet Telephony*) или спам по IP-телефонии, аналогичен попыткам фишинга и другому спаму в электронных письмах. SPIT содержит предварительно записанные сообщения, которые отправляются по телефонным системам VoIP. Эти звонки в основном мешают виртуальным телефонным номерам, но спам несет в себе и другие риски, такие как вирусы, вредоносное ПО и другие вредоносные атаки.

Для защиты IP-сети от подобных нападений следует использовать протоколы шифрования трафика, брандмауэры для SIP (например, решение SIParator), пограничные котроллеры сессий [6].

8. Атаки «человек посередине». Атака происходит, когда хакер внедряется между атакуемой сетью VoIP и предполагаемым пунктом назначения вызова. Обычно это происходит в общедоступных и незащищенных сетях Wi-Fi. Хакеры могут легко перехватить вызов и вместо этого перенаправить его через свои собственные серверы, где они могут легко заразить его шпионским ПО, вредоносным ПО и вирусами.

Предотвратить атаки можно отказавшись от общедоступной сети Wi-Fi, установив надежное шифрование WAP/WEP в точках доступа, а также улучшив учетные данные для входа в маршрутизатор, используя VPN и т. д. [7].

Критериальный анализ предложенной выборки уязвимостей. Необходимо провести оценку уязвимостей, опираясь на информацию об атаках. Критерии выбраны таким образом, чтобы как можно шире охватить проблематику последствий совершенной атаки и использованных ею уязвимостей.

Выделены следующие критерии для оценки уязвимостей, использованных при совершении атаки:

Степень критичности (К1) – критерий, характеризующий масштаб возможных последствий проведения атаки. Оценивается как: Низкая\Средняя\Высокая;

Популярность (К2) – наиболее освещаемые в статьях и других открытых источниках. Оценивается как: Низкая\Средняя\Высокая;

Человеческий фактор (участие в создании уязвимости) (К3). Оценивается как: Да\Нет \Частично;

Местонахождение уязвимости (уровень модели OSI) (К4) – выбирается уровень на котором реализована уязвимость (с 1 по 7);

Масштабность использования (К5) – возможность применения как можно большего количества уязвимостей. Оценивается как: Один\Несколько\Много.

ТАБЛИЦА. Критерии оценки уязвимостей

Рассмотренные атаки		Критерии				
		К1	К2	К3	К4	К5
1	Перехват	Средняя	Высокая	Да	3-4	Несколько
2	VOMIT	Средняя	Низкая	Да	3-4	Несколько
3	Уязвимые АТС и шлюзы	Высокая	Средняя	Да	2,7	Несколько
4	Dos\DDos-атаки	Высокая	Высокая	Да	1-7	Много
5	Вредоносное ПО и вирусы	Средняя	Высокая	Частично	7	Несколько
6	Фрикерская атака	Средняя	Средняя	Да	3	Несколько
7	SPIT(спам)	Низкая	Высокая	Частично	3	Несколько
8	«Человек посередине»	Средняя	Средняя	Да	2-7	Несколько

Исходя из результатов таблицы, можно сделать вывод о том, что по всем критериям превалирующим уровнем критичности обладают Dos\DDos-атаки. Говоря о критичности, важно помнить, что во время атаки замедляется или вообще приостанавливается работа сервисов компании, жертва теряет клиентов, что является значительным ударом по репутации. Сервис-провайдер может заблокировать IP-адрес жертвы, чтобы минимизировать ущерб для других клиентов. На восстановление уходят время и средства. По данным опроса компании HaltDos, DDoS-атаки рассматриваются половиной организаций как одна из самых серьезных киберугроз. Так же использует уязвимости почти на всех уровнях модели OSI.

Заключение

Решения на базе VoIP более масштабируемы, легко интегрируемы и их стоимость ниже классических решений. Однако, любая организация, внедрив VoIP решение, должна быть в курсе возможных угроз, а также предпринимать всевозможные усилия для увеличения степени информационной безопасности в сети. В результате этого исследования был сделан вывод о том, что наиболее важным вопросом в сфере безопасности VoIP сетей являются Dos\Ddos-атаки. С каждым годом количество проведенных Dos-атак становится все больше. Это подтверждается большим количеством статей о краже данных и статистикой, собранной различными открытыми источниками (например, *Positive Technologies*).

Список используемых источников

1. Полугина Ю.К. Угрозы безопасности VoIP // Региональная ифнорматика и информационная безопасность: сб. науч. тр. / Изд-во Санкт-Петербургского общества информатики, вычислительной техники, систем связи и управления, 2017. С. 231–234.

2. Баталова Н. Безопасность VoIP у операторов связи: «классика» IP-сетей и новые задачи // Connect! Мир связи. 2011. N 6. С. 12–16.

3. Балашов Д. Безопасность VoIP // Технологии и средства связи. 2013. N 4. С. 38–40.

4. Алексеев А. С., Сокол Д. С. Обеспечение защищенности VoIP // Вестник современных исследований. 2019. N 3.3. С. 4–8.

5. Матрохина К. В. Принципы защиты информации в VoIP и IM системах // Научно-технический прогресс // Актуальные и перспективные направления будущего: материалы VIII межд. науч. конф., Санкт-Петербург, 16 июля 2018 г. С. 46–48.

6. Ковцур М. М. Протоколы обеспечения безопасности IP-телефонии // Первая миля. 2012. Т. 32. N 5. С. 18–27.

7. Липатников В. А., Сокол Д. С. Модель нарушителя безопасной передачи информации в сетях VoIP-телефонии // Транспорт России: проблемы и перспективы: материалы юбилейной межд. науч. конф., Санкт-Петербург, 10-11 ноября 2020 г. С. 187-188.

Статья представлена
заведующим кафедрой ЗСС СПбГУТ
кандидатом технических наук, доцентом А. В. Красовым.

УДК 004.056.57
ГРНТИ 81.93.29

ПОСТРОЕНИЕ ОБЩЕЙ МОДЕЛИ АДАПТИВНОЙ СИСТЕМЫ RPA ДЛЯ ЗАЩИТЫ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ В ЛОКАЛЬНО-ВЫЧИСЛИТЕЛЬНОЙ СИСТЕМЕ

Е. И. Максимова, И. Г. Штеренберг

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Самомодифицирующийся код для стеговложения информации в адаптивной системе RPA - элемент программы RPA, а именно самомодифицирующийся код, который может быть доступен для использования оператором. Особенность самомодифицирующегося кода в его стегонаграфических преобразованиях, то есть в возможности оставаться незамеченным для системы и наиболее успешно сохраняться в файловых структурах. В дополнение он обладает механизмом самодописания или самомодификации, чем скорее напоминает полиморфные компьютерные вирусы. Однако элемент скрытности и развития иллюстрирует аналогию с бионическими системами, где каждая живая клетка стремиться выжить и защититься. Такой уклад и такая возможность позволят RPA защититься от тотального уничтожения и активироваться в системе вновь.

АС – Адаптивная система, RPA– Robotic process automation, ПО-программное обеспечение, Методы защиты, адаптивные системы.

Анализ скрытых каналов включает в следующие задачи:

– проведение классификации объектов защиты в зависимости от степени опасности воздействия злоумышленника с использованием СК;

– определение типов анализируемых СК в зависимости от объектов защиты и требований доверия;

– проведение анализа потенциальных СК, включающее в себя: идентификацию (выявление) СК, оценку пропускной способности СК и оценку опасности, которую несет их скрытое функционирование;

– подтверждение наличия (отсутствия) потенциальных скрытых каналов;

– получение обоснованных выводов по результатам анализа.

– определение указаний по эксплуатации, направленных на защиту от воздействия злоумышленника, реализуемого с использованием СК, и включающие в себя: принятие решений о внедрении защитных мер для противодействия угрозам безопасности, противодействие реализации СК вплоть до его уничтожения.

Классификация объектов защиты

В таблице (ТАБЛИЦА) представлены предустановленные роли объекта оценки (ОО), объекты защиты и разрешенные виды доступа.

ТАБЛИЦА 1 Предустановленные роли ОО

Наименование роли	**Объекты доступа и ассоциированные с ними тип доступа**				
	Объект_1	**Объект_2**	**Объект_3**	**Объект_3**	**Объект_M**
Роль_1	Полный доступ	Полный доступ	Полный доступ	Полный доступ	Полный доступ
Роль_2	Только чтение	–	Полный доступ	Полный доступ	–
Роль_N	–	Полный доступ	–	–	–

В зависимости от степени опасности атак с использованием СК защищаемые объекты классифицированы как активы, содержащие информацию ограниченного доступа или персональные данные и обрабатываемые в системах, имеющих технические интерфейсы с открытыми сетями или компьютерными системами общего доступа, а также компьютерными системами, не предполагающими защиту от утечки по техническим каналам [1].

Защищаемые объекты также можно классифицировать как активы, связанные с функционированием критически важных объектов и как активы, содержащие аутентификационную/парольную информацию, в том числе аутентификационная информация систем защиты информации и пароли доступа к иным активам.

Угрозы безопасности, которые могут быть реализованы с помощью СК, включают в себя:

– утечку кодов аутентификации или паролей;

– утечку отдельных информационных объектов.

В соответствии с РД ФСТЭК России «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» при проведении испытаний на соответствие пятому уровню доверия должны быть выполнены требования по выявлению и последующему анализу скрытых каналов по памяти.

Анализ скрытых каналов

В соответствии с ГОСТ Р 53113.2-2009 опасность СК основана на предположении постоянного доступа нарушителя безопасности к информационным ресурсам эксплуатирующей организации и воздействии через эти каналы на информационную систему для нанесения максимального ущерба организации [2].

Общая схема механизма функционирования СК в автоматизированной системе, элементы которой являются средой функционирования ОО представлена на рис.

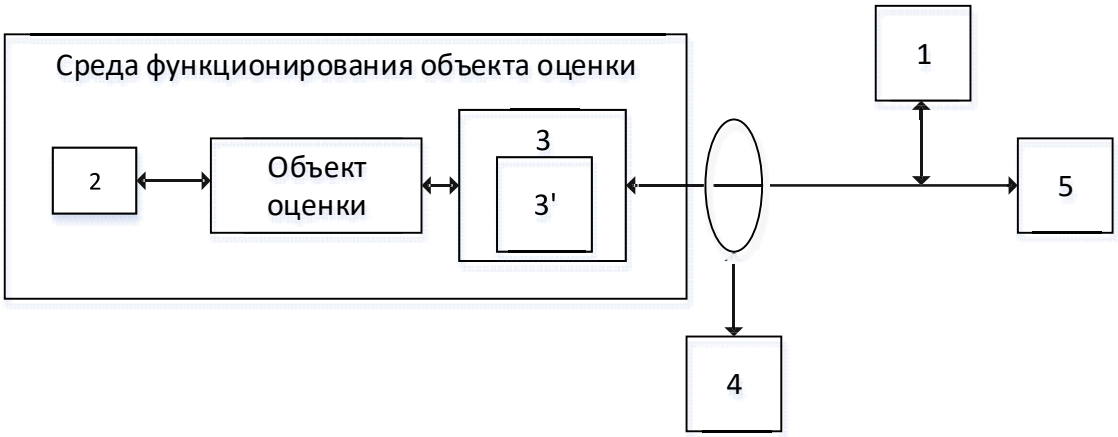


Рисунок. Общая схема механизмов СК ОО в среде функционирования

На рисунке введены следующие обозначения:

1 – нарушитель безопасности (злоумышленник), целью которого является несанкционированный допуск (НСД) к информации ограниченного доступа либо несанкционированное влияние на автоматизированную систему (АС);

2 – информация ограниченного доступа либо критически важная функция;

3 – субъект, имеющий санкционированный доступ к *2* и *5*;

3′ – агент нарушителя безопасности, находящийся в замкнутом контуре с *2* и взаимодействующий с *2* от имени субъекта *3*;

4 – инспектор (программное, программно-аппаратное, аппаратное средство или лицо), контролирующий (ее) информационное взаимодействие *3*, пересекающее замкнутый контур, отделяющий объект информатизации от внешней среды;

5 – субъект, находящийся вне замкнутого контура, с которым *3* осуществляет санкционированное информационное взаимодействие.

Взаимодействие между субъектами *3* и *5* является санкционированным и необходимым для правильной работы ОО. Задача агента *3′* заключается в том, чтобы обеспечить регулярное интерактивное взаимодействие между агентом и злоумышленником. Агент должен передать информацию ограниченного доступа *2* злоумышленнику *1* либо по команде злоумышленника *1* оказать воздействие на критически важную функцию *2*. Скрытность канала взаимодействия между злоумышленником *1* и агентом *3′* заключается в том, что субъект *3*, инспектор *4* и субъект *5* не обнаруживают факт передачи информации или команды [3].

СК позволяют злоумышленнику регулярно интерактивно осуществлять взаимодействие со своим агентом, использующим в среду функционирования ОО.

В рамках проводимого анализа рассматриваются потенциальные скрытые каналы по памяти.

Поиск потенциальных скрытых каналов по памяти осуществляется в следующем порядке:

1) Проанализировать на предмет наличия информационных потоков, использующих интерфейс функций безопасности объекта (ИФБО) и интерфейс функций объекта (ИФО), а также информационных потоков образованных ОО и средой его функционирования и ОО проектную документацию в составе:

– Функциональная спецификация,
– Технический проект,
– Эскизный проект,
– Архитектура безопасности.

2) По результатам анализа составить перечень потенциальных скрытых каналов, использующих элементы среды функционирования и которые могут участвовать в формировании информационных потоков в интересах нарушителя или агента нарушителя. Перечень оформляется в виде таблицы (табл. 2).

ТАБЛИЦА 2. Форма представления перечня потенциальных скрытых каналов

№ п/п	Идентификатор	Носитель	Кем формируется	Пропускная способность	Класс

Выявление скрытых каналов с использованием внешней памяти достигается последовательным решением следующих задач:

– анализ программного обеспечения (ПО) (Изделия) на наличие фактов использования файлов в качестве разделяемых ресурсов, когда один процесс (поток) записывает данные в память, а другой процесс (поток) имеют возможность читать/модифицировать эти данные;

– исследование ПО на возможность использования разделяемых ресурсов процессами (потоками), обладающими разными привилегиями на доступ к защищаемой информации.

Тестирование скрытых каналов внешней памяти

Тестирование скрытых каналов внешней памяти осуществляется исследованием ОО на возможность использования разделяемых ресурсов процессами (формирующими информационные потоки), соответствующим разным пользователям (ассоциированными с различными субъектами доступа

среды функционирования), например, когда «авторизованный» процесс (информационный поток, сформированный с привилегиями авторизованного пользователя) записывает в разделяемую память защищаемую информацию, которую может прочитать «неавторизованный» процесс (информационный поток, сформированный непривилегированным пользователем), не имеющий доступа к защищаемой информации [6].

Для компонент ОО, функционирующих под управлением операционной системы (ОС) Linux тестирование осуществляется с помощью ПО Strace, ПО Inotifywatch и ПО Inotifywait, в приведенной ниже последовательности действий:

1. В ходе проведения функционального тестирования, проводимого согласно документу программа и методика испытаний. определить процессы ОО, осуществляющие запись защищаемой информации в файлы (с помощью ПО Strace и экспертным анализом). Зафиксировать имена и размеры выделяемой оперативной памяти для каждого из процессов.

2. Зафиксировать перечень файлов, в которые осуществляется запись защищаемой информации и соответствующие процессы (с помощью ПО Strace и экспертным анализом).

3. Выделить процессы, которые читают записанную защищаемую информацию из файлов, зафиксированных на шаге 2.

4. Сравнением состава процессов осуществляющих чтение и процессов выполняющих запись выявить разделяемые ресурсы среды функционирования (с помощью ПО Inotifywatch, ПО Inotifywait и экспертным анализом).

5. Проверить соответствие владельцев процессов записи и чтения, а также наличия разрешения у неуполномоченных пользователей на доступ к разделяемым ресурсам (файлам).

6. Сформулировать выводы о «авторизованном» или «неавторизованном» использовании разделяемых ресурсов.

ПО Strace (см. Шаги 1 и 2) осуществляет трассировку исследуемого ОО, путем перехвата (отслеживания) системных вызовов, порождаемых процессами ОО, включая дочерние. Среди всех возможных системных вызовов она выбирает (фильтрует) и регистрирует только те, которые связаны с записью информации в файлы ОО. Перечень системных вызовов, зарегистрированных ПО Strace, подвергается экспертному анализу с целью составления списка файлов, которые могут быть использованы в качестве разделяемых ресурсов. При этом в качестве основного критерия фильтрации всех возможных событий надо использовать наличие соответствующих процессов, которые осуществляют запись в файлы защищаемой информации. В дальнейшем, даже временно записанная в эти ресурсы информация, не должна читаться процессами, влалельцами которых является непривилегированный пользователь среды функционирования [7].

На Шаге 3 (выявление разделяемых ресурсов) реализуется последовательным использованием ПО Inotifywatch и ПО Inotifywait применительно к файлам, выявленным на шаге 2. С помощью ПО Inotifywatch формируется таблица, содержащая статистические данные по использованию файлов, а с помощью ПО Inotifywait – формирование списка процессов, выполняющих чтение для последующего их сравнения с процессами выполняющими запись.

Шаги 4 и 5 реализуются методом экспертной оценки.

В таблице 3 представлена методика осуществления проверки скрытых каналов по памяти.

Тестирование скрытых коммуникационных каналов

Тестирование потенциальных скрытых коммуникационных каналов включает в себя:

– оценку архитектуры ОО и имеющихся в ней коммуникационных каналов, образованных ИФБО и ИФО;

– выявление возможных путей обмена скрытой информацией между злоумышленником и его агентом в среде функционирования ОО путем анализа сетевого взаимодействия в ходе проверки ФБО;

– оценку опасности выявленных СК для защищаемой информации;

– принятие решения о целесообразности противодействия каждому из выявленных СК.

Для ОО тестирование осуществляется в приведенной ниже последовательности действий:

1) Проанализировать указанные в документации ИФБО и ИФО на предмет использования ими коммуникационных каналов связи.

Коммуникационные каналы связи, образованные ИФБО и ИФО используют протоколы, которые представлены в таблице 4.

ТАБЛИЦА 1. Последовательность действий для перехвата событий, связанных с использованием внешней памяти в качестве ресурса

№ п/п	Описание выполняемого действия	Ожидаемый результат
1	*Установить (при отсутствии) используемые инструментальные средства от имени администратора:* *..# apt install strace* *..# apt install inotify* *..# apt install inotify-tools*	*Отображение процесса установки на экране монитора*
1.1	Проверить установку утилит командой выдачи справочной информации: *..# strace -h* *..# inotifywatch -h* *..# inotifywait –h*	Выдача справочной информации по использованию *установленных* утилит на экран монитора
2	*Выявление процессов (потоков) Изделия, осуществляющих запись защищаемой информации в файлы*	
2.1	Запустить утилиту «strace» для перехвата системных вызовов, порождаемых процессами исследуемого ПО и связанных с записью информации в файлы: *strace -xff -e trace=open,write -o stracelog <имя приложения>* Назначение параметров команды: *x* – выводить не-ASCII строки в шестнадцатеричном формате; *-o stracelog* – запись «лога» трассировки в файл «*stracelog.**»; *ff* – (совместно с параметром *–o)* «лог» каждого трассируемого процесса будет записан в файл «*stracelog.pid*», где *pid* – идентификатор процесса; *-e trace=open, write* отслеживать системные вызовы «открытия файла»» и «записи» информации в файл.	Наличие одного или нескольких (по числу отслеживаемых процессов) лог-файлов с именами «*stracelog.pid*»
2.2	Для получения сведений о запущенных процессах выполнить команду: *ps -l > procname.txt*	Сведения о запущенных процессах (имена, PID и др.) записаны в файл «procname.txt»
2.3	Выполнить экспертный анализ результатов «трассировки» исследуемого ПО с целью составления списка файлов, которые могут быть использованы в качестве «разделяемых» ресурсов: 1.Анализируя перечень системных вызовов в лог-файлах «*stracelog.pid*», оставить имена только тех файлов, в которые осуществлялась запись защищаемой информации. При этом PID процесса-писателя содержится в расширении имени каждого лог-файла «*stracelog.pid*». 2.Дополнительную информацию о каждом процессе-писателе с указанным PID, можно получить из файла «*procname.txt»*, созданного на шаге 2.2. 3.Отредактировать каждый текстовый файл «*stracelog.pid*» таким образом, чтобы он содержал построчную информацию о файлах, в которые осуществлялась запись, в следующем виде:	Один или несколько «*stracelog.pid*» файлов, в которых построчно указаны: • полный путь к каждому файлу, предполагаемому для использования в качестве разделяемого; • имя этого файла.

№ п/п	Описание выполняемого действия	Ожидаемый результат
	<полный путь>/<имя файла>.	
3	*Выявление процессов (потоков) Изделия, осуществляющих чтение информации из выявленных ранее файлов*	
3.1	Собрать статистику по использованию операций чтения информации из ранее выявленных файлов с помощью утилиты «*inotifywatch*»: *inotifywatch -e access -z --fromfile stracelog.pid > watchLog.pid* которая собирает статистику за наблюдаемыми файлами, указанными в «*stracelog.pid»,* и записывает её в файл «*watchLog.pid*». Повторить запуск указанной выше утилиты для каждого файла «*stracelog.pid».* Полученные статистические данные следует использовать при экспертном анализе на шаге 3.3.	Один или несколько файлов «*watchLog.pid*», содержащих статистические данные по событию *«access»* для каждого из наблюдаемых файлов.
3.2	Регистрация событий, связанных с чтением ранее записанной информации. Для каждого файла «*stracelog.pid*», отредактированного на шаге 2.3, выполнить команду запуска утилиты «*Inotifywait»* в режиме ожидания событий: *inotifywait -e access -m -o inotiLog.pid --fromfile stracelog.pid* По этой команде в файл «*inotiLog.pid»* будут записываться события «*access*» (файл был прочитан), относящиеся к каждому отслеживаемому файлу из «*stracelog.pid»*.	Выдача сообщения: *Setting up watches.* *Watches established*. Выход из режима – CTRL+Z
3.3	Выполнить экспертный анализ результатов работы утилит «*Inotifywatch»* и «*Inotifywait»* на шаге 3.1-3.2 с целью составления списка файлов, которые могут быть использованы в качестве «разделяемых» ресурсов. Для этого необходимо сравнить PID процесса-читателя с PID процесса-писателя для каждого отслеживаемого файла.	Составлен список файлов, которые могут быть использованы в качестве «разделяемых» ресурсов
4	*Проверить соответствие уровней доступа процессов-писателей уровням доступа процессов-читателей*	
4.1	Исследовать процессы (потоки), осуществляющие информационное взаимодействие (связь по информации) с использованием разделяемых ресурсов. С этой целью применять все возможные и необходимые дополнительные инструментальные средства и команды среды функционирования (в частности, команду PS), документацию на ПО, позволяющие получить достаточно полную информацию о каждом выявленном разделяемом файле и соответствующих процессах (потоках).	Составлен список разделяемых ресурсов и соответствующих им процессов (потоков) в виде таблицы
5	*Сделать выводы о наличии/отсутствии скрытых каналов в исследуемом ПО, основанных на использовании разделяемых ресурсов*	
5.1	Анализ информации, полученной на предыдущих шагах о процессах (потоках) и разделяемых ими ресурсах. Сделать выводы о «легитимном» или «нелегитимном» использовании «разделяемых» ресурсов. При наличии операции чтения ранее записанной информации менее доверенным процессом (потоком) зафиксировать возможность скрытой передачи информации (наличие скрытого канала)	Выводы о наличии/отсутствии скрытых каналов, основанных на использовании разделяемых ресурсов

ТАБЛИЦА 4. Перечень протоколов, используемых в коммуникационных каналах связи ИФБО и ИФО

№ п/п	Название	Протокол	Влияние на ФБО
1.	ИФО 1	Syslog	Не влияет на ФБО
2.	ИФО 2	SNMP	Не влияет на ФБО
3.	ИФО 3	WMI/RPC	Не влияет на ФБО
4.	ИФО 4	OPSEC LEA	Не влияет на ФБО
5.	ИФО 5	ODBC API	Не влияет на ФБО
6.	ИФО 6	HTTP/HTTPS	Не влияет на ФБО
7.	ИФО 7	NFS/SMB	Не влияет на ФБО
8.	ИФО 8	SSH	Не влияет на ФБО
9.	ИФБО 1	HTTPS	Влияет на ФБО
10.	ИФБО 2	SMTP	Влияет на ФБО

2) С помощью ПО Wireshark в ходе проведения функционального тестирования, проводимого согласно документу Программа и методика испытаний снять дамп сетевого трафика, передаваемого через все физические сетевые интерфейсы ОО.

3) Проанализировать сохраненный дамп сетевого трафика.

По результатам анализа установлено, что в ходе испытаний объект оценки не выполнял попыток несанкционированных сетевых подключений к сторонним сервисам. При передаче сетевого трафика данные направлялись в соответствии с параметрами инкапсуляции. На сетевых интерфейсах СВТ, являющихся средой функционирования ОО отсутствовали сетевые пакеты, адресованные сторонним получателям. Все сетевые потоки генерировались в рамках установленных соединений. По протоколам, использующим инкапсуляцию (HTTPS, SMB, SSH, NFS, OPSEC LEA) защищаемая информация в открытом виде не передавалась, по протоколам, не использующим инкапсуляцию, в открытом виде передавались только журналы событий безопасности ОО (от ОО на указанный в конфигурации сервер Syslog) и события безопасности внешних источников (от внешних источников на ОО). Все информационные потоки генерируется ИФБО и ИФО и соответствуют проектной и технической документации на ОО.

В ходе тестирования и анализа его результатов не было выявлено скрытых каналов передачи информации, при выполнении указаний по эксплуатации ОО. ОО не генерирует побочных сетевых пакетов незапланированного в ходе испытаний информационного обмена.

Список используемых источников

1. Штеренберг С. И., Андрианов В. И. Исследование методики адаптивных атак на основе скрытого вложения в исполнимые файлы // в сб.: Наука, Техника, Инновации

2014 сб. ст.й Международной научно-технической конференции. Под общей редакцией А. Л. Сафонова. 2014. С. 287–294.

2. Коцыняк М. А., Лаута О. С., Нечепуренко А. П., Штеренберг И. Г. Методика оценки устойчивости информационно-телекоммуникационной сети в условиях информационного воздействия. // Труды учебных заведений связи. 2016. Т. 2. № 4. С. 82–87.

3. Закалкин П. В., Сагдеев А. К., Стародубцев Ю. И., Сухорукова Е. В. Проблема формирования системы динамической защиты государственных информационных систем // Актуальные проблемы инфотелекоммуникаций в науке и образовании. V Международной научно-технической и научно-методической конференции сб. науч. ст. в 3 т. СПб.: СПбГУТ, 2016. С. 239–243.

4. Анисимов В. В., Величко В. М., Чукариков А. Г. Постановка задачи на обеспечение превентивной защиты ИТКС СН // Актуальные проблемы инфотелекоммуникаций в науке и образовании. V Международной научно-технической и научно-методической конференции: сб. науч. ст. в 3 т. СПб.: СПбГУТ, 2016. С. 91–95.

5. Красов А. В., Штеренберг С. И., Москальчук А. И. Методология создания виртуальной лаборатории для тестирования безопасности распределенных информационных систем // Вестник Брянского государственного технического университета. 2020. № 3 (88). С. 38–46.

6. Штеренберг С. И., Штеренберг И. Г. Вероятностные методы построения элементов самообучения адаптивных информационных систем // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2016. № 1. С. 53–56.

7. Казаков В. В., Кравцов А. Н., Самойлов Е. Б. Методы обработки и анализа телеметрической информации при управлении космическими средствами: курс лекций. СПб.: ВКА имени А. Ф. Можайского, 2011. 152 с.

УДК 004.6
ГРНТИ 20.53.17

РАЗРАБОТКА МНОГОФУНКЦИОНАЛЬНОЙ ПЛАТФОРМЫ УЧЁТА ПРОИЗВЕДЕНИЙ ИСКУССТВА С ПРИМЕНЕНИЕМ ТЕХНОЛОГИИ РАСПРЕДЕЛЕННЫХ РЕЕСТРОВ

Н. С. Минеев, А. В. Помогалова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Настоящий проект направлен на создание платформы, которая позволяет как безопасно проводить финансовые операции с предметами искусства, так и вести учёт арт-объектов. С помощью технологии блокчейн, которая является разновидностью распределенного реестра, пользователь может быть уверен в том, что за его организацией закреплены определенные объекты искусства за счёт сертификата подлинно-

сти для физических арт-объектов, а также записи в самом блокчейне. С помощью записи в блокчейне все пользователи могут отследить описание объекта искусства, историю владельцев с момента первой регистрации на платформе, автора произведения искусства, а также текущую стоимость произведения искусства.

Для реализации проекта используется блокчейн Ethereum ввиду возможности создавать смарт-контракты внутри самого блокчейна, что позволяет безопасно проводить операции, связанные с объектами искусства, а также большого сообщества разработчиков, которое предоставляет множество различных инструментов для разработки и тестирования смарт-контрактов на базе блокчейна Ethereum, а также их внедрения в структуру клиент-серверного приложения.

блокчейн-сеть, блокчейн, распределенный реестр, хранение данных, авторское право, интеллектуальная собственность.

На сегодняшний момент остро стоит проблема с безопасным хранением данных, а также доступом к этим данным. Несмотря на распространенность различных баз данных и систем безопасных взаимодействий с ними, довольно нередки случаи несанкционированного доступа, что приводит как к утечкам персональных данных, так и к подмене/удалению данных, что непосредственно влияет на доверие к таким системам, а также использования их в качестве средств подтверждения авторского права.

Текущий разрабатываемый проект представляет из себя многофункциональную платформу, которая позволяет хранить авторскую информацию о предметах искусства. За счёт использования технологии распределённых реестров, в нашем случае блокчейн-сети, возможно достичь защищенного хранения данных о произведениях искусства и организациях-держателях. Это происходит благодаря неизменяемость и невозможности подмены зафиксированной в блокчейн-сети информации, а также децентрализованного хранения данных, то есть копия реестра хранится у каждого узла блокчейн-сети [1, 2].

Актуальность разрабатываемого проекта состоит в следующем:

- Необходимость обеспечения защиты финансовых сделок между пользователями;
- Необходимость защищённого и децентрализованного хранения пользовательских данных;
- Учёт предмета искусства от разных организаций на одной платформе
  - Текущая стоимость предмета искусства;
  - Текущее расположение предмета искусства;
  - Текущий владелец предмета искусства;
  - Предыдущие владельцы предмета искусства.
- Возможность просматривать информацию о предметах искусства.

Цель проекта состоит в следующем: разработать многофункциональную платформу, которая позволяет каждой организации безопасно вести

учёт своих предметов искусства, при этом проводить сделки покупки/продажи/аренды предметов искусства между другими организациями.

Для выполнений поставленной цели необходимо выполнить следующие задачи:

- Разработать смарт-контракты, то есть программы внутри самой блокчейн-сети, которые будут выполнять роли следующих сущностей:
  - Пользователь;
  - Организация;
  - Предмет искусства.
- Разработать систему аутентификации и авторизации пользователя через блокчейн-сеть;
- Разработать систему учёта и подтверждения подлинности объектов искусства;
  - Система учёта должна включать в себя следующие вещи:
    - Создание предмета искусства как отдельного смарт-контракта в блокчейн-сети;
    - Взаимодействие со смарт-контрактами предметов искусства, в том числе получение информации о каждом отдельном объекте.
  - Также каждая организация должна подтвердить, что созданный арт-объект в блокчейн-сети действительно принадлежит ей.
    - Для этого организация должна предоставить сертификат подлинности и дождаться обработки и подтверждения этого документа.
- Разработать систему продажи и аренды объектов искусства, чтобы организации могли обмениваться между собой предметами искусства без необходимости связываться через сторонние сервисы.

Также стоит учесть, что хоть система и делает учёт предметов искусства, однако позволяет переквалифицироваться в полноценную платформу учёта авторского права на различную интеллектуальную собственность.

На рис. 1 указана текущая архитектура смарт-контрактов, необходимая функциональность которых была указана ранее.

Рис. 1. Архитектура смарт-контрактов

На текущий момент были выполнены следующие задачи:

- Разработаны смарт-контракты для каждой ранее указанной сущности;
- Разработана система аутентификации и авторизации пользователя через блокчейн-сеть;
- Частично разработана система учёта предметов искусства;
  - Сейчас возможно отслеживать текущего владельца предмета искусства, а также текущие стоимости аренды и покупки арт-объекта.
- Реализована галерея объектов искусства для всех авторизированных и неавторизированных пользователей на основной странице платформы.

На рис. 2 представлены результаты проведенного исследования и разработки – полноценная функционирующая платформа на базе блокчейн-сети Ethereum.

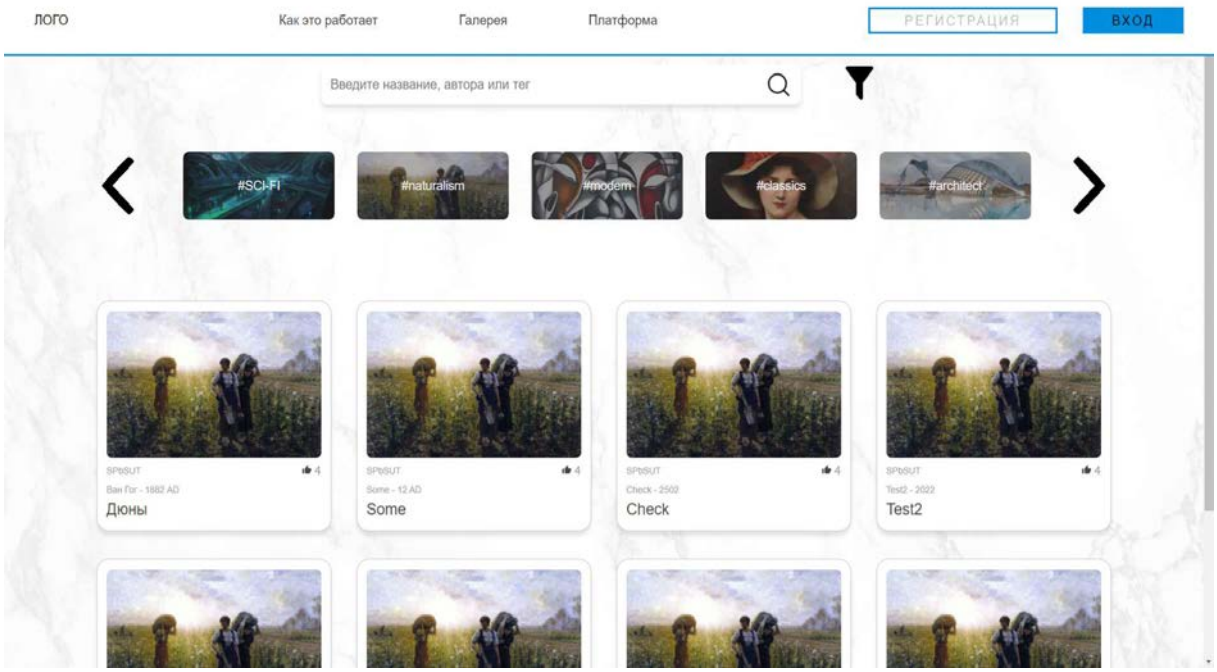


Рис. 2. Разработанная платформа

Платформа базируется на блокчейн-сети *Ethereum*, что позволяет использовать разработанные сообществом различные программные решения, а также разрабатывать собственные смарт-контракты. Благодаря библиотеки ethers.js, которая разработана для языка программирования JavaScript и базируется на библиотеке web3.js, было реализовано взаимодействие разработанного программного решения с ранее упомянутой блокчейн-сетью как для получения данных, так и для внесения новых [2–4].

В конечном итоге была разработана платформа по учёту предметов искусства для различных организаций. Большая часть задач, которые указаны

ранее в настоящей статье, была выполнена, однако в будущих версиях программного обеспечения планируется доработка существующих и создание новых систем платформы.

Список используемых источников

1. Елагин В. С., Спиркина А. В., Владыко А. Г., Иванов Е. И., Помогалова А. В., Аптриева Е. А. Основные сетевые характеристики blockchain трафика и подходы к моделированию // T-Comm: Телекоммуникации и транспорт. 2020. Том 14. № 4. С. 39–45.

2. Осваиваем Ethereum : создание смарт-контрактов и децентрализованных приложений / Андреас Антонопулос, Гэвин Вуд ; [перевод с английского М. А. Райтман, А. В. Власова]. Москва : Эксмо, 2021. 512 с.

3. Руководство по языку программирования Solidity : официальный сайт. URL: docs.soliditylang.org (дата обращения: 01.09.2021).

4. Руководство по библиотеке ethers.js : официальный сайт. URL: docs.ethers.io (дата обращения: 01.09.2021).

Статья представлена
директором НИИ «Технологии связи», доцентом кафедры ИКС СПбГУТ,
кандидатом технических наук, доцентом В. С. Елагиным.

УДК 004.056
ГРНТИ 49.33.35

АНАЛИЗ ПРОЦЕССОВ БЕЗОПАСНОЙ РАЗРАБОТКИ DEVSECOPS

А. А. Миняев, Е. А. Паршин

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В публикации затрагивается тема безопасной разработки DevSecOps. Рассмотрены преимущества данного процесса, необходимые требования для успешного внедрения. Помимо всего было выяснено зачем следует автоматизировать безопасность, какие могут быть проблемы при неопытном или неправильном использовании. Можно ли успешно внедрить DevSecOps без определенного опыта. Мы обнаружили, что многие понимают DevSecOps как интеграцию тестирования и практики безопасности в методологию разработки DevOps. Каждый ли должен нести ответственность за обеспечение безопасности? Что и с помочью чего необходимо автоматизировать в безопасной разработке? Автор постарался ответь на все вопросы и на основе этого сделать соответствующие выводы.

DevSecOps, информационная безопасность, безопасная разработка, DevOps.

Это исследование проводится, чтобы понять, что означает DevSecOps, и выяснить, могут ли команды без опыта в области безопасности успешно внедрить эту практику, а также преимущества и проблемы, с которыми могут столкнуться такие команды. Чтобы четко обозначить цель статьи, были сформулированы вопросы исследования:

1) Зачем следует автоматизировать безопасность.
2) Какие преимущества DevSecOps.
3) Что не следует автоматизировать.
4) Необходим ли опыт для успешного внедрения безопасности в процессы DevOps.
5) С какими проблемами можно столкнуться при внедрении безопасности в процессы DevOps.

Для начала необходимо обозначить DevSecOps – это гибкая практика соответствия требованиям, которая интегрирует безопасность в жизненные циклы разработки программного обеспечения и ИТ-операций. В DevOps встроены возможности SecDev и SecOps, что обеспечивает комплексный подход к обеспечению безопасности при доставке программного обеспечения и систем. DevSecOps находится в центре DevOps, SecDev и SecOps (рис.), поскольку он должен обеспечивать надлежащий баланс для каждого действия. Безопасность должна быть «встроена», а не «приделана», механизм должен работать как единый организм [1].

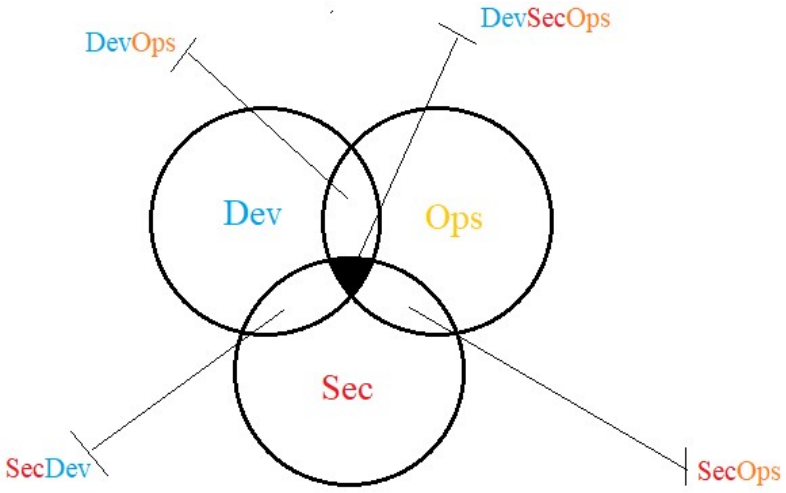


Рисунок. Графическая визуализация состава DevSecOps

Практика DevSecOps основана на пяти принципах для успешного внедрения безопасности в жизненный цикл разработки:

•Культура DevSecOps поощряет совместную ответственность за безопасность и сотрудничество между командой разработки, безопасности и эксплуатации. Каждый отдел должен интегрировать безопасность в свою работу, а это означает, что специалисты по безопасности должны привле-

каться к работе с самого начала проекта. DevSecOps предполагает включение и совместную работу в команде и стремится устранить традиционную практику обособленности [2].

•DevSecOps фокусируется на 100 % автоматизации элементов управления и процессов безопасности таким образом, чтобы не снижать скорость и гибкость. Действия по тестированию программного обеспечения выполняются автоматически с использованием инструментов тестирования, чтобы делать то, что тестировщик-человек делает вручную. И речь идет не только о тестировании и развертывании, это также включает в себя управление релизами, управление конфигурацией, мониторинг. Однако автоматизация тестирования не может устранить или полностью заменить ручное тестирование, поскольку невозможно автоматизировать все тестовые случаи. В некоторых случаях ручные проверки жизненно важны, поскольку определенные ошибки или проблемы, такие как аутентификация и авторизация, невозможно обнаружить с помощью инструментов автоматического тестирования.

•DevSecOps поощряет использование командами мониторинга и метрик для измерения уязвимостей и угроз, что важно для ведения учета производительности и повышения качества программного обеспечения. Все, что имеет значение, должно быть измерено, команды не смогут улучшить свой продукт, если измерения не учитываются.

•DevSecOps поддерживает обмен знаниями между всеми командами с целью интеграции безопасности в каждый процесс. Это обучение и перекрестное обучение каждого члена группы разработки, эксплуатации и безопасности своим обязанностям в области безопасности. Процессы безопасности можно улучшить только тогда, когда команды постоянно делятся проблемами, с которыми они сталкиваются, и тем, как они могут помочь друг другу.

Для дальнейшей работы попробуем разобраться что же нельзя автоматизировать и какие типы тестирования безопасности существуют в DevSecOps. Решение о том, что и когда автоматизировать в тестирование программного обеспечения, важно, поскольку неправильное решение может привести к неприятным последствиям, если автоматизация применяется с неправильными инструментами и подходами. Однако, что и когда автоматизировать, зависит от проекта и технологий. Согласно исследованиям, выделяют пять факторов, влияющих на то, что не следует автоматизировать при тестировании программного обеспечения, сюда входит [3]:

- испытываемое программное обеспечение,
- факторы, относящиеся к тестовому сценарию,
- факторы, относящиеся к тестовым инструментам,
- человеческие и организационные факторы,
- межотраслевой фактор.

Помимо всего есть тесты безопасности, которые необходимо включить в DevSecOps, чтобы помочь выявить уязвимости в программном обеспечении, и все эти тесты требуют хороших навыков и знаний в области безопасности.

- Статическое тестирование безопасности приложений (SAST).
- Динамическое тестирование безопасности приложений (DAST).
- Сканирование на наличие уязвимостей методом черного ящика.
- Выявление распространенных уязвимостей с точки зрения злоумышленника.
- Управление конфигурацией и соблюдение требованиям безопасности.
- Грамотная настройка приложений и соблюдение политик безопасности.
- Написанные сценариев, которые будут запускаться автоматически для запуска тестирования и безопасного развертывания без ошибок согласованным образом
- Непрерывный мониторинг.

Рассмотрим инструменты DevSecOps:

- Jenkins предоставляет простой и легкий способ к среде непрерывной доставки (CD) и непрерывной интеграции (CI) практически для любого сочетания языков. Jenkins [4] достигает непрерывной интеграции с помощью плагинов. Это позволяет интегрировать различные этапы DevOps.
- SonarQube – это инструмент, который упрощает интеграцию результатов или статистики в конвейер сборки. Он используется для непрерывной проверки качества кода и руководства разработчиками при проверке кода.
- Проверка зависимостей OWASP – это инструмент, который распознает зависимости проекта и определяет наличие уязвимостей любого типа. Этот плагин может независимо выполнять исследование Dependency Check и наблюдать за результатами.
- Docker – это утилита, используемая для сборки, развертывания и запуска проекта через контейнеры. Это виртуальная машина, но она не похожа на виртуальные машины, на которых построена совершенно отдельная операционная система. Это позволяет программам использовать ядро Linux той самой машины, на которой оно установлено, и, пользуясь этим преимуществом, может привести к тому, что программы будут готовы к отправке на другие машины, которые работают под той же ОС Linux с разными конфигурациями.

К безопасности нужно относиться серьезно, чтобы избежать потенциальных судебных исков и штрафов, надежная безопасность начинается с разработки программного обеспечения [5].

Рассмотрим ряд преимуществ процессов DevSecOps:

•Автоматизация безопасности: ручное тестирование безопасности не соответствует скорости DevOps. Безопасность должна постоянно участвовать в каждом этапе и автоматически запускать тесты, чтобы не отставать от изменений. Автоматизация безопасности позволяет расширить рабочую нагрузку и область действия, ускорить контроль и сделать возможным обнаружение ошибок и создание отчетов.

•Инструменты статического анализа: это одна из вещей, которые помогают проверить на безопасность заранее, поскольку их можно запускать с кодами раньше, прежде чем развертывать в среде. Однако не многие организации обладают опытом, позволяющим наилучшим образом использовать эти инструменты [6].

•Стоимость: безопасность с самого начала проекта позволит командам быстрее находить ошибки и исправлять их. Многие считали, что попытка исправить ошибки в производстве может стоить целое состояние. В случае кибератаки предприятия могут столкнуться с финансовыми санкциями из-за компрометации дыры в безопасности или несоблюдения некоторых правил [6].

Согласно исследованиям, внедрение безопасного DevOps означает, что команды должны развивать опыт и процессы для обнаружения угроз и рисков, и защиты от них [7]. Многие убеждены, что моделирование угроз и оценка рисков являются важной практикой DevSecOps, требующей знаний и навыков. Моделирование угроз – это метод, который необходимо использовать для защиты приложений и API, поскольку он позволяет командам выявлять и определять приоритеты возможных угроз, которые могут использовать злоумышленники. Применение неправильных стандартов и элементов управления является распространенной ошибкой в организациях, команды должны знать язык, структуру и другие технологии, чтобы правильно настроить правила тестирования безопасности. Надлежащее сотрудничество и понимание методов обеспечения безопасности должны быть распространены между командами с полным изменением отношения людей к безопасности для успешной адаптации DevSecOps [7].

В ходе работы был выявлен ряд проблем в адаптации процесса:

Обеспечить безопасность разработки непросто из-за сложности программного обеспечения. Внедрение DevSecOps означает, что организации должны принять изменения, а барьеры между командами безопасности, командой разработки и эксплуатации должны быть устранены.

Методы безопасности в DevOps должны быть гибкими, и эти методы должны быть понятны и приняты всеми командами. Для создания безопасности в процессе DevOps требуются навыки и обучение персонала.

Получение правильных инструментов и правильных конфигураций жизненно важно для поиска ошибок и других проблем[5]. Понимание возможностей и ограничений этих инструментов является серьезной проблемой для команд.

На какие тезисы необходимо обратить внимание при внедрении безопасной разработки?

- Разработка программы требует четко сформулированных общих целей и комплексного спонсорства со стороны руководства.
- Инструментарий безопасности и инфраструктуры должен быть интегрирован так, чтобы соответствовать ожиданиям по пропускной способности.
- Требуется постоянное командное обучение для обеспечения технической и ситуационной готовности.
- Управление и соблюдение нормативных требований требуют реструктуризации для поддержки гибкости системы безопасности.

Вывод

В этой статье мы исследовали, что означает DevSecOps, и могут ли организационные группы без знаний или опыта в области безопасности успешно внедрить DevSecOps. Мы также определили ключевые принципы, которых должны придерживаться команды, преимущества успешного внедрения и некоторые проблемы DevSecOps. Мы обнаружили, что многие понимают DevSecOps как интеграцию тестирования и практики безопасности в методологию разработки DevOps и что каждый должен нести ответственность за обеспечение безопасности. Изучив некоторую литературу, стало ясно, что для реализации безопасности необходимы опыт и хорошее понимание безопасности, и эти знания должны быть распространены среди членов команд, чтобы избежать неграмотности в вопросах безопасности.

Список используемых источников

1. Состояние DevOps в России. URL: https://habr.com/ru/company/oleg-bunin/blog/524556/ (дата обращения: 20.11.2021)

2. Дэвис Дженнифер Философия DevOps. Искусство управления IT. СПб.: Питер, 2017. 416 с.

3. Утечки данных: ущерб и борьба российских компаний. URL: https://softline.ru/about/news/utechki-dannyih-uscherb-i-borba-rossiyskih-kompaniy (дата обращения: 21.11.2021).

4. What is Jenkins? The CI server explained. URL: https://www.infoworld.com/article/3239666/what-is-jenkins-the-ci-server-explained.html

5. Форсгрен Н., Хамбл Д., Ким Д. Ускоряйся! Наука DevOps : Как создавать и масштабировать высокопроизводительные цифровые организации / пер. с англ. А. Техненко. Москва : Интеллектуальная Литература, 2020. 216 с. ISBN 978-5-6042881-1-5.

6. Rangnau T, Buijtenen RV, Fransen F, Turkmen F. Continuous Security Testing: A Case Study on Integrating Dynamic Security Testing Tools in CI/CD Pipelines // Proceedings – 2020 IEEE 24th International Enterprise Distributed Object Computing Conference, EDOC 2020 2020. С 145–154. URL: https://doi.org/10.1109/edoc49727.2020.00026 (дата обращения: 20.01.2022).

7. Tony Hsu. Hands-On Security in DevOps. Ensure continuous security, deployment, and delivery with DevSecOps. Packt Publishing 2018. 356 p.

УДК 621.396.4
ГРНТИ 50.37.03

АНАЛИЗ БАЗОВЫХ ПРИНЦИПОВ И ТРЕБОВАНИЙ К ПОСТРОЕНИЮ ПОДСИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ В СОВРЕМЕННЫХ СИСТЕМАХ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

И. В. Морозов, И. Б. Паращук, В. А. Саяркин

Военная орденов Жукова и Ленина Краснознаменная академия связи
имени Маршала Советского Союза С. М. Буденного

Проведен анализ требований к построению подсистем защиты информации для современных систем электронного документооборота. Сформулированы общеметодологические принципы построения и функционирования подсистем такого класса. Эти результаты призваны помочь при разработке и технической реализации высокоэффективных средств и комплексов, нацеленных на оперативное и качественное решения задач, возлагаемых на подсистему защиты информации для современных систем обработки электронных документов.

подсистема защиты информации, система электронного документооборота, электронный документ, принципы, требования, ресурсы, пользователь, система.

Эволюция современного информационного общества невозможна без инновационных решений и, зачастую, революционных шагов в рамках совершенствования IT-инфраструктуры. При этом различные грани совершенствования IT-инфраструктуры отражают как эволюционные процессы в информационном пространстве страны, так и частные процессы развития инфокоммуникаций в экономике, здравоохранении и в других областях деятельности, включая оборонную сферу. Важным компонентом, влияющим не только на масштабы (диапазон) предоставляемых современной IT-инфраструктурой услуг пользователям, но и в целом, на качество (и эффек-

тивность) ее функционирования, с учетом традиционных показателей своевременности, достоверности и безопасности, являются системы электронного документооборота (СЭД), получившие широкое распространение в последние годы как в мировой, так и отечественной практике телекоммуникаций [1–3]. При этом считается, что СЭД является организационно-техническим объектом, предназначенным для обеспечения процессов порождения (генерации, производства) электронных документов (ЭД), для их передачи и приема (распределения между пользователями и исполнителями), для контроля доступа к ним в сетях учреждений и организаций, а также для обеспечения оперативного управление трафиком ЭД, т. е., их потоками документов в подобных инфраструктурах [1, 2, 4].

Рынок средств и технологий СЭД стремительно развивается, но особую озабоченность у разработчиков, администраторов и пользователей на современном этапе вызывают вопросы, связанные с отысканием новых эффективных организационных и технологических (аппаратных и программных) решений по защите информации, циркулирующей и хранящейся в СЭД [2, 5].

Каждый из администраторов и пользователей, кто с юридической точки зрения является лицом (субъектом) информационных отношений при реализации процедур электронного документооборота, является, априори, слабо защищенным, легкоуязвимым перед лицом современных угроз информационной безопасности. Эти администраторы и пользователи СЭД, безусловно, потенциально подвержены нанесению им материального либо морального, прямого либо опосредованного ущерба, реализуемого либо посредством воздействия на критичную для них информацию и ее носители, либо путем нелегитимного использования (противоправного оборота) такой информации.

Вследствие этого у всех лиц (субъектов), участвующих в информационных отношениях при реализации процедур электронного документооборота, особый интерес вызывают практические вопросы обеспечения информационной безопасности. Для реализации легитимных полномочий и интересов таких лиц (субъектов), для гарантирования их информационной безопасности, очень важно постоянно поддерживать высокую степень реального обеспечения заданных требований с точки зрения характеристик защищенности, как самой информации, так и систем ее обработки в рамках СЭД. Притом весьма важно не утратить такие атрибуты защищенности информации, как целостность (невредимость, неискаженность), временная и топологическая доступность, а также конфиденциальность (неразглашение, доверительность) информации [6, 7].

Так как вред лицам (субъектам), участвующим в информационных отношениях при реализации процедур электронного документооборота, может быть нанесен не только напрямую, но и опосредованно, путем воздействия на саму информацию и ее носители, то вполне обоснованно

обнаруживается интерес таких лиц (субъектов) в обеспечении защищенности как самих электронных документов (ЭД), так и подсистем их обработки.

Другими словами, сама информация (контент, т. е., ЭД), процедуры ее обработки, а также ее носители, могут и должны рассматриваться в качестве объектов СЭД, нуждающихся и подлежащих безусловной защите.

Рассмотрим требования к СЭД, использующим методы и средства обеспечения защищенности ЭД от искажения, извращения и деформации (ущерб целостности), от утраты, потери или понижения уровня временной либо топологической доступности информации, противоправного тиражирования (ущерб доступности), а также от неоправданного и незаконного их оглашения (ущерб конфиденциальности).

Подсистема защиты информации (ПЗИ) СЭД представляет собой взаимоувязанную по целям, времени и месту организационно-техническую совокупность алгоритмов, средств и специальных процедур, запроектированных и реализованных в СЭД для решения определенных задач обеспечения безопасности ЭД.

Краеугольным требованием к ПЗИ принято считать требование по способности данных подсистем к адаптации. Под этим понимается способность подсистем такого класса к адресному, целевому приспособлению своей структуры и поведения к внешним условиям и вводимым управлениям при изменении параметров, режимов и условий функционирования СЭД. Особая значимость способности ПЗИ к адаптации предопределяется, во-первых, тем, что обстоятельства, влияющие на защищенность СЭД, имеют тенденцию неожиданно (и, зачастую, кардинально) изменяться, во-вторых, тем, что ключевые технологические процедуры обеспечения безопасности ЭД традиционно реализуются в условиях неопределенности параметров среды, неполноты и нечеткости исходных данных [8].

Вдобавок к требованию, определяющему способность ПЗИ к адаптации, принято формулировать ряд более предметных, установочных требований, которые условно подразделяются на технические, организационные, функциональные, эргономические и экономические требования.

Помимо формирования базовых требований, важное значение имеет формулировка общеметодологических принципов разработки и эксплуатации ПЗИ для СЭД. Перечень таких принципов разработки и эксплуатации ПЗИ для СЭД, на наш взгляд, должен включать:

– тотальность (исчерпывающая достаточность) контроля безопасности в СЭД – все процессы электронного документооборота должны контролироваться подсистемой защиты в полном, исчерпывающем объеме, при этом общие и частные параметры контроля должны фиксироваться в специализированных регистрационных журналах;

– концептуальная цельность (согласованность, единство) – структура, технологические схемы, организация и обеспечение функционирования как

ПЗИ для СЭД в целом, так и ее элементов, должны анализироваться, рассматриваться и реализовываться комплексно и в строгом соответствии с основными положениями единой концепции защиты информации;

– соответствие ключевым требованиям – подсистема защиты информации для СЭД должна создаваться как адекватная система, в строгом соответствии с ключевыми требованиями к защите;

– опциональная (функциональная) самодостаточность – ПЗИ для СЭД создается и функционирует как самостоятельная вспомогательная подсистема СЭД и при реализации опций (функций) защиты ЭД не зависит от других подсистем;

– комфортность и практичность использования – подсистема защиты информации для СЭД не только должна быть удобной, но и не должна создавать дополнительного дискомфорта для пользователей и персонала СЭД;

– максимальное уменьшение предоставляемых прав – каждому пользователю СЭД и каждому лицу из состава персонала ПЗИ СЭД должны представляться лишь те минимальные полномочия на доступ к ЭД, без которых выполнение ими своих обязанностей невозможно или крайне затруднено;

– минимизация затрат на создание и функционирование ПЗИ для СЭД – при условии соблюдения иных принципов и при условии выполнения всех рассмотренных требований, финансовые, временные, энергетические, вычислительные и людские затраты (расходы) на такую подсистему должны быть экономными;

– инициативность и энергичность реагирования на нарушения – подсистема защиты информации для СЭД должна немедленно и активно реагировать на любые попытки несанкционированных действий.

Таким образом, рассмотрены требования к построению подсистем защиты информации для современных систем электронного документооборота. Сформулированы общеметодологические принципы создания и функционирования подсистем такого класса. Предполагается, что следование данным принципам и выполнение сформулированных требований позволит осуществить разработку и техническую реализацию высокоэффективных средств и комплексов, нацеленных на оперативное и качественное решения основных задач, возложенных на подсистему защиты информации для современных систем автоматизированной обработки электронных документов.

Список используемых источников

1. Постановление Правительства РФ от 22 сентября 2009 г. № 754 «Об утверждении Положения о системе межведомственного электронного документооборота».

2. Куняев Н. Н., Демушкин А. С., Фабричнов А. Г. Конфиденциальное делопроизводство и защищенный электронный документооборот. Москва : Логос, 2011. 452 с.

3. Чернов В. Н. Системы электронного документооборота. Москва: РАГС, 2009. 84 с.

4. Национальный стандарт Российской Федерации ГОСТ Р ИСО 30300-2015 СИБИД. Информация и документация. Системы управления документами. Основные положения и словарь Москва : Стандартинформ, 2015. 18 с.

5. Коржук В. М., Попов И. Ю., Воробьева А. А., Защищенный документооборот. Часть 1: Учебно-методическое пособие. СПб. : Университет ИТМО, 2021. 67 с.

6. Булдакова Т. И., Глазунов Б. В., Ляпина Н. С. Оценка эффективности защиты систем электронного документооборота // Доклады Томского государственного университета систем управления и радиоэлектроники. 2012. № 1 (25), Ч. 2, С. 52–56.

7. Десницкий В. А., Паращук И. Б. Анализ и обеспечение защищенности данных пользователей беспроводных сенсорных сетей: показатели доступности, целостности и конфиденциальности // Региональная информатика и информационная безопасность. Сб. тр. Выпуск 7 / СПОИСУ. СПб., 2019. С. 34–38.

8. Федорченко Е. В., Паращук И. Б. Подходы к устранению неопределенности входной информации безопасности в задачах анализа защищенности систем индустриального Интернета вещей // Информационная безопасность регионов России (ИБРР-2021) XII-я Санкт-Петербургская Межрегиональная конференция. Санкт-Петербург, 27–29 октября 2021 г., Материалы конференции. СПб.: СПОИСУ, 2021. С. 100–102.

УДК 04.007.3
ГРНТИ 19.65.45

ВОЗМОЖНОСТИ ИСПОЛЬЗОВАНИЯ СЕТЕЙ ПЯТОГО ПОКОЛЕНИЯ В ДИАПАЗОНЕ МИЛЛИМЕТРОВЫХ ВОЛНАХ, ДЛЯ РАБОТЫ IoT

А. С. А. Мутханна, Е. Д. Никитин

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Сети связи пятого поколения разрабатывались с учетом трех основных задач – это увеличение пропускной способности, уменьшение задержек и поддержка надежного соединения. Для решения этих задач в 2019 году 3GPP был разработан набор спецификаций для NR, одной из наиболее важных разработок стала возможность использования технологии в диапазонах миллиметровых волн. Но стоит отметить тот факт, что вопрос о реализации приложений Интернета вещей все еще находится в стадии исследования. В данной статье будет исследована возможность работы таких устройств в диапазонах миллиметровых волн.

сети пятого поколения, диапазон миллиметровых волн, IoT.

Введение

Сети пятого поколения гарантируют очень высокую скорость передачи данных, сверхнизкую задержку и увеличение энергоэффективности по сравнению с предыдущими поколениями беспроводных сетей. Чтобы соответствовать этим требованиям, консорциум 3GPP выпустил набор спецификаций для NR [1], которые включают, помимо измененного радиодоступа и основной сети, поддержку связи в диапазоне миллиметровых волн. С одной стороны, огромное количество доступного спектра в диапазонах миллиметровых волн позволяет достичь скоростей передачи в несколько Гбит/с, а также повысить безопасность и конфиденциальность благодаря направленной передаче [2]. Однако, использование данного диапазона является сложной задачей для устройств среднего рынка Интернета вещей, которые ограничены по габаритам, стоимости, сложности и энергоэффективности.

Для решения вышеуказанных задач необходимо расширить спецификации NR для поддержки более простой версии NR, которую обычно называют NR-Light. Она должна удовлетворять требованиям более высокой скорости передачи данных, повышенной надежности и меньшей задержки, чем текущие технологии для услуг IoT, при этом гарантируя уменьшение стоимости, более длительный срок службы батареи, а также широкое покрытие. Новый радио интерфейс 5G является предметом в Release 17 [3], который, среди прочего, рассматривает возможность работы пользователей NR-Light в диапазонах миллиметровых волн для улучшения производительности сети. Однако, несмотря на привлекательность для частных сетей, например, для поддержки приложений недорогих устройств в промышленной сфере, прямое применение данного диапазона в IoT-подобных случаях использования ставит множество проблем, включая то, как удовлетворить требования к низкой стоимости/низкому энергопотреблению устройств NR-Light, обеспечивая при этом достаточный уровень производительности.

1. 3GPP NR-Light в диапазонах ММВБ

Предполагается, что NR-Light будет поддерживать работу сети как в FR1 (между 410 МГц и 7125 МГц), так и в FR2 (между 24,25 и 52,6 ГГц, т. е. в нижней части спектра мм-волн) [3].

A. Работа на миллиметровых волнах

Несмотря на неоспоримый потенциал, связь на миллиметровых волнах создает новые проблемы для всего стека протоколов [2].

Во-первых, потеря мощности сигнала в свободном пространстве пропорциональна квадрату частоты и расстоянию между передатчиком и приемником. Таким образом, сильное затухание, наблюдаемое на мм-волнах,

обычно не позволяет устройствам поддерживать связь на большом расстоянии. Определенные диапазоны миллиметровой волны, например, около 22 и 60 ГГц, подвержены еще более сильному затуханию из-за водяного пара и молекул кислорода в воздухе. Более того, данный диапазон волн к дождю.

Во-вторых, сигналы плохо распространяются через большинство препятствий, включая стены и окна. Как следствие, обеспечение равномерного покрытия является сложной задачей, а достижение «бесшовной» связи в закрытых помещениях с благодаря использованию наружных антенн невозможно. Люди также могут быть источником затухания: этот эффект в основном зависит от «формы» закрывающего тела и конфигурации антенны, и лишь слабо зависит от количества людей в среде. Для движущихся мобильных устройств эффект Доплера может привести к рассеиванию.

В-третьих, использование широкого спектра позволяет достичь скоростей передачи в несколько Гбит/с, которые для устройств среднего рынка, могут быть не нужны, но в свою очередь могут фактически ухудшить производительность сети.

B. Миллиметровые волны для возможного использования IoT

IoT характеризуют основные виды сценариев, а именно:

1. Дальность использования (порядка километров);

2. Использование трафика с низкими требованиями производительности;

3. Энергоемких архитектур и сетевых функций с низкой сложностью.

Учитывая вышеописанные ограничения, системы в миллиметровом диапазоне волн не могут быть использованы в данных сценариях.

В связи с этим, возникает логичный вопрос «Почему промышленные сообщества исследуют архитектуры NR-Light, работающие в миллиметровом диапазоне волн?» С одной стороны, предъявляют более высокие требования к скорости передачи данных, надежности и задержкам, чем текущие услуги IoT, для которых большая пропускная способность, доступная в миллиметровом диапазоне волн, является привлекательным вариантом. В то же время получение лицензии в миллиметровом диапазоне дешевле, по сравнению с более распространенными диапазонами 6 ГГц, что позволяет операторам использовать большие полосы частот. Кроме того, ограниченный диапазон распространения и невозможность проникновения через стены делают миллиметровый диапазон подходящими для реализации частных сетей.

2. Ключевые технологические факторы для NR-Light

Существующие устройства NR считаются слишком сложными, дорогими и энергоемкими для случаев использования, на которые нацелен NR-

Light. В следующем разделе демонстрируются возможные упрощения для NR-Light.

A. Упрощенная конструкция MIMO

Главной особенностью систем является реализация massive MIMO (m-MIMO) для преодоления серьезных потерь при распространении, наблюдаемые на высоких частотах. Однако архитектура m-MIMO требует использования нескольких аппаратных компонентов, что приводит к значительному потреблению энергии. В свою очередь, сценарии использования NR-Light, требуют низкого энергопотребления и меньшей сложности, поэтому упрощение радиостанции очень важный этап.

B. Недорогие аппаратные компоненты

Критическим свойством вышеописанных систем является фазовый шум, который приводит к случайным колебаниям фазы сигнала, что снижает достижимую спектральную эффективность. Эта проблема может быть решена путем использования высокоточных генераторов, которые дорого стоят, но способны производить несущий сигнал с низким уровнем шума. Однако это решение не может быть применено в устройствах NR-Light, поскольку их стоимость может оказаться слишком высокой. Более экономически эффективным решением является конфигурация опорных сигналов с фазовым отслеживанием (PTRS), специфичных для 5G-NR, для отслеживания и компенсации изменений фазового шума в пределах слота, а также принятие более высокого расстояния между поднесущими для избежания межнесущих помех.

Еще один перспективный аспект исследований – снижение стоимости физического оборудования NR-Light за счет облачной реализации сети радиодоступа (RAN), что позволяет реализовать функциональные возможности NR-Light с помощью программного обеспечения.

C. Снижение пропускной способности

Высокое энергопотребление радиостанций обусловлено их радиочастотными (РЧ) компонентами, потребляемая мощность которых линейно растет с увеличением пропускной способности системы. Устройства NR Release 15 поддерживают полосу пропускания до 400 МГц на несущую в FR2, которая может быть дополнительно увеличена с помощью агрегации несущих. В свою очередь, невысокие требования к сети в сценариях использования NR-Light теоретически позволяют уменьшить поддерживаемую полосу пропускания, тем самым минимизируя энергопотребление. Более того, уменьшение полосы пропускания позволяет использовать более дешевые АЦП, поскольку снижается требуемая частота дискретизации. Например,

уменьшение полосы пропускания с 200 до 50 МГц позволяет сэкономить до 23,5% стоимости радиомодуля [3]. По этим причинам 3GPP предусматривает полосу пропускания от 50 до 100 МГц для устройств NR- Light, работающих в диапазоне ммВолны.

D. Ослабление максимального порядка модуляции

Стандарт NR поддерживает эффективный механизм адаптивной модуляции и кодирования (AMC), который позволяет регулировать порядок модуляции и скорость кодирования, используемые передатчиком, в зависимости от качества канала.

E. Функциональные возможности энергосбережения

NR-Light может иметь различные схемы передачи данных по сравнению, например, с сотовыми сетями NR. Для сценария IoT обоснованно ожидать, что трафик будет характеризоваться короткими и регулярными передачами, например, для периодической перадачи данных датчиков, чередующимися с длительными периодами простоя. Поэтому система NR-Light должна определять слоты, в которых устройство должно прослушивать управляющие сообщения, и слоты, в которых устройство может простаивать [3].

Более того, NR-Light может унаследовать некоторые сетевые функции, которые были специально разработаны для недорогих сценариев IoT с низким энергопотреблением. В частности, NR-Light может реализовать механизм прерывистого приема (eDRX), режим энергосбережения (PSM) или сигналы пробуждения для оптимизации энергопотребления в режимах простоя и увеличения времени работы батареи. Кроме того, учитывая направленный характер связи, можно уменьшить допустимый уровень мощности передачи для устройств, которые находятся ближе к передатчику, что способствует уменьшению помех при увеличении времени работы батареи.

Выводы

Можно сделать выводы, что полноценная архитектура 5G NR, может не поддерживать среднерыночные варианты использования IoT, от видеонаблюдения до промышленной автоматизации, работает над новой (облегченной) версией NR, получившей название NR-Light, для поддержки требований к IoT, таких как высокая надежность, приемлемая задержка и пропускная способность, а также низкое энергопотребление.

Чтобы восполнить этот пробел, в данной статье мы сначала показали потенциал передачи данных в миллиметровом диапазоне волн для использования в IoT на среднем рынке. Далее были описаны требования для NR-Light, с ограниченной поддержкой полосы пропускания и более простых

конфигураций антенн. Можно сделать вывод, что уменьшение функций в радиоинтерфейсе сетей пятого поколения дает выигрыш в электропотреблении, при этом удовлетворяя требованиям приложений.

Список используемых источников

1. 3GPP, «Общее описание NR и NG-RAN» // TS 38.300, 2018.
2. Раппапорт Т. С. и др., "Мобильная связь на миллиметровых волнах для 5G сотовой связи: Это будет работать! // IEEE Access. 2013.vol. 1. pp. 335–349.
3. 3GPP, «Исследование по поддержке устройств NR с пониженными возможностями – выпуск 17» // TR 38.875, 2020.
4. Varsier, N., Dufre`ne, L.-A., Dumay, M., Lampin, Q., and Schwoerer, J., A 5G New Radio for Balanced and Mixed IoT Use Cases: Проблемы и ключевые факторы в диапазоне FR1 // IEEE Communications Magazine. May 2021. vol. 59, no. 4. pp. 82–87.
5. 3GPP, «Исследование связи для автоматизации в вертикальных областях (CAV) – выпуск 15» // TR 22.804, 2020.
6. Gundall M. et al., 5G as Enabler for Industry 4.0 Use Cases: Challenges and Concepts // in IEEE 23rd International Conference on Emerging Technologies and Factory Automation (ETFA), Turin, Italy, 2018.
7. Oyekanlu E. A. et al., A Review of Recent Advances in Automated Guided Vehicle Technologies: Интеграционные проблемы и области исследований для приложений умного производства на базе 5G // IEEE Access. 2020. Vol. 8. pp. 202 312–202 353.
8. Хаджадж С. С. Х. и М. Сахари К. С. Обзор сельскохозяйственной робототехники: Практичность и осуществимость // IEEE International Symposium on Robotics and Intelligent Sensors (IRIS). 2016.
9. Бородин А. С., Волков А. Н., Мутханна А. С. А., Кучерявый А. Е. Искусственный интеллект в сетях связи пятого и последующих поколений // Электросвязь. 2021. № 1. С. 17–22.
10. A Al-Ansi, AM Al-Ansi, A Muthanna, IA Elgendy, A Koucheryavy Survey on Intelligence Edge Computing in 6G: Characteristics, Challenges, Potential Use Cases, and Market Drivers Future Internet. 13 (5), 118.
11. Аббас В. Б., Гомес-Куба Ф. и Зорзи М. Эффективность приемника миллиметровых волн: Всестороннее сравнение схем формирования луча с АЦП низкого разрешения // IEEE Transactions on Wireless Communications. Oct. 2017. Vol. 16, no. 12. pp. 8131–8146,

УДК 004.72
ГРНТИ 49.38.99

НЕОБХОДИМОСТЬ ПЕРЕХОДА К ПОГРАНИЧНЫМ ВЫЧИСЛЕНИЯМ В ПРОМЫШЛЕННОМ ИНТЕРНЕТЕ ВЕЩЕЙ

А. С. А. Мутханна, А. А. Русаков

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В данной статье будут рассмотрены существующие концепты Промышленного интернета вещей и пограничных вычислений, а также преимущества внедрения пограничных вычислений в промышленный интернет вещей и возможную архитектуру сети, построенную с применением данного подхода.

промышленный интернет вещей, пограничные вычисления, туманные вычисления.

Введение

Промышленный Интернет Вещей (IIoT – *Industrial Internet of Things*) является одним из дальнейших развитий Интернета Вещей (IoT), которое подразумевает объединение промышленного оборудования через сеть передачи данных, получение, обмен и анализ данных, а также использование обработанной информации для оптимизации работы всей системы, тем самым увеличивая продуктивность и уменьшая затраты на обслуживание. Внедрение пограничных вычислений (Edge Computing) позволяет решить одну из главных задач сетей нового поколения, а именно – сокращение задержки передачи данных путем исключения сетевой составляющей круговой задержки. К тому же, использование пограничных вычислений позволяет разгрузить вышележащий канал, путем замыкания локального трафика, проведения части вычислений в пределах локальной сети и отправки только обработанной информации в «облако». Ещё одним немаловажным преимуществом является повышение безопасности сети, так как большая часть сигнальной информации будет циркулировать в пределах локальной сети, что затруднит доступ к ней для злоумышленников. Также, данный подход делает систему более отказоустойчивой за счет возможности каждого сегмента определённое время работать без доступа к центральному серверу, а при выходе из строя локального хранилища пограничного устройства, агрегированные данные в «облачном» хранилище не пострадают.

IIoT, как одна из ветвей развития IoT, состоит из множества соединений Machine-to-Machine (M2M), и с дальнейшим расширением сети их количе-

ство будет расти в геометрической прогрессии. Для поддержки бурного увеличения соединений M2M, сетевая инфраструктура должна поддерживать большое количество подключенных устройств и сложных приложений. Для этого требуются внести сильные изменения в существующую структуру сетей. Понадобится разработка абсолютно новых систем автоматизации управления сетями на замену существующим системам поддержки эксплуатации (OSS), рассчитанных на постоянно растущее количество устройств и их взаимодействие между собой.

Архитектура Промышленного Интернета Вещей

Эталонная архитектура IIoT предполагает разделение на 3 основных уровня: уровень приложений, сетевой уровень и физический уровень [1].

Под уровнем приложений подразумевается объединение систем для организации «умного» производства, использующих данные полученные с множества датчиков, с целью мониторинга, точного контроля и эффективного управления.

Сетевой уровень – это объединение различных сетевых технологий таких, как Программно-конфигурируемые сети (SDN), M2M, 5G, Беспроводные сети сенсоров и актуаторов (WSAN), и так далее. Новые сетевые решения требуются для организации и поддержки взаимодействий между устройствами в промышленности.

Физический уровень состоит из физических устройств, генерирующих данные, которые будут в дальнейшем использованы для обработки на уровне приложений. Ими могут являться все возможные датчики и сенсоры, производственное оборудование, смартфоны, умные терминалы и прочие устройства, подключенные к сети.

Туманные и Пограничные вычисления

На данный момент исследования в сфере Пограничных вычислений активно ведутся, но пока нет какой-либо единой архитектуры, поэтому можно взять за основу Туманные вычисления, которые имеют несколько предложенных архитектур, основанных на стандартах компании OpenFog. Основная суть подходов схожа – перенести часть вычислений из «облака» ближе к конечным устройствам. Однако, концепт «тумана» предполагает только создание инфраструктуры между «облаком» и некоторым количеством конечных устройств, в то время как Пограничные вычисления будут учитывать постоянно растущее количество устройств IoT, их мобильность, давать возможность проводить вычисления на любом типе устройств.

Такие сетевые технологии, как SDN, Виртуализация сетевых функций (NFV) и 5G стали неотъемлемой частью исследований в области Пограничных вычислений [3,4]. SDN позволяет освободить устройства отвечающие за передачу данных от задачи самостоятельного выбора маршрута, получаю

необходимую информацию от логически централизованного узла управления, что упрощает управление сетью, её настройку и масштабирование [5]. NFV разделяет ПО и физическую аппаратуру классической сети, позволяет виртуализировать различные функции сетевого оборудования, дает возможность делить физический ресурс, из-за чего ускоряется развертывание функций и повышается эффективность использования «железа». Комплекс технологий 5-ого поколения включает в себя технологии massive MIMO, Beamforming, micro-base-station, которые ускоряют беспроводную передачу данных, снижают задержки, увеличивают число обслуживаемых устройств и улучшают Quality-of-Service (QoS) [6].

Архитектура IIoT с внедрением Пограничных вычислений

Архитектуру сети IIoT с ЕС стоит рассматривать как разделенную на 3 уровня: Уровень устройств, Пограничный уровень и Уровень облачных приложений [2].

Уровень устройств: Уровень устройств включает в себя все возможные датчики, терминалы, инструменты и измерительные приборы, «умные» устройства, транспортные средства с поддержкой протоколов интернета вещей, роботы и другие подобные приборы. Через проводные (Modbus, Industrial Ethernet, Industrial Optical Fiber, и т. д.) и беспроводные (Wi-Fi, Bluetooth, RFID, NB-IoT, LoRa, 5G, и т. д.) сети эти устройства передают большие потоки данных, собранные с сенсоров этих устройств, на Пограничный уровень и ждут управляющих сигналов в обратном направлении.

Пограничный уровень: Пограничный уровень является центральным в данной архитектуре. Этот уровень в основном отвечает за получение, обработку и пересылку потока данных с Уровня устройств, предоставление сервисов чувствительных к задержкам, пограничный анализ данных, оптимизацию процессов и контроль в реальном времени. Учитывая, что вычислительные мощности различных устройств на этом уровне могут варьироваться на несколько порядков, уровень можно разделить на 3 подуровня: Ближний, Средний и Дальний.

а) Дальний Пограничный уровень: Дальний Пограничный уровень состоит из пограничных контроллеров, которые собирают данные с Уровня устройств, производят первоначальную фильтрацию данных и передают поток управления с других Пограничных уровней и Уровня облачных приложений вниз. Из-за неоднородности датчиков на Уровне устройств, устройства данного уровня должны быть совместимы с различными протоколами используемых на уровне ниже и иметь возможность подключаться к ним для сбора данных в реальном времени для приборов чувствительных к задержкам. После сбора данных, их нужно обработать и отфильтровать, для чего устройства этого уровня должны обладать соответствующими алгорит-

мами. Дальний Пограничный уровень должен обладать задержками, измеряемыми в миллисекундах и меньше, так как на этом уровне принимаются решения для чрезвычайных ситуаций, например, в случае обнаружения человека на дороге сенсорами беспилотного автомобиля.

b) Средний Пограничный уровень: Средний Пограничный уровень в основном содержит пограничные шлюзы и отвечает за сбор данных с Дальнего Пограничного уровня через проводные и беспроводные сети, кэширование собранных данных и произведение смешанных вычислений. Пограничные шлюзы на этом уровне отвечают за передачу потока управления с верхних уровней на нижние уровни, управление оборудованием этого и Дальнего Пограничного уровня. На этом уровне выполняется предобработка, объединение и кэширование смешанных данных, собранных на Дальнем Пограничном уровне. Когда собрано достаточно данных, запускается процесс анализа на встроенной системе, подобный анализу «Big Data» или применению обработки Искусственным Интеллектом. Средний Пограничный уровень также обладает модулем с множеством функций управления (управления устройствами, управления доступом, и т.д.). Решения для событий, которые позволяют задержку в несколько секунд или минут, выносятся на данном уровне. Эти решения являются более обширными и учитывают информацию с большого количества устройств. Например, контроллер на этом уровне может получить данные о транспортных средствах в районе своей ответственности, по этим данным проанализировать уличный трафик и предугадать возможные пробки на дорогах и разослать информацию на конечные устройства для разгрузки транспортной сети.

c) Ближний Пограничный уровень: Ближний Пограничный уровень состоит из мощных пограничных серверов и отвечает за сложные и критически важные обработки информации, делая решения для дальнейшего управления системой, основанные на данных, полученных со Среднего Пограничного уровня через проводную сеть, к тому же должен уметь управлять циклом жизни бизнес-процессов. Пограничные сервера этого уровня обладают большими вычислительными мощностями, чем два уровня ниже и используются в основном для массовой обработки и управления разнородными данными, создания и обучения точных моделей для получения лучших решений по дальнейшей организации устройств в сети. Этот уровень управляет всеми ресурсами Пограничных уровней, поэтому должен уметь управлять эксплуатацией и техобслуживанием, а также виртуализацией и быть способным выделять соответствующе количество ресурсов всем функциям, находящимся под контролем. Задержки на Ближнем Пограничном уровне измеряются в часах, так как принимаются решения для больших зон и на более длительное время. Например, сервер ответственный за «умную» фабрику оптимизирует параметры выпускаемого продукта, основыва-

ясь на информации полученной со всех конвейерных линий и производственного оборудования, которое было задействовано при изготовлении этого продукта.

Уровень облачных вычислений: На Уровне облачных вычислений происходит обработка огромного количества данных, полученных от Пограничного уровня через публичную сеть, а также иных источников, для определения оптимального распределения ресурсов на предприятии, в регионе или даже на уровне страны. Облачные приложения поддерживают приложения верхних уровней, таких как приложения для разработки продукта или процесса, управления продажами и собирают данные из отзывов. Время обработки на данном уровне обычно измеряется в днях.

Заключение

В данной статье были рассмотрены существующая эталонная архитектура IIoT, организация пограничных вычислений с существующими технологиями, пример внедрения пограничных вычислений в IIoT и преимущества данного подхода. Вышеприведенное исследование показывает, что уже на данный момент у нас достаточно технологий для начала постройки подобных сетей, но не хватает формализованной документации и общепринятой архитектуры.

Исследование выполнено в рамках выполнения ПНИ по государственному заданию СПбГУТ на 2021 год.

Список используемых источников

1. Xu, H., Yu, W., Griffith, D., and Golmie, N. A survey on Industrial Internet of Things: A cyber-physical systems perspective // IEEE Access. 2018. Vol. 6. pp. 78238–78259,

2. Qiu, T., Member, S., Chi, J. and Zhou, X. Edge Computing in Industrial Internet of Things: Architecture Advances and Challenges // IEEE Commun. Surv. Tutorials. 2020. pp. 1–28.

3. Мутханна А. С. Интеллектуальная распределенная архитектура сети связи для поддержки беспилотных автомобилей // Электросвязь. 2020. №. 7. С. 29–34.

4. Ateya A. A. et al. Energy-aware offloading algorithm for multi-level cloud based 5G system //Internet of Things, Smart Spaces, and Next Generation Networks and Systems. Springer, Cham, 2018. pp. 355–370.

5. Khakimov A. et al. Flexible architecture for deployment of edge computing applications // Simulation Modelling Practice and Theory. 2022. V. 114. pp. 102402.

6. Lingen et al. F. “The unavoidable convergence of NFV, 5G, and fog: A model-driven approach to bridge cloud and edge // IEEE Commun. Mag. Aug. 2017. Vol. 55, no. 8. pp. 28–35,

УДК 004.77
ГРНТИ 49.33.29

ИССЛЕДОВАНИЕ АСПЕКТОВ РАЗВЕРТЫВАНИЯ БПЛА ДЛЯ РЕАЛИЗАЦИИ ПРИЛОЖЕНИЙ УМНОГО ГОРОДА

А. С. А. Мутханна, Н. А Тагандурдыев

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

5G – технология, позволяющая воплотить в жизнь огромное количество концепций и идей, которые ранее были не реализуемы в силу ограниченных возможностей вычислительных, телекоммуникационных систем. Умный город является одним из таких концепций. Ультравысокие скорости, массовая межмашинная связь, ультранизкие задержки – это услуги, которые способны предоставить прочную основу для реализации приложений умного города. Мониторинг окружающей среды, трекинг автомобильного трафика, система вызова экстренных служб – это малая часть приложений, которую способен предложить умный город и в свою очередь 5G.

Эффективность и качество реализации вышеописанных услуг 5G зависит от технологический решений вычислительной среды. MEC – одно из таких решений. Построение беспилотных летательных аппаратов на основе MEC приведет к повышению эффективности и качества предоставляемых услуг для умного города.

В данной статье производится анализ организации беспилотных летательных аппаратов совместно с технологиями MEC и SDN для реализации концепции умного города. Эта статься иллюстрирует функциональные особенности архитектуры городской сети будущего. Также показываются особенности взаимодействия городских узлов связи с сетевой инфраструктурой.

5G, Интернет Вещей, Умный город, Интернет Вещей, БПЛА.

Введение

Во все времена существовала потребность в быстром и качественном обмене информацией на огромных расстояниях. В настоящее же время эта потребность не только не потеряла актуальность, но увеличилась в связи с более новыми потребностями в высокой безопасности, мобильности, надежности и поддержки огромного числа устройств. 5G является следующей ступенью для удовлетворения информационных потребностей общества. 5G, в отличие от предыдущих поколений, делает ставку на реализации следующий услуг:

- сверхширокополосная мобильная связь (Embb);
- сверхнадежная связи с низкими задержками (URLLC);
- поддержка массовой межмашинной связи (Mmtc) [1].

Эти услуги и стали основным толчком в дальнейших развитии «умной» среды.

Умный город – идея, обретающая всю большую популярность в научно-исследовательской среде. Это происходит из-за стремления объединить сложно управляемые городские информационные системы и создать единую экосистему умного города. Умный город позволит упростить управление процессами городской среды: оптимизация работы транспортной системы, повышение энергоэффективности и экономии используемых ресурсов, повышение безопасности граждан. БПЛА способна предложить улучшенные условия для реализации вышеописанных задач, так как БПЛА имеет такие достоинства как гибкость, мобильность. Эти достоинства в свою очередь позволят оптимизировать ресурсы вычислительной среды 5G.

Основная часть

Несмотря на то, что БПЛА не разрабатывались для гражданский целей, их использование для целей умного города является очень перспективной. БПЛА смогут предоставить гибкую систему для вычислительной среды, что, в свою очередь, поможет снизить стоимость построения чувствительной к задержкам сети и повысить эффективность использования каналов передачи данных.

Отчет, подготовленный McKinsey and Company, показывает, что мировые расходы на строительство и инфраструктуру городов составляют около 2 триллионов долларов США в год, а расходы на ИКТ составляют от 1,5 до 2 % от этого числа [4]. БПЛА, как одна из перспективных решений проблем городской среды, смогут получить высокое внимание не только телекоммуникационных компаний, но и государств.

Планируется, что БПЛА при будут выполнять следующие функции:

•Трекинг дорожного трафика. Дроны могут собирать информацию о трафике и с помощью нейросетей анализировать состояние дорожного трафика в городах и передавать информацию в телекоммуникационные узлы для использования этих данных в приложения управления трафиком (навигация, статистический анализ и т. д.). Эта функция позволит практически полностью оптимизировать использование дорог.

•Сбор информации с сенсорных узлов. БПЛА может выступать в качестве устройства для мониторинга опасных для здоровья и жизни человека объектов городской инфраструктуры. Такая возможность позволит своевременно реагировать на потенциально опасные для жизни граждан происшествия.

•Борьба со стихийными бедствиями и мониторинг ситуации. Кроме сенсорных датчиков БПЛА снабжены и камерами высокого разрешения. Такая возможность позволит оперативно вести сбор данных в зонах чрезвычайных ситуаций без риска для жизни и здоровья людей.

•Перевозка грузов. БПЛА в силу своей мобильности могут стать одним из способов доставки малогабаритных грузов [2].

Вышеописанные идеи требуют новый подход к архитектуре построения сети. Для уменьшения задержек необходимо построить архитектуру на основе граничных вычислений. Кроме уменьшения задержек такой подход так же позволит уменьшить нагрузку с ядра сети. Технология SDN позволит оптимизировать маршрут вырабатываемого устройствами умного города трафика за счет балансировки нагрузки между узлами связи.

На основе вышеописанных суждений была предложена архитектура (рис.) для оптимального использования БПЛА для задач умного города.

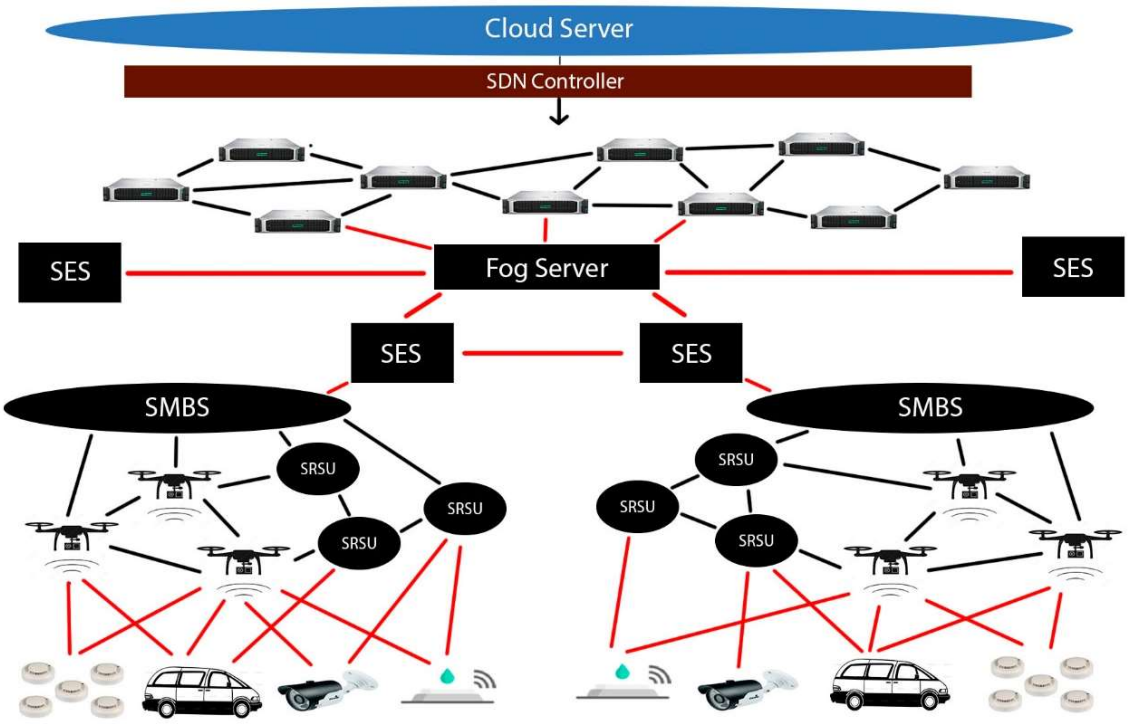


Рисунок. Архитектура сети умного города на основе БПЛА

Задачи умного города, такие как система беспилотных автомобилей, требуют быстрых вычислений и мгновенный обмен между участниками движения. Эти задачи не смогут быть решены при вычислении всех данных в облачных центрах. Несмотря на огромные вычислительные мощности ЦОД, накладываются большие ограничения на пропускную способность сетей с традиционной архитектурой. Локальные вычисления (MEC) на границе сети позволят решить эту проблему. В силу способности граничных устройств обрабатывать данные быстро, но при этом небольших объемов, предлагается обрабатывать в облаке не требовательные к задержкам данные.

MEC делит сеть на 3 уровня вычислений: Cloud Server, Fog Server, Edge Server.

SDN отделяет функцию управления и физической передачи данных, обеспечивает балансировку нагрузки между узлами сети. SDN применяется в гибридном режиме, то есть реализовывается не только в ядре сети, но и в граничных вычислительных серверах (Fog Server, SES, SMBS). БПЛА плотно взаимодействуя с граничными устройствами SMBS и SES получает управленческие данные для размещения в сети и разгрузки трафика.

Предложенная архитектура способна стать основой для построения сети умного города.

Заключение

Умный город является концепцией будущего, которая, бесспорно, улучшит не только качество телекоммуникационных услуг, но и качество жизни в целом. Технологии 5G закладывают огромный потенциал в разнообразие предоставляемых услуг. Конечно, для устойчивого развития таких услуг требуется пересмотр и поиск более эффективных аналогов к ранее используемым технологиям. Одним из таких аналогов является БПЛА, которое на основе предложенной архитектуры готовы создать основу для безопасного, комфортного и эффективного города будущего.

Исследование выполнено в рамках выполнения ПНИ по государственному заданию СПбГУТ на 2021 год.

Список используемых источников

1. Услуги 5G. URL: http://1234g.ru/5g/uslugi-5g (дата обращения: 25.02.2020).
2. Вырелкин А. Д., Кучерявый А. Е. Использование летательных аппаратов для решения задач «умного города» // Информационные технологии и телекоммуникации. 2017. Т. 5. № 1. С. 105–113.

УДК 004.233.2
ГРНТИ 50.09.47

МОДЕЛИРОВАНИЕ КОНЕЧНОГО АВТОМАТА ДЛЯ УПРАВЛЕНИЯ ДИНАМИЧЕСКИМ ПРОГНОЗИРОВАНИЕМ ПЕРЕХОДОВ

О. Л. Неелова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

При рассмотрении вопроса прогнозирования переходов в литературе представлены различные методы формирования таблиц теговой памяти с ответными битами прогнозирования. Наиболее точным представляется прогнозирование по 2-м битам: биту совершенного перехода и биту прогнозирования. Однако при этом алгоритм управляющего конечного автомата дан в общем виде. Для учебного курса «Архитектура вычислительных систем» дается описание работы этого устройства.

прогнозирование переходов, биты прогнозирования, конечный автомат, теговая память.

Важнейшим моментом при разработке и проектировании процессорных ядер является повышение их производительности [1]. Наиболее проблемной группой команд, приводящих к большим потерям процессорного времени, всегда остаются команды переходов. Сократить простои позволяет прогнозирование переходов. Различают статическое прогнозирование (на уровне компилятора) и динамическое (на уровне ядра, в блоке предварительной выборки команд). Статическое прогнозирование позволяет предсказать переход с вероятность не более 75 %, для динамического прогнозирования этот показатель выше. Динамическое прогнозирование строится на использовании табличной теговой памяти, в которую заносятся статистические данные об исполняемых командах перехода в программах при тестовой апробации. В теговую память записывается в качестве тегового слова адрес перехода, подтверждаемый битом достоверности. Ответом на тег служит бит прогнозирования. Наиболее точные результаты прогнозирования дает табличная память, основанная на двух ответных битах: бите свершившегося

Рис. 1. Табличная память
для прогнозирования переходов

перехода и бите прогнозирования. В этом случае бит прогнозирования устанавливается при двух подряд свершившихся переходах. Структура теговой памяти для этого случая показана на рис. 1.

Занесение бита совершенного перехода и бита прогнозирования в ответную часть теговой памяти производится с помощью управляющего конечного автомата. Структура автомата – устройство формирования переходов из одного состояния в другое и исполнительное устройство, обеспечивающее формирование событий внутри каждого состояния. Конечный автомат начинает работу при получении в блоке предварительной выборки команды с подтвержденным адресом перехода. В начальный момент состояние ответных битов устанавливается равным нулю, и автомат ожидает исполнения команды. Если ветвление подтверждается, бит совершенного перехода устанавливается в «1». Граф переходов конечного автомата представлен на рис. 2.

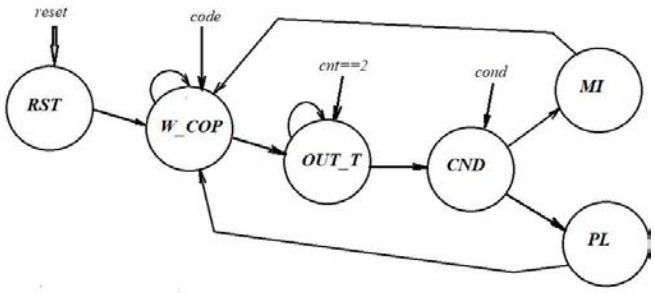


Рис. 2. Граф переходов конечного автомата

Автомат имеет 6 состояний: одно начальное и пять рабочих переходов.

Состояния автомата определяются следующим образом:

RST – состояние автомата в момент включения системы;

W_COP – ожидание поступления команды перехода;

OUT_T – вывод состояния ответных битов;

CND – проверка условия перехода;

MI – переход не выполнен;

PL – переход выполнен.

В случае повторно выполненного перехода оба бита устанавливаются в «1», и переход происходит, не дожидаясь проверки условия. Если же на этапе очередного исполнения условие перехода не подтвердилось, сбрасывается только бит совершения перехода, а прогноз пока сохраняется. Прогноз удаляется после двух подряд неподтвержденных условий перехода.

Исполнительное устройство автомата выставляет на выходной шине одно из 4-х возможных состояний. Фрагмент состояний выходной шины для случаев подтвержденного и неподтвержденного условия будет выглядеть следующим образом:

```
PL:
begin
if(out1==2'b00)
out1<=2'b01;
else
```

```
out1<=2'b11;
end
MI:
begin
if(out1==2'b11)
out1<=2'b10;
else
out1,<=2'b00;
end
```

Полностью программа работы конечного автомата разбирается на лекции по курсу Архитектура вычислительных систем. Программа написана на языке *Verilog HDL.* В лаборатории кафедры Программной Инженерии и Вычислительной техники с помощью этой программы возможно производить моделирование управлением динамическим прогнозированием переходов.

Список используемых источников:

1. Таненбаум Э., Остин Т. Архитектура компьютера: пер. с англ. 6-е изд. СПб.: Питер, 2018. 816 с. ISBN 978-5-496-00337-7.

Статья представлена заведующим кафедрой ПИВТ, доктором технических наук, доцентом Р. В. Киричком.

УДК 530.145
ГРНТИ 29.05.15

КВАНТОВАЯ СЕНСОРИКА. СОВРЕМЕННОЕ СОСТОЯНИЕ И ТЕНДЕНЦИИ РАЗВИТИЯ

Б. К. Никитин, Е. В. Полякова, А. Н. Сергеев

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Квантовые технологии, обеспечивая высокую степень контроля микросостояния системы, позволяют создавать сверхточные квантовые сенсоры, что в ближайшем будущем стимулирует развитие множества отраслей: космос, беспилотный транспорт, строительство, нефтедобычу, геологоразведку, медицинскую диагностику, оборонно-промышленный комплекс и др.

квантовая сенсорика, квантовые датчики, высокоточные измерительные приборы.

Квантовые технологии представляют собой ту часть физики, в которой используются особенности работы законов квантовой механики. Основой работы квантовых технологий являются несколько фундаментальных особенностей поведения квантоворазмерной системы, такие как [1]:

- принцип неопределённости Гейзенберга;
- квантовая суперпозиция состояний систем;
- дискретность уровней энергии, по-другому называемая квантово-размерным эффектом;
- прохождение квантов через потенциальные барьеры;
- сцепленность состояний отдельных квантов.

Квантовые технологии являются по сути своей развитием новейших достижений современной науки. Ввиду того, что советская, а затем и российская школа квантовой физики всегда находилась на передовых рубежах мировой физики, и этот потенциал удалось удержать, то сложились все предпосылки для дальнейшего развития квантовых технологий и даже занятия лидирующих положений в отдельных направлениях этой науки. Особую уверенность придает этому тот факт, что во всем мире квантовые технологии в их промышленном применении находятся в стадии пусть не начального, но все же не сильно продвинутого уровня.

Квантовые технологии делятся на три основных части [2]:

1. Квантовые вычисления (КВ);
2. Квантовые коммуникации (КК);
3. Квантовые сенсоры и метрология.

Квантовые сенсоры – это устройства и приборы, основанные на квантовых эффектах. Благодаря максимально достижимым на сегодняшний день частотам, измерительные приборы на этих принципах имеют высочайшую точность и разрешающую способность. Отсюда возникает возможность управлять процессами в макросистемах на микроуровне, что дает максимальные метрологические характеристики измерительных систем.

В настоящее время из всех видов квантовых технологий наиболее проработанной являются квантовые коммуникации. Квантовая сенсорика не может похвастаться такими же достижениями. Это не очень хорошо, но здесь надо помнить, что слабая изученность вопроса дает огромные возможности для исследований, в результате которых появятся новые устройства, приборы и методы измерений.

Таким образом, в перспективных квантовых сенсорах будет заложено сверхточное пространственное разрешение с минимальной временной дискретизацией, что многократно повысит точность и разрешение по сравнению с существующими классическими сенсорами (табл. 1).

При этом существует возможность осуществлять высококачественный контроль состояния различных процессов и систем, а это позволяет создавать квантовые сенсоры со сверхвысокой чувствительностью. Создание и

дальнейшее развитие технологий изготовления датчиков нового поколения готовит революционные изменения в самых разных отраслях экономики, например, таких как:

– оборона и безопасность жизнедеятельности,

– навигационные системы позиционирования макро- и микрообъектов;

– строительство безопасных, экологически чистых и сейсмически устойчивых зданий и сооружений,

– добыча и переработка природных ископаемых;

– медицинские технологии диагностики и лечения заболеваний;

– индустрия 4.0 (или четвёртая промышленная революция – новый подход к производству, основанный на массовом внедрении информационных технологий в промышленность, автоматизации бизнес-процессов и распространении искусственного интеллекта).

Существует система оценки готовности к созданию и использованию приборов, устройств и методов. Эта система разработана специалистами NASA и имеет девять уровней, обозначаемых аббревиатурой TRL[1].

Уровни готовности технологии [3]:

- TRL 1 – разработка основных принципов.
- TRL 2 – разработка и оценка области применения.
- TRL 3 – научно-исследовательские работы. Подтверждение характеристик.
- TRL 4 – проверка работы в лабораторных условиях.
- TRL 5 – проверка в реальных условиях.
- TRL 6 – испытания готовой модели в реальных условиях.
- TRL 7 – испытания опытного образца в условиях эксплуатации.
- TRL 8 – испытание готовой системы в условиях эксплуатации.
- TRL 9 – доведение системы или образца до промышленного применения.

Развитие квантовой сенсорики в целом достигает уровни TRL 3–9, а в РФ TRL 1–5.

Квантовые сенсоры позволяют измерять различные физические величины. К их основным техническим характеристикам можно отнести:

– Точность измерения;

– Высокую чувствительность к изменению измеряемой величины;

– Отличную геометрическую разрешающую способность;

– Великолепную разрешающую способности во времени;

– Огромный динамический диапазон измеряемых сигналов;

– Широкий диапазон работы по разным параметрам, например, по частоте или по температуре;

– Сверхмалое время отклика;

– Низкая потребляемая мощность.

К недостаткам таки устройств можно отнести сложность технического обслуживания и высокую стоимость развертывания и эксплуатации.

Несмотря на перечисленные недостатки в мире наблюдается рост развития квантовых технологий в целом и, в частности, квантовой сенсорики. Основными разработчиками устройств на основе квантовых эффектов являются университеты и научно-исследовательские институты.

В настоящее время в России выполнены исследования по перспективным направлениям развития квантовой сенсорики. В результате можно отметить несколько направлений развития, по которым Российская Федерация имеет существенные преимущества. К числу таких направлений относятся [4]:

– часы на внутриатомных фотонных эффектах;

– измерители гравитации и устройства выделения гравитационного ускорения из общего ускорения объекта;

– гироскопы на анализе поведения групп спинов в твердом теле;

– сосредоточенные датчики магнитного поля, электрического поля и температуры;

– сенсоры на основе спин-поляризованного токопереноса;

– сенсоры, основанные на методе оптического детектирования микроволнового поглощения;

– твердотельные фотоумножители толщиной несколько микрометров;

– устройства непрерывной регистрации всего спектра падающего излучения;

– генераторы и приемники одиночных фотонов.

По каждому из вышеперечисленных направлений имеются практические наработки и реальные приборы и устройства.

Важным направлением развития квантовой сенсорики и квантовых технологий в целом является разработка недорогих однофотонных приемников, а также источников генерации и излучения фотонов.

Продукты на основе квантовой сенсорики и метрологии смогут преобразить многие виды производств и экономики.

Основными направлениями применения продуктов квантовой сенсорики в настоящее время являются:

– медицина;

– интернет вещей;

– глобальные навигационные системы.

ТАБЛИЦА. Современное состояние развития квантовых сенсоров и перспективы развития

Показатель	2019	2021	2024
Количество разработанных типов промышленных образцов квантовых сенсоров	2	4	6

Показатель	2019	2021	2024
Среднее квадратическое относительное двухвыборочное отклонение измеренного значения меры частоты за интервал 10 ч	10^{-16}	10^{-17}	10^{-18}
Пространственное разрешение сенсоров на центрах окраски, мкм	10	2	0,5
Предельная дальность вне лаборатории, км		200	250

Невозможно разработать универсальные технические характеристики для всех квантовых сенсоров. Поэтому развитие квантовой сенсорики будет иметь приоритетный вид, то есть произойдет выделение отдельных направлений, для каждого из которых разработают общие группы технических характеристик.

В настоящее время сенсоры сгруппированы в три группы [5]:

1. Часы, приборы для высокоточного измерения силы тяжести, устройства для оценки скорости изменения состояния физической величины;
2. Датчики электрических и магнитных полей;
3. Квантовые метрологические датчики.

Значительные успехи достигнуты в разработке частотных стандартов, по оптическим часам к 2024 году планируется выход на TRL-8, к 2030 году – создание высокоточных систем позиционирования макрообъектов с разрешением в сантиметровом диапазоне и внедрение прецизионных самосинхронизирующихся систем для управления передачей потоков данных.

В России разработкой и исследованием квантовых сенсоров занимаются следующие организации [4]:

- Сибирское отделение Института лазерной физики РАН (СО ИЛФ РАН);
- Институт прикладной физики РАН (ИПФ РАН);
- Центр квантовых технологий физического факультета МГУ имени М. В. Ломоносова (ЦКТ ФФ МГУ);
- Факультет вычислительной математики и кибернетики МГУ (ВМК МГУ имени М.В. Ломоносова);
- Национальный исследовательский университет ИТМО;
- Физико-технический институт им. А. Ф. Иоффе;
- Всероссийский научно-исследовательский институт физико-технических и радиотехнических измерений (ВНИИФТРИ);
- Базовая кафедра квантовой оптики и телекоммуникаций ЗАО «Сконтел» (Московский институт электроники и математики МИЭМ НИУ ВШЭ);
- Институт спектроскопии Российской академии наук (ИСАН);
- Национальный исследовательский технологический университет МИСиС (НИТУ МИСиС);
- Московский педагогический государственный университет;

- Институт физики твердого тела РАН (ИФТТ РАН);
- Академия криптографии Российской Федерации;
- АО «Концерн «Автоматика».

Основные успехи и достижения:

– создан сверхминиатюрный квантовый сенсор на основе атомного стандарта частоты;

– разработана технология производства ячеек микро-электро-механических систем (MEMS);

– разработана теоретическая база и проводятся экспериментальные и исследования для создания высокочувствительных квантовых сенсоров инерциальных сил (гравиметров, акселерометров и гироскопов);

– разработана теоретическая база и проводятся экспериментальные исследования с целью создания компактных магнитометров;

– разработано многоканальное однофотонное приемное устройство;

– разработаны приборы, размещаемые в квантовых оптических интегральных схемах;

– созданы генераторы одиночных фотонов и их детекторы;

– ведется опытно-конструкторские работы по созданию охлаждаемой однофотонной видеокамеры с диапазоном чувствительности 0,4–2,0 мкм;

– разрабатываются часы и гравиметр на основе первого в России атомного чипа;

– ведутся работы в области физической реализации квантовых генераторов случайных чисел и их статистического тестирования случайности;

– разработаны физические основы и построены прототипы устройств «абсолютной квантовой фотометрии».

Впереди очень большая и длинная дорога по совершенствованию существующих и созданию новых технологий, приборов и устройств квантовой сенсорики, которая потребует большого числа высококвалифицированных специалистов.

Список используемых источников

1. Квантовые технологии. Атомная энергия. URL: https://www.atomic-energy.ru/quantum/experts (дата обращения: 29.01.2022).

2. Дорожная карта развития «сквозной» цифровой технологии «квантовые технологии». М., 2019. URL: https://digital.gov.ru/uploaded/files/07102019kvantyi.pdf

3. Technology Readiness Level. URL: https://www.nasa.gov/directorates/heo/scan/engineering/technology/technology_readiness_level

4. Квантовые сенсоры и метрология. Аналитический центр при правительстве Российской Федерации. URL: https://digitech.ac.gov.ru/technologies/quantum_technologies/kvantovye-sensory-i-metrologiya (дата обращения: 29.01.2022).

5. Красников Геннадий. Квантовые сенсоры: достижения и перспективы развития // Российская Академия Наук. URL: http://www.ras.ru/news/shownews.aspx?id=21c0779b-1764-4efe-8451-0d5bdfc82014 (дата обращения: 29.01.2022).

УДК 004.056
ГРНТИ 81.93.29

АНАЛИЗ ПОДХОДОВ К ПОСТРОЕНИЮ СИСТЕМ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ НА ОСНОВЕ ПРИНЦИПОВ ФЕДЕРАТИВНОГО ОБУЧЕНИЯ

Е. С. Новикова

Санкт-Петербургский Федеральный исследовательский центр Российской академии наук

Одной из открытых проблем, связанных с безопасностью систем, построенных на основе технологии Интернета Вещей, является обеспечение защищенности критических важных данных, необходимых в т.ч. при обнаружении вторжений. Возможным способом решения данной проблемы является применение федеративного обучения для построения систем обнаружения вторжений. Федеративное обучение (ФО) - это относительно новая модель построения распределенного машинного обучения, которая позволяет строить системы анализа, обеспечивающие приватность персональных и других критически важных данных. В настоящем докладе исследуется подходы к построению систем обнаружения вторжений на основе принципов федеративного обучения. анализируются представленные в литературе системы, обсуждаются их достоинства и недостатки.

интернет Вещей, выявление аномалий, конфиденциальность данных, федеративное обучение.

В настоящее время методы машинного обучения широко используются для обнаружения вторжений в информационных системах. Разработано множество подходов, основанных на методах классического машинного обучения, таких как метод опорных векторов, деревья решений, метод k-ближайших соседей, самоорганизующиеся карты Кохонена, методах глубокого обучения, таких как сверточные нейронные сети, рекурентные нейроные сети, машина Больцмана, глубокие автоенкодеры и т. д. [1, 2]. Применение данных методов требует наличия достаточно большого объема данных. Эта проблема чаще всего решается применением единого облачного хранилища, где собираются данные как от различных источников, так и различных их владельцев. При таком подходе помимо рисков, связанных

с нарушением конфиденциальности, целостности и доступности, возникают риски, связанные с обработкой персональных данных. Согласно многим законодательным документам стран мира в области защиты персональных данных к ним относятся не только паспортные данные, биометрия, данные о состояния здоровья, но и уникальные идентификаторы устройств, приложений и точек беспроводного доступа и т. д. Последние полезны при обнаружении сетевых вторжений, а также аномалий, связанных с внутренним нарушителем, поэтому необходим поиск решений, которые позволили бы найти компромисс между эффективностью обнаружения вторжений и защищенностью персональных и других критически важных данных.

В 2016 году М. МакМахан и др. предложили новую вычислительную парадигму распределенного машинного обучения [3]. Согласно ей, обучение данных осуществляется непосредственно на узлах, на которых хранятся данные, а затем результаты локального обучения передаются узлу, выполняющему агрегирование параметров локальных моделей и вычисление глобальной модели анализа. Таким образом формируется модель, которая учитывает данные, принадлежащим разным узлам, без их передачи по сети и сбора в едином хранилище. Ключевым отличием федеративного обучения от распределенного машинного обучения является использование узлов в качестве источников данных и выполнение вычислений как можно ближе к данным, в то время как при распределенном машинном обучении узлы используются в качестве источников вычислительных ресурсов для масштабирования параллельной обработки больших объемов данных. Благодаря такому решению использование ФО позволяется снизить риск несанкционированного доступа к данным, поскольку они не передаются по сети; снизить объемы передаваемого трафика, т. к. результаты обучения обычно гораздо меньше по объему, чем сами данные.

Одной из первых работ, в которой предложена концепция системы обнаружения вторжений, построенная на принципах ФО, является работа [4]. В ней представлена автономная самообучающаяся распределенная система D¨IOT для обнаружения скомпрометированных устройств Интернета Вещей. Данная система строит профили устройств на основе их сетевого поведения, и именно для обучения моделей, которые выявляют аномалии в поведении устройств, используется ФО.

В [5] авторы также предложили систему обнаружения вторжения для устройств Интернета Вещей, в основе которой лежит федеративное обучение конволюционной нейронной сети с механизмом памяти FedACNN. Проведенные эксперименты показали, что данная модель способна обеспечить обнаружение вторжений с высокой точностью (до 99,76 %) при относительно хорошей производительности логического вывода. В качестве обучающего тестового датасета был использован открытый набор данных NSL-

KDD, однако авторы не описали, каким образом было смоделирована экспериментальная среда с несколькими клиентами.

Первая система обнаружения вторжений для промышленных киберфизических систем представлена в [6]. Авторы провели серию экспериментов с различным числом клиентов и показали, предложенная модель обнаружения вторжений превосходит многие другие современные походы по метрикам качества машинного обучения, и все модели анализа, разработанные для разных сценариев атак сходятся после достаточного раундов аггрегирования параметров локальных моделей.

Дж. Шинджи и др. предложили применить схему сегментированного ФО Segmented-FL для построения более эффективной системы обнаружения вторжений [7]. Ключевым отличием схемы сегментированного ФО от обычного является разбиение клиентов или владельцев данных на группы (сегменты), и каждая выделенная группа узлов работает с определенной глобальной моделью для адаптивного обучения. Эта схема используется как для обмена параметрами между клиентами, так и для автоматической группировки клиентов. Последнее используется для повышения адаптивности системы к различным параметрами сетевой инфраструктуры. В частности, в ней реализуется периодическая локальная оценка модели, на основе которой происходит сегментация клиентов: клиенты со схожими параметрами сетевой инфраструктуры объединяются в одну группу. Кроме того, в системе Segmented-FL реализована функция взвешенной агрегацией параметров локальных моделей, которая учитывает количество образцов обучающей выборки на каждом клиенте. Такие модификации федеративного обучения позволили авторам построить адаптивную систему обнаружения вторжений, которая также устойчива к возможным отличиям в сетевых инфраструктурах. В качестве обучающих выборок использовались датасеты CIDDS-001 и CIDDS-002.

В [8] авторы исследовали, как влияют отличия в распределении данных на клиентах на точность выявления вторжений. Авторы создали три различных сценария атак на основе датасета CIC-ToN-IoT, который затем был распределен между клиентами для моделирования различного распределения данных. Проведение авторами исследование показало, что влияние не идентично распределенных данных с сильным перекосом распределений в классах значительно влияет на эффективность моделей обнаружения атак. Для устранения данной проблемы авторы предложили алгоритм выбора экземпляров локальной выборки, основанный на оценки энтропии Шеннона, применение которого позволяет повысить общую точность и получить схожие результаты по сравнению со сценарием, в котором наборы данных сбалансированы между клиентами.

Таким образом, анализ литературы показывает, что разработка подходов обнаружения вторжений, использующих принципы ФО находится пока

еще в начальном состоянии. Авторы в основном тестируют применимость федеративного обучения как способа обучения модели анализа в распределенных системах. Для этого используются известные наборы данных, на основе которых моделируется горизонтальное распределение данных. Отсутствие датасетов, моделирующих реально распределение данных между разными клиентами, приводит к тому, что только в некоторых работах оценивается влияние несбалансированных датасетов на качество решения задачи обнаружения вторжений. Вопросы построения систем обнаружения вторжений для систем, в которых данные распределены вертикально, т. е. для случая, когда каждый узел системы хранит только часть атрибутов об некотором объекте, в научной литературе практически не изучены представлены.

Работа выполнена при финансовой поддержке РНФ (проект РНФ № 22-21-00724).

Список используемых источников

1. Браницкий А. А., Котенко И. В. Анализ и классификация методов обнаружения сетевых атак // Труды СПИИРАН. 2016. № 2 (45). С. 207–244.

2. Гайфулина Д. А., Котенко И. В. Анализ моделей глубокого обучения для задач обнаружения сетевых аномалий Интернета вещей // Информационно-управляющие системы. 2021. № 1. С. 28–37. URL: https://doi.org/10.31799/1684-8853-2021-1-28-373.

3. Kairouz, P., McMahan, H. B., Avent, B., Bellet, A., Bennis, M., Bhagoji, A. N., d'Oliveira, R.G. Advances and open problems in federated learning. URL: arXiv:1912.04977 2019 (дата обращения: 20.02.2022).

4. Nguyen, T. D., Marchal, S., Miettinen, M., Fereidooni, H., Asokan, N., Sadeghi, A. DÏoT: A Federated Self-learning Anomaly Detection System for IoT // Proceedings of the IEEE 39th International Conference on Distributed Computing Systems (ICDCS). 2019. pp. 756–767.

5. Zhao, R., Yin, Y., Shi, Y., Xue, Z. Intelligent intrusion detection based on federated learning aided long short-term memory // Physical Communication. 2020. № 42.

6. Li, B., Wu, Y., Song, J., Lu, R., Li, T., Zhao, L. DeepFed: Federated Deep Learning for Intrusion Detection in Industrial Cyber–Physical Systems // IEEE Transactions on Industrial Informatics. 2021. № 17 (8). pp. 5615–5624. doi: 10.1109/TII.2020.3023430.

7. Shingi, G., Saglani, H., Jain, P. Segmented Federated Learning for Adaptive Intrusion Detection System. URL: arXiv:abs/2107.00881.2021 (дата обращения: 20.02.2022).

8. Campos, E. M., Saura, P. F., González-Vidal, A., Ramos, J. L., Bernabé, J. B., Baldini, G., Gómez-Skarmeta, A. F. Evaluating Federated Learning for Intrusion Detection in Internet of Things: Review and Challenges. URL: arXiv:abs/2108.00974 2021 (дата обращения: 20.02.2022).

УДК 004.413
ГРНТИ 50.41.25

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ДЛЯ БИЗНЕС АНАЛИЗА И ПРОЕКТИРОВАНИЯ ПРИЛОЖЕНИЙ

Д. В. Окунева

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье представлен обзор возможностей современной среды разработки прикладных решений 1С:EDT. В основе лежит среда разработки модульных кроссплатформенных приложений Eclipse. Основное отличие от конфигуратора 1С:Предприятие 8 заключается в том, что при использовании 1С:EDT можно вести разработку конфигурации в альтернативной среде. 1С:EDT обеспечивает создание прикладных решений на встроенном языке 1С:Предприятие 8, облегчает работу программиста за счет встроенных инструментов автоматизации, позволяя расширить функционал инструментов разработки с помощью технологии плагинов. Кроме того, для анализа структуры бизнес-приложения в виде ER-диаграммы используется функционал «Схема данных». Преимуществами являются групповая разработка и версионирование обеспечиваемое внешней системой контроля версий Git.

1С:EDT, GIT, бизнес анализ, конфигуратор, прикладные решения, java, eclipse.

В настоящее время процесс импортозамещения стоит довольно остро. Поддержка государства и риск санкций способствуют разработке и внедрению отечественного программного обеспечения.

Фирма 1С многие годы занимается разработкой программного обеспечения, эффективность которого не вызывает сомнений. С помощью программных продуктов 1С автоматизирован учет многих компаний не только в России, но и других странах.

Появление платформы 1С:EDT (1С:Enterprise Development Tools), среды разработки нового поколения, ориентированной на разработку крупных прикладных решений, является логичным продолжением развития программных продуктов 1С.

Она создана на основе свободной интегрированной среды разработки модульных кроссплатформенных приложений Eclipse, широко используемой разработчиками во всем мире.

1С:EDT поддерживает ключевые принципы создания прикладных решений на платформе «1С:Предприятие 8» (рис.). 1С:EDT содержит большое количество инструментов автоматизации разработки, делающих работу программиста более быстрой и комфортной, а также позволяет расширять

функциональность инструментов разработки с помощью технологии плагинов [1].

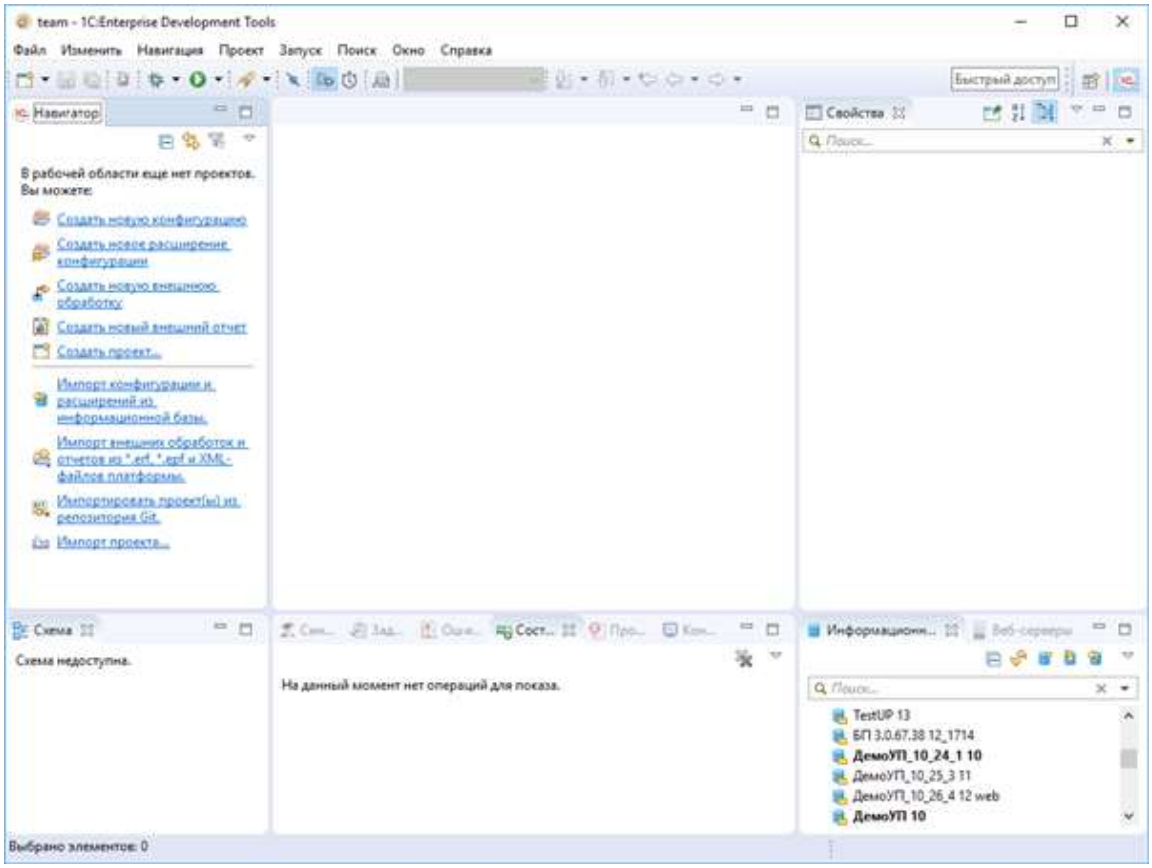


Рисунок. Окно перспективы 1C:Enterprise.

1C:EDT содержит ряд функциональных и архитектурных возможностей, отсутствующих в 1С: Конфигураторе.

В качестве основных преимуществ 1C:EDT можно выделить следующие возможности: использование разных версий платформы и информационных баз для отладки конфигурации, а также поддержка групповой разработки и версионирования с помощью Git`a; удобство разработки мобильных приложений за счет использования встроенного веб-сервера и выбора устройств для их запуска; использование схемы данных в виде ER-диаграммы для бизнес анализа архитектуры решения [2].

Система контроля и управления версиями программного обеспечения Git (*Global Information Tracker*) обеспечивает управление версиями для большого количества проектов по разработке программного обеспечения, как коммерческих, так и с открытым исходным кодом. Система кроссплатформенная, может применяться со многими средами разработки [3].

При использовании Git`a в рамках разработки на 1C:EDT достаточно локальных файлов и ресурсов, чтобы посмотреть историю проекта, Git’у не нужно соединяться с сервером для её получения и отображения. В отличие

от других систем контроля версий Git сравнивает версии между собой, отображая изменения, а не копирует их [2].

Такой подход существенно позволяет повысить производительность разработки программных продуктов.

При коллективной разработке бизнес приложений возникает проблема синхронизации моделей, созданных различными разработчиками. Такая проблема актуальна, когда над одной системой работает большое количество разработчиков.

Моделирование используется для изучения бизнес логики и углубления понимания структуры информационной базы. Использование ER-диаграмм позволяет в понятном формате отобразить структуру данных и связи между ними, что позволяет анализировать структуру информационной базы и ее корректировать.

При разработке бизнес приложения необходимо также учитывать возможность создания мобильной версии, предоставляющий оперативный доступ к данным системы в удаленном формате.

До появления 1С:EDT для мобильной разработки необходимо было развернуть на стационарном компьютере веб-сервер Apache, комплект средств разработки Android SDK и мобильную платформу 1С:Предприятие 8 [4].

В рамках среды 1С:EDT разработка мобильных приложений стала удобнее за счет возможностей использования встроенного веб-сервера для их отладки и возможностью выбора устройств для их запуска. При этом разработку разных проектов можно вести в рамках одного окна, не запуская под каждое приложение «свой» конфигуратор.

Проверка конфигурации выполняется «на лету» прямо в процессе изменения ее структуры и в процессе редактирования модулей. Найденные ошибки и возможные неполадки отображаются удобным образом. Все изменения, вносимые разными разработчиками, отображаются в одном окне. Например, это удобно при обновлении конфигурации в 1С:EDT.

Последнее время достаточно много разработчиков используют для разработки новых прикладных решений уже существующие – типовые. Внесенные в типовую конфигурацию изменения необходимо учитывать при обновлениях. Использование 1С:EDT позволяет удобнее обновлять модифицированные прикладное решение, при этом все вносимые изменения в типовой конфигурации будут отображаться в процессе.

Из минусов 1С:EDT, стоит отметить ее ресурсоемкость и человеческий фактор – людям довольно сложно перейти на новые технологии.

Развитие 1С:EDT фирмой 1С осуществляется довольно интенсивно, что говорит о перспективности и актуальности данной среды разработки.

Список используемых источников

1. 1C:Enterprise Development Tools. Руководство разработчика. Издание 2021.3.4. URL: https://its.1c.ru/db/edtdoc
2. 1C:EDT. URL:https://edt.1c.ru/
3. Git how to. URL: https://githowto.com/ru
4. Хрусталева Е. Ю. Знакомство с разработкой мобильных приложений на платформе "1С:Предприятие 8". Изд. 3. Москва: ООО "1С-Паблишинг", 2022. ISBN 978-5-9677-3181-5.

УДК 004.056(075.8)
ГРНТИ 81.96

СПОСОБ ОБЕСПЕЧЕНИЯ АНОНИМНОСТИ ЭЛЕКТРОННОГО ГОЛОСОВАНИЯ ОТ АТАКИ ОТСЛЕЖИВАНИЯ ГОЛОСОВ ОТДЕЛЬНЫХ ИЗБИРАТЕЛЕЙ

Д. А. Орлов, В. Д. Салман, В. А. Яковлев

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Предложен способ защиты анонимности избирателей на основе представления голоса избирателя (числа), как суммы слагаемых и шифровании по отдельности каждого слагаемого. Далее криптограммы, полученные при шифровании слагаемых, направляются на разные сервера для перемножения. Анонимность голоса избирателя обеспечивается, если будет «честным» хотя бы один сервер.

электронное голосование, гомоморфная система шифрования, криптосистемы Пэйе, анонимность электронного голосования.

Электронная система голосования – это удаленная система, использующая интернет, мобильные компьютеры, смартфоны для того, чтобы дать возможность избирателям голосовать на выборах.

В [1] представлен подробный обзор распространенных моделей электронного голосования: mix-net, гомоморфная и слепой подписи. Предоставлено подробное описание основных идей, лежащих в основе этих схем.

Одним из важнейших требований электронного голосования является тайна голосования и анонимность избирателей. Анонимность электронного голосования может быть обеспечена на основе использования гомоморфной системы шифрования. В такой системе обеспечение тайны голосования и анонимности основываются на том, что выполняется следующее условие

$$D_{\widehat{K}}\left(E_K(m_1)\cdot E_K(m_2)\cdot \ldots\ldots\cdot E_K(m_N)\right) = m_1 + m_2 + \cdots + m_N, \quad (1)$$

где $E_K(m_i)$ – зашифрованный голос m_i i-го избирателя, $D_{\widehat{K}}(E)$ – результат дешифрования криптограммы, составленной из произведения криптограмм всех избирателей. Суть выражения (1) заключается в том, что результат дешифрования произведения зашифрованных голосов равен сумме этих голосов. За счет шифрования обеспечивается тайна голоса при его передаче по каналам системы, а за счет того, что при расшифровании получается сумма всех голосов сразу, обеспечивается анонимность индивидуальных голосов. Шифрование каждый избиратель осуществляет на едином для всех открытом ключе K, дешифрование осуществляет счетная комиссия на закрытом ключе – $\widehat{K}$, который до начала подсчета голосов хранится в разделенном на части виде и восстанавливается для подсчета голосов сразу после окончания голосования.

В [2] представлена схема выборов с тайным голосованием с участием многих доверительных центров, которая гарантирует конфиденциальность, универсальную проверяемость и надежность. Система включает в себя: избирателя, избирательную комиссию, орган власти и электронную доску объявлений (ЭДО). В этой системе используются следующие криптографические схемы: схема Эль-Гамаля, пороговая криптосистема Эль-Гамаля, доска объявлений, доказательства действительности бюллетеня. Избиратель шифрует бюллетень с помощью схемы Эль-Гамаля и публикует ее на ВВ с подтверждением действительности бюллетеня. доверительный центр проверяет действительность бюллетеня. Наконец, доверительный центр выполняет протокол дешифрования.

Рис. 1. Схема тайного электронного голосования

Однако анонимность отдельных избирателей может быть нарушена, если между и избирательной комиссией и одним из серверов, на который избиратель направляет свой зашифрованный бюллетень, есть сговор. В этом

случае ИК может получить у этого сервера голоса избирателей (даже после выборов) и, используя секретный ключ, который был восстановлен для расшифрования произведения бюллетеней, расшифровать полученные от сервера бюллетени их и узнать, за кого проголосовал тот или иной избиратель.

Для решения проблемы отслеживания голосов отдельных избирателей, предлагается способ на основе представления голоса избирателя (числа) в виде нескольких слагаемых (по количеству серверов) и шифрования по отдельности каждого слагаемого. На рис. 2 показана схема, поясняющая способ разделения голоса. Схема включает в себя: избирателя, избирательную комиссию (ИК) и несколько серверов.

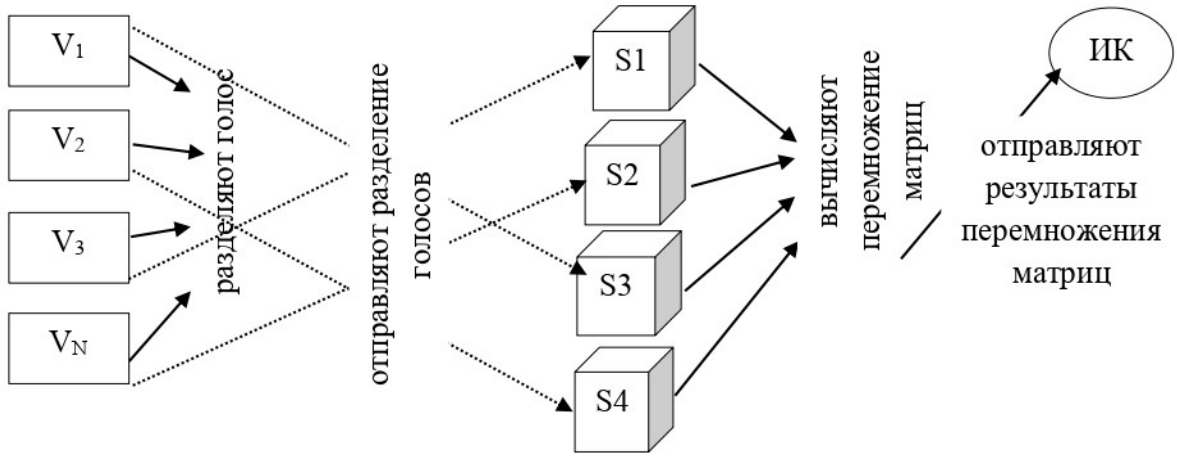


Рис. 2. Предлагаемая схема разделения голосов

Пусть в схеме голосования имеется P серверов и T избирателей.

1. Избиратель с номером *i* голосует в соответствии с регламентом голосования за нескольких кандидатов и его голос может быть представлен как число m_i. Далее он разделяет свои голос на части (количество частей равно числу серверов в системе). Разделенный голос может быть записан в виде:

$$m_i = m_{iT} \cdot b^{P-1} + m_{i(T-1)} \cdot b^{P-2} + \cdots + m_{i2} \cdot b^1 + m_{i1} \cdot b^0, \qquad (2)$$

где b – основание системы счисления. b выбирается из условия $\max m_i \le b^P$.

2. Избиратель шифрует каждое слагаемое в (2) по схеме Пэйе [3], используя ранее полученный открытый ключ одинаковый для всех избирателей. По свойству гомоморфности можно записать:

$$E\left(m_{ij} b^{j-1}\right) = E\left(m_{ij}\right)^{b^{j-1}}.$$

Обозначим криптограмму $E\left(m_{ij}\right)^{b^{j-1}} = E'(m_{ij})$. Заметим, что при расшифровании криптограммы $E'(m_{ij})$ автоматически восстанавливается

место слагаемого m_{ij} в его b- ичном представлении. Зашифрованный голос i-го избирателя может быть записан как $E'(m_i) = \prod_{j=1}^{P} E'(m_{ij})$.

3. Каждый избиратель отправляет криптограммы $E'(m_{i1}).E'(m_{i2}),\dots,E'(m_{iP})$ по одному на серверы в случайном порядке.

4. Далее каждый сервер перемножает, поступившие на него части от всех избирателей. например, для сервера S_1:

$$\prod_{S_1} = \left(E'_{1j_s} \cdot E'_{2j_s} \cdot E'_{3j_s} \cdot \dots \cdot E'_{Tj_s}\right),$$

где E'_{ij_s} – криптограмма, полученная первым сервером от i-го избирателя и соответствующая j_s – части его сообщения $s = (1,2,\dots,P)$.

Полученную криптограмму-произведение сервер отправляет в избирательную комиссию.

5. В ИК осуществляется перемножение криптограмм, полученных от всех серверов. $E_{\sum} = \prod_{S_1} \cdot \prod_{S_2} \cdots \prod_{S_P}$.

6. Далее избирательная комиссия, используя закрытый ключ, восстановленный из его частей, осуществляет расшифрование криптограммы $E_{\sum}$.

Несложно показать, что поскольку в произведении участвуют все зашифрованные части голосов от каждого избирателя и эти части на основании свойства (2) имеют свой вес получим: $D\left(E_{\sum}\right) = (m_{11}b^0 + m_{12}b^1 + \dots + m_{1P}b^{P-1}) + (m_{21}b^0 + m_{22}b^1 + \dots + m_{2P}b^{P-1}) + \dots + (m_{T1}b^0 + m_{T2}b^1 + \dots + m_{TP}b^{P-1}) = m_1 + m_2 + \dots + m_T$.

Видим, что в данном случае каждый сервер получает только одну часть сообщения (голоса) от избирателя, причем не известно какому слагаемому в представлении (2) она соответствует.

Определить голос i-го избирателя избирательная комиссия сможет, только если будет иметь все слагаемые его числа m_i. Поэтому, если хотя бы один сервер будет честным, то сговор ИК с группой, оставшихся серверов, не даст результата.

Список используемых источников

1. Okediran Oladotun Olusola G. R. A., Omidiora Elijah Olusayo, Olabiyisi Stephen Olatunde, A Review of the Underlying Concepts of Electronic Voting // Inf. Knowl. Manag., 2012. vol. 2, no. 1. p. 14.

2. Cramer, R., Gennaro, R., and Schoenmakers, B. A secure and optimally efficient multi- authority election scheme // Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics). 1997. vol. 1233, pp. 103–118. doi: 10.1007/3-540-69053_9.

3. Pascal, P., Secure hash-and-sign signatures without the random oracle // Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). 1999. vol. 1592. Springer, pp. 123–139. doi: 10.1007/3-540-48910-X_9.

УДК 004.056.5
ГРНТИ 81.93.29

НЕЧЕТКАЯ ИДЕНТИФИКАЦИЯ УЯЗВИМОСТЕЙ В ИНТЕРФЕЙСАХ БЕСПИЛОТНОЙ ТРАНСПОРТНОЙ СРЕДЫ «УМНОГО ГОРОДА»

И. Б. Паращук[1], **А. А. Чечулин**[1,2]

[1]Санкт-Петербургский Федеральный исследовательский центр Российской академии наук
[2]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Предложен подход к формальному описанию признаков уязвимостей в интерфейсах беспилотной транспортной среды «умного города» с целью идентификации угроз. Данный подход базируется на методе решения задач идентификации объектов и процессов в условиях нечеткости их наблюдаемых признаков. Этот метод ориентирован на устранение нечеткости (как одного из видов неопределенности) идентификации уязвимостей интерфейсов такого класса. Он основан на использовании нечетких и лингвистических переменных при обработке нечетких знаний о характеристиках потенциальных уязвимостей. Решение подобных задач позволит повысить достоверность контроля защищенности интерфейсов, повысить безопасность систем управления беспилотным транспортом.

умный город, интерфейс, беспилотные транспортные средства, уязвимость, нечеткие множества, лингвистическая переменная.

К программно-аппаратным интерфейсам беспилотной транспортной среды (БТС) «умного города» в современных условиях предъявляются жесткие требования по защищенности. Это связано, как с бурным развитием беспилотных средств частного и общественного транспорта (метро, автобусы, такси, дроны), беспилотных средств вспомогательной автотехники (для уборки дорог, вывоза мусора), так и с постоянно растущими возможностями потенциальных нарушителей по реализации уязвимостей БТС [1].

При этом важную роль, с точки зрения уязвимостей и их эксплуатации нарушителями в интересах снижения защищенности данных, циркулирующих в контуре управления БТС «умного города», играют интерфейсы взаимодействия типа «человек – искусственный интеллект». Являясь немаловажным компонентом современных БТС «умного города», интерфейсы типа «человек – искусственный интеллект» (ИИ) создаются, как правило, путем симбиоза программно-информационной среды и конкретных физических объектов. Поэтому они требуют повышенного внимания с точки зрения выполнения требований по защищенности от актуальных угроз информационной безопасности.

Специфика исследования механизмов информационной безопасности человеко-машинных интерфейсов взаимодействия заключается, как в уникальности самих интерфейсов – совокупности средств, методов и правил взаимодействия (управления, контроля и т. п.) между ИИ, БТС и иными элементами транспортной среды «умного города», так и в относительной новизне физических и программных уязвимостей, присущих объектам такого класса.

Более того, появляющиеся новые классы этих уязвимостей пока мало изучены, опыт защиты интерфейсов БТС от нарушений, эксплуатирующих эти уязвимости, невелик. Вместе с тем, подавляющее большинство решений по выявлению уязвимостей в системах такого класса принимается в условиях неопределенности (нечеткости) наблюдаемых данных о признаках таких уязвимостей. Именно поэтому актуальными, на наш взгляд, являются задачи, связанные с разработкой алгоритмов нечеткой идентификации (выявления, обнаружения и категорирования) уязвимостей в интерфейсах беспилотной транспортной среды «умного города».

Задачи идентификации (обнаружения и категорирования) аномальных данных, характеризующих атрибуты («симптомы») потенциальных «дыр» в безопасности интерфейсов БТС в условиях нечеткости наблюдаемых признаков таких уязвимостей, могут быть решены на основе понятий, методов и алгоритмов обработки нечетких множеств [2, 3].

При этом возможные признаки уязвимостей интерфейсов БТС детально описаны в работах [4, 5]. С учетом этого, идентификация (обнаружение и категорирование) в условиях нечеткости может быть осуществлена для пяти основных групп (классов) нечетко заданных признаков уязвимостей интерфейсов БТС: $\tilde{\tilde{\chi}}_{\text{код}}$ – нечетко заданные (наблюдаемые) признаки уязвимостей кода – уязвимости, появившиеся в процессе разработки программного обеспечения для интерфейсов БТС; $\tilde{\tilde{\chi}}_{\text{конф}}$ – нечетко заданные признаки уязвимостей конфигурации – уязвимости, появившиеся в процессе задания конфигурации (настройки) программного обеспечения и технических средств интерфейсов БТС; $\tilde{\tilde{\chi}}_{\text{арх}}$ – нечетко заданные признаки уязвимостей архитектуры (появившиеся в процессе проектирования интерфейсов БТС; $\tilde{\tilde{\chi}}_{\text{орг}}$ – нечетко заданные признаки организационных уязвимостей, появившихся как результат отсутствия (недостатка) организационных мер защиты интерфейсов БТС, а также $\tilde{\tilde{\chi}}_{\text{мфу}}$ – нечетко заданные признаки многофакторных уязвимостей, появившаяся в результате наличия комбинации нескольких рассмотренных ранее угроз интерфейсам БТС.

Идентификация нечетко заданных (наблюдаемых) признаков уязвимостей интерфейсов БТС осуществляется с целью их однозначного, достовер-

ного (объективного) обнаружения и категорирования. Иными словами, конечной целью является отнесение угроз и уязвимостей (по результатам идентификации их признаков), например, к опасной, не очень опасной или не опасной категории. Это, по сути, определение, являются ли эти уязвимости критичными (с набольшей степенью опасности) для интерфейсов БТС, или нет. Причем, степень опасности конкретного типа уязвимости рассматривается как некая сравнительная мера, характеризующая подверженность интерфейсов БТС этой уязвимости и ее влияние на нарушение свойств безопасности данных, циркулирующих в рамках интерфейса взаимодействия БТС «умного города».

С точки зрения задач идентификации (выявления, обнаружения и категорирования) уязвимостей интерфейсов взаимодействия БТС в условиях нечеткости исходных данных, предлагается подход, использующий понятия, методы и алгоритмы описания и обработки нечетких множеств. Этот подход позволит учитывать субъективные факторы, вносимые администратором (аудитором) безопасности БТС «умного города» при определении уровня критичности (опасности) угроз и уязвимостей интерфейсов такого класса. Метод идентификации уязвимостей интерфейсов БТС в условиях нечеткости исходных данных должен реализовывать процедуру обработки большого количества нечетко наблюдаемых признаков таких угроз и уязвимостей, а также опираться на мнения, суждения и разнообразные, нечеткие (чаще всего, экспертные) знания о степени негативных последствий в случае успешной эксплуатации таких уязвимостей потенциальными нарушителями.

Описание нечетко заданных идентификационных атрибутов («симптомов») потенциальных «дыр» в безопасности интерфейсов БТС представляет собой формальное описание таких объектов и явлений с помощью нечетких множеств и состоит в определении тех признаков уязвимостей, которые позволяют относительно достоверно считать эти угрозы и уязвимости принадлежащими, например, к опасной, не очень опасной или не опасной категории. Это описание можно осуществить посредством представления знаний о степени (глубине, уровню) принадлежности признаков уязвимостей к конкретному типу. При этом должны учитываться экспертные знания, которые могут быть представлены как в количественной (числовая переменная), так и в лингвистической форме. Экспертные нечеткие знания применяются и обрабатываются, опираясь на числовую меру и на семантический и синтаксической смысл понятий, используемых экспертом для выделения из всего множества признаков угроз и уязвимостей тех признаков, которые, на его взгляд, характеризуют критичные (наиболее опасные) угрозы и уязвимости.

Рассмотрим некоторые аспекты применения понятий, методов и алгоритмов обработки нечетких множеств в задачах идентификации (обнаруже-

ния и категорирования) уязвимостей интерфейсов БТС в условиях нечеткости. При описании с помощью нечетких множеств объектов и явлений в задачах идентификации уязвимостей, предлагается использовать известные понятия нечеткой и лингвистической переменных, а также нечетких чисел. При этом описывается нечеткая переменная, например, для нашей задачи, для нечетко заданного признака уязвимости $\widetilde{\widetilde{\chi}}_{\text{код}}$ – «высокий уровень угрозы с использованием уязвимости программного кода интерфейса БТС». Эта нечеткая переменная характеризуется тремя значениями, которые в теории нечетких множеств называют «кортежем» [2, 3]:

$$< x, U, \widetilde{C} > . \tag{1}$$

Тем самым, с помощью выражения (1) на основе кортежа $< x, U, \widetilde{C} >$ может быть описана нечеткая переменная, где x – название переменной; U – универсальное множество, область определения переменной x ; множество $\widetilde{C}$ – нечеткое множество на U, описывающее нечеткое ограничение на значения переменной u, обусловленное x [3]:

$$\widetilde{C} = \bigcup_{u \in U} u \,|\, \mu_u . \tag{2}$$

При этом множество $\widetilde{C}$ в теории нечетких множеств принято называть функцией совместимости нечеткой переменной. Данное множество описывает семантику нечеткой переменной, причем переменная u является для x базовой переменной. Множество $\widetilde{C}$ определяет ту степень (глубину), с которой элементу x соответствует значение u, при этом значения нечеткой переменной есть числа. В рамках задачи идентификации уязвимостей интерфейсов БТС, как это принято в теории нечетких множеств, лингвистической переменной будем называть кортеж [3]

$$< x, T(x), U, G, M >, \tag{3}$$

где x – название переменной, характеризующей степень (глубину, уровень) принадлежности признаков уязвимости интерфейсов БТС к конкретному типу критичных (наиболее опасных) угроз и уязвимостей; $T(x)$ – терм-множество, характеризующее названия лингвистических значений x из универсального множества U – области определения переменной x; G – синтаксическое правило, описывающее процесс получения новых значений лингвистической переменной; M – семантическое правило, позволяющее ставить каждой нечеткой переменной x ее смысл M [x].

В задачах идентификации уязвимостей интерфейсов БТС дожны быть различимы числовые и нечисловые лингвистические переменные, причем лингвистическая переменная называется числовой, если ее область определения U есть подмножество из R_1, т. е., из взята множества вещественных чисел. Примером нечисловой лингвистической переменной может служить переменная «опасная», формализующая понятие «опасная уязвимость интерфейсов БТС» со значениями «не очень опасная», «опасная», «очень опасная», «очень-очень опасная».

В качестве иного примера может быть рассмотрена числовая лингвистическая переменная «стоимость реализации уязвимости» – описывает финансовые последствия эксплуатации конкретной уязвимости нарушителем. Она может быть описана следующим образом:

< стоимость реализации уязвимости интерфейса БТС T, [0, 1], G, M >, (4)

где T = {«невысокая стоимость», «высокая стоимость», «очень высокая цена потерь»}; G – процедура перебора элементов из T; M – ограничения, обусловленные значениями из T и определяющие смысл лингвистических значений. Это семантическое правило, позволяющее ставить каждой нечеткой переменной x ее смысл M [x], может быть записано в виде ограничений по стоимости в денежных единицах (потерях, например, в долларовом эквиваленте), например для M [невысокая стоимость] [2, 3]:

$$M\,[\text{невысокая стоимость}] = \begin{cases} \dfrac{1}{1+0{,}01(u-200)^2}, & u \geq \$200; \\ 0, & u > \$500. \end{cases} \qquad (5)$$

Таким образом, описан пример, характеризующий применение теории нечетких множеств для решения задач достоверной идентификации уязвимостей интерфейсов БТС в условиях нечеткости наблюдаемых значений признаков этих уязвимостей. Предпринята попытка показать, что процедуры идентификации признаков уязвимостей интерфейсов БТС «умного города» могут быть удобно и достоверно описаны формально с использованием нечетких и лингвистических переменных.

Это позволяет устранить неопределенность (типа нечеткость) исходных данных, имеющую место при решении задач описания и идентификации признаков уязвимостей интерфейсов БТС в реальных условиях. В конечном итоге, это позволяет повысить достоверность (объективность) контроля защищенности современных систем «умного города», где БТС, где активно внедряется и применяется.

Работа выполнена при финансовой поддержке РФФИ (проект 19-29-06099) в СПб ФИЦ РАН (СПИИРАН).

Список используемых источников

1. Sladkowski A., Pamula W. (Eds.) Intelligent transportation systems – problems and perspectives (Vol. 32). Springer International Publishing, 2016. 303 p.
2. Shahbazova S.N., Sugeno M., Kacprzyk J. Recent Developments in Fuzzy Logic and Fuzzy Sets: Dedicated to Lotfi A . Zadeh. Springer, 1st. ed. 2020. 211 p.
3. Паращук И. Б., Бобрик И. П. Нечеткие множества в задачах анализа сетей связи. СПб.: ВУС, 2001. 80 с.
4. Виткова Л.А., Израилов К.Е., Чечулин А.А. Классификация уязвимостей интерфейсов транспортной инфраструктуры умного города // Актуальные проблемы инфотелекоммуникаций в науке и образовании. IX Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4 т. СПб.: СПбГУТ, 2020. Т. 1. С. 253–258.
5. Паращук И. Б., Чечулин А. А. Защищенность человеко-машинного интерфейса для интеллектуальной транспортной среды // Перспективные направления развития отечественных информационных технологий (ПНРОИТ-2020): Материалы VI межрегиональной научно-практической конференции. Севастополь, 22–26 сентября 2020 г. / Севастопольский государственный университет. Науч. ред. Б. В. Соколов. Севастополь: СевГУ, Т. 1, 2020. С. 65–66.

УДК 004.056.53
ГРНТИ 81.93.29

К ВОПРОСУ ОБНАРУЖЕНИЯ АНОМАЛИЙ В СИГНАЛЬНОМ ТРАФИКЕ НА ОСНОВЕ ИНТЕЛЛЕКТУАЛЬНОГО АНАЛИЗА ДАННЫХ

М. С. Пахомов, Д. В. Сахаров

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В данной работе представлены методы интеллектуального анализа данных по обнаружению аномалий в сигнальном трафике 5G. Проведен эксперимент по генерированию аномалий в сигнальном трафике, разработаны подходы и алгоритмы детектирования аномалий. Проведен сравнительный анализ и сформированы выводы об эффективности приведенных методов для решения поставленной задачи.

сигнальный трафик, анализ данных, машинное обучение, информационная безопасность, обнаружение аномалий.

Введение

В настоящее время активное развитие инфокоммуникационных систем и новых поколений связи, в частности 5G, только сильнее обостряет вопрос информационной безопасности (ИБ) и повышает требования к мониторингу

сетевых компонентов сетей [1, 2]. С течением времени инфокоммуникационные системы всё больше усложняются, в связи с этим, становится труднее анализировать трафик и детектировать аномалии. Также вопрос обнаружения аномалий в сигнальном трафике напрямую связан с тем, что с каждым новым поколением связи увеличивается поток, объем и скорость передаваемых пакетов данных [3], например, в пятом поколении связи скорость передачи достигает 20 Гбит/с.

Анализ

Классификация причин аномалий

Аномальное поведение трафика представляет собой отклонение от нормы общей закономерности передаваемого трафика. Возникновение аномалий в сигнальном трафике может иметь различные причины. Аномалии могут быть связаны, например, с неисправностью сетевого телекоммуникационного оборудования, деятельностью хакеров, осуществляющих атаки, ошибками в программном обеспечении (рис. 1) и сами по себе могут не иметь видимых признаков, но при этом приводить к фатальным сбоям [4].

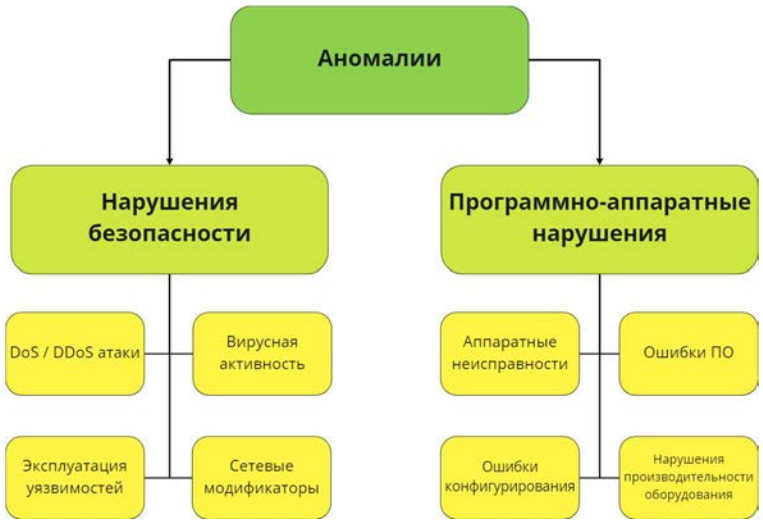


Рис. 1. Классификация причин аномалий трафика

Существующие методы детектирования аномалий и атак, как правило, основаны на сигнатурном анализе [5]. Данный подход не может позволить обнаруживать новые, не встречавшиеся ранее атаки и не способен детектировать распределенные во времени атаки. Преимущество использования практик искусственного интеллекта и методов интеллектуального анализа данных заключается в адаптации моделей и алгоритмов к различной «природе» данных и новым условиям, а именно в способности к обобщению результатов и их проецирования на новые ситуации и сценарии [6].

Сценарии возникновения аномального поведения

С точки зрения возникновения аномального поведения сигнального трафика 5G можно выделить множество сценариев его побуждающих. Рассмотрим два из таких сценариев:

- *Сценарий 1*: UE захвачен и повторно отправляет запросы передачи сигналов;
- *Сценарий 2*: вредоносные UE инициируют множество handover-запросов, вызывая большое количество сигнальных взаимодействий.

Основными объектами взаимодействия в данных сценариях являются пользовательское устройство (UE) и точки доступа радиосети (NG-RAN – New Generation Radio Access Network). При этом, в первом сценарии взаимодействие данных объектов сети обеспечивается по интерфейсу N1, во втором – по интерфейсу N2.

Создание наборов данных с аномалиями

В статистике существует два основных способа к определению аномалий (выбросов) в выборках: (1) метод трёх сигм, (2) межквартильный метод.

Метод трёх сигм (1). Пусть $\exists \{x_i\}^n \; \forall i \in \mathbb{N}$, при этом $\overline{x} = \frac{x_1+x_2+\ldots+x_n}{n}$ – среднее данного ряда, $\sigma = \sqrt{\frac{1}{n-1}\sum_{i=1}^{n}(x_i - \overline{x})^2}$ – стандартное отклонение. Если $|x_i - \overline{x}| > 3 \cdot \sigma$, то x_i – аномалия данного ряда $\{x_i\}^n$.

Как видно из распределения на рис. 2, 99,73 % данных выборки лежат в интервале 3σ. В соответствии с данным подходом, все значения, лежащие за пределами 3σ допустимо интерпретировать как аномальные.

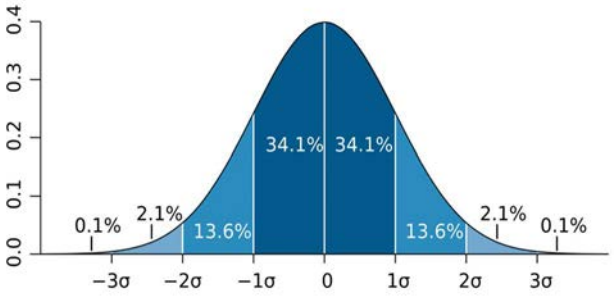


Рис. 2. Правило трёх сигм

Межквартильный метод (2). Данный метод основан на понятии межквартильного размаха (IQR – *Interquartile Range*), который вычисляется $IQR = Q_3 - Q_1$, где Q_1 и Q_3 – первый и третий квартили распределения, соответственно. Пусть, как и в (1) $\exists \{x_i\}^n \; \forall i \in \mathbb{N}$, тогда $x_{min} = Q_1 - 1.5 \cdot IQR$, $x_{max} = Q_3 + 1.5 \cdot IQR$. Если $x_i < x_{min}$ или $x_i > x_{max}$, то x_i – аномалия данного ряда $\{x_i\}^n$ (рис. 3).

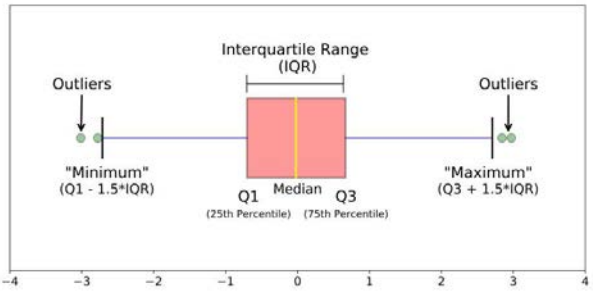
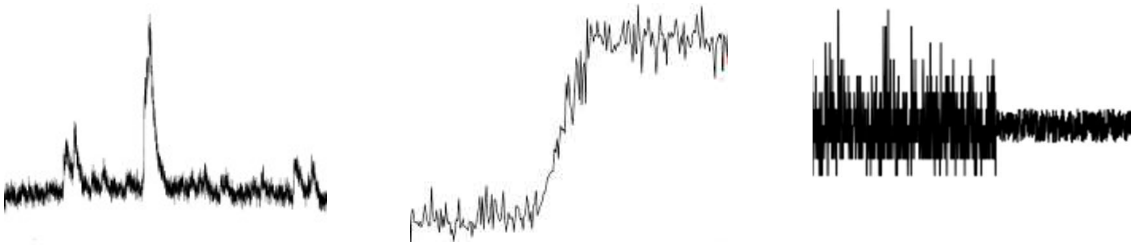


Рис. 3. Межквартильный метод

Используя методы (1) и (2) были сгенерированы аномалии сигнального трафика, путем искажения количества пакетов с сообщениями для которых ответ обязателен (Сценарий 1) и путем частого инициирования пакетов с сообщениями handover-запросов (Сценарий 2). Во временной области аномалии могут быть представлены в виде пиковых отклонений от линии тренда (рис. 4 а), сдвига (рис. 4 б), вариативности распределения (рис. 4 в).



а) б) в)

Рис. 4. Представление аномалий во временной области

Подходы к обнаружению аномалий

Классификация подходов к обнаружению аномалий, предлагаемая в настоящей работе представлена в виде условной схемы на рис. 5.

Рис. 5. Классификация методов обнаружения аномалий

В результате изучения релевантных работ [7–10] и анализа, примененных в них решений, было решено рассмотреть следующие методы для детектирования аномалий:

- Авторегрессионный анализ (модель ARIMA);
- Кусочно-линейную аппроксимацию;
- Алгоритмы градиентного бустинга (модель XGBoost);
- Рекуррентные нейронные сети (архитектура LSTM).

Сравнительный анализ реализованных подходов

Для сравнения подходов обнаружения аномалий в сигнальном трафике был произведен анализ работы данных методов (табл. 1). Сравнительный анализ был построен на основе метрик: полнота (recall), точность (precision), а также по времени обучения алгоритма и времени работы алгоритма для трафика из 1 000 пакетов.

ТАБЛИЦА. Сравнительная характеристика методов обнаружения аномалий

	ARIMA	Аппроксимация	XGBoost	LSTM	Аппроксимация + XGBoost
Recall	0.914	0.962	0.959	0.975	0.987
Precision	0.881	0.995	0.934	0.990	1.000
Время обучения, с	10.3	1.1	1320.0	10800.0	1322.0
Время работы, с	1.2	0.8	1.2	1.4	1.2

Исходя из сравнения результатов в таблице, можно сделать заключение, что лучшая по всем критериям – комбинированная модель на основе кусочно-линейной аппроксимации и XGBoost.

Заключение

В данной статье были рассмотрены различные подходы к обнаружению аномалий в сигнальном трафике 5G и после сравнительного анализа выделен самый робастный из них.

Список используемых источников

1. Березина Е. О., Виткова Л. А. Модель угроз IoT в программно-конфигурируемых сетях // Актуальные проблемы инфотелекоммуникаций в науке и образовании. IX Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4 т. СПб.: СПбГУТ, 2020. С. 130–134.

2. Виткова Л. А., Махова И. О., Сахаров Д. В. Исследование технологий пакетного транспорта в гибридной среде SD-WAN // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VI Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4 т. СПб.: СПбГУТ, 2017. С. 156–160.

3. Проничев А. П., Виткова Л. А. Разработка архитектуры децентрализованной системы анализа сетевого трафика // В сборнике: Информационная безопасность регионов россии (ИБРР-2019). Материалы конференции. Санкт-Петербург, 2019. С. 546-548.

4. Ahmad I., Kumar T., Liyanage M., Okwuibe J., Ylianttila M., Gurtov, A. (2018). “Overview of 5G Security Challenges and Solutions”.

5. Muhammad Junaid Nazar, Adi Alhudhaif, Kashif Naseer Qureshi, Saleem Iqbal, Gwanggil Jeon. Signature and flow statistics based anomaly detection system in software-defined networking for 6G internet of things network, 2021, International Journal of System Assurance Engineering and Management.

6. Jani Suomalainen, Arto Juhola, Shahriar Shahabuddin, Aarne Mämmelä, Ijaz Ahmad. Machine Learning Threatens 5G Security // IEEE Access. 2020.Vol. 8. pp. 190822–190842,

7. Lorenzo Fernández Maimó, Ángel Luis Perales Gómez, Félix J. García Clemente, Manuel Gil Pérez, Gregorio Martínez Pérez, A Self-Adaptive Deep Learning-Based System for Anomaly Detection in 5G Networks // IEEE Access. 2018. Volume 6. pp. 7700–7712.

8. Mingyan Teng. Anomaly detection on time series. 2010, IEEE International Conference on Progress in Informatics and Computing.

9. Christian Callegari, Sandrine Vaton, Michele Pagano. A new statistical method for detecting network anomalies in TCP traffic, European transactions on telecommunications. 2010. Vol. 21. N. 7. pp. 575–588,

10. Pankaj Malhotra, Lovekesh Vig, Gautam Shroff, Puneet Agarwal, Long Short-Term Memory Networks for Anomaly Detection in Time Series // ESANN 2015, pp. 89–94.

УДК 621.372.54
ГРНТИ 49.03.13

СИСТЕМА МОНИТОРИНГА И ПАСПОРТИЗАЦИИ ВОЛОКОННО-ОПТИЧЕСКОЙ ИНФРАСТРУКТУРЫ СЕТЕЙ СВЯЗИ ОБЩЕГО ПОЛЬЗОВАНИЯ НА ОСНОВЕ ИНТЕРФЕРОМЕТРИЧЕСКИХ МЕТОДОВ

А. С. Пермяков, И. Ю. Смирнов

Военная орденов Жукова и Ленина Краснознаменная академия связи
имени Маршала Советского Союза С. М. Буденного

В данной работе рассмотрен вопрос организации мониторинга и паспортизации волоконно-оптической инфраструктуры в сетях связи общего пользования. Предлагаемый авторами вариант по развитию системы мониторинга и паспортизации направлен на повышение информированности лиц, принимающих управляющие решения, о состоянии волоконно-оптической инфраструктуры сетей связи общего пользования.

сети связи общего пользования, волоконно-оптические линии связи, инфраструктура мониторинг, паспортизация, интерферометр, база данных.

Развитие современных инфотелекоммуникационных сетей связи операторов связи связано с постоянным ростом объемов циркулирующих данных. Постоянный обмен данными происходит не только между абонентами, но и между телекоммуникационными устройствами [1, 2]. Развитие технологии сетей мобильной и фиксированной связи и рост трафика сети Интернет представлен на рис. 1.

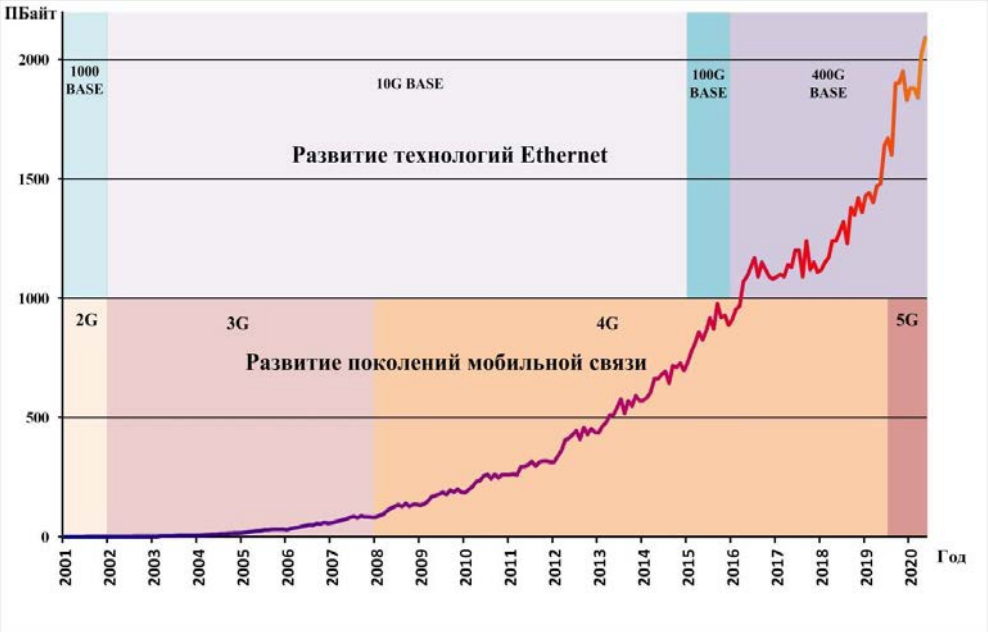


Рис. 1. Развитие технологии сетей мобильной
и фиксированной связи и рост трафика сети Интернет

На настоящее время средой передачи, обеспечивающей пропускную способность такого объема информации с минимальными задержками и искажениями, является только оптическое волокно [3]. Сравнение максимальной скорости передачи данных различных поколений сотовой связи с возможностями передачи данных различными родами связи представлено на рис. 2.

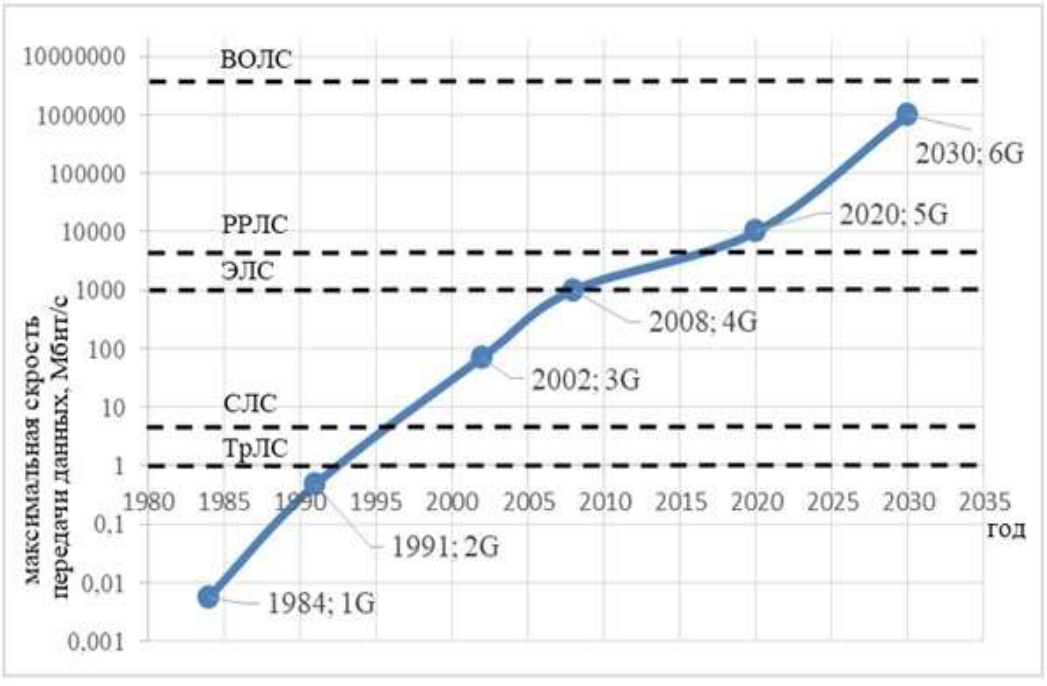


Рис. 2. Развитие технологии сетей мобильной
и фиксированной связи и рост трафика сети Интернет

Постоянное увеличение пропускной способности ведет к тому, что преобладающей транспортной средой передачи трафика в настоящее время являются волоконно-оптические линии связи (ВОЛС) [4, 5].

Эксплуатация ВОЛС, проложенных в земле, часто вызывает необходимость точного определения трассы прокладки кабеля. Основными методами обнаружения трассы закладки полностью диэлектрических оптических кабелей (ОК), проложенных в земле, является размещение рядом с кабелем металлического проводника (ленты) или специальных маркеров [6]. Однако, все эти методы обладают явным недостатком – зависимостью точности определения трассы прокладки от состояния металлических маркерных элементов.

В последнее время для поиска трасс прокладки ВОЛС применяют интерферометрические методы. Данные методы основаны на применении когерентных рефлектометров [7], построенных, наиболее часто на основе двулучевых интерферометрических схем (Маха – Цандера, Майкельсона). Двулучевые интерферометрические схемы регистрируют изменение интерферометрической картины из-за изменения фазы одного из оптических сигналов (рис. 3). Когерентное излучение (1), выходящее из лазера (Л), расщепляется на два идентичных луча: опорный (2) и измерительный (3). Каждый из лучей проходит различное расстояние, что создает разность фаз между ними. Перед попаданием на фотодетектор (ФД) лучи сводятся в суммарный (4). При совпадении лучей по фазе пики обоих лучей усиливают друг друга, если не совпадают - гасятся, в зависимости от расхождения фаз.

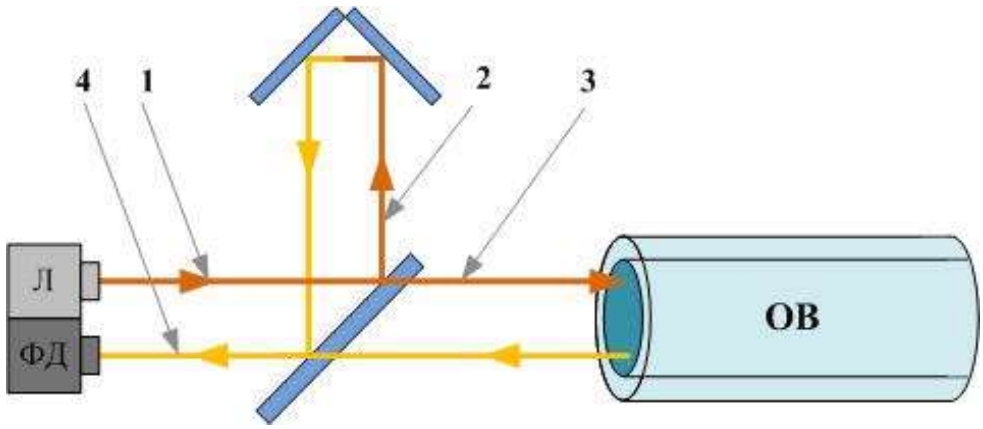


Рис. 3. Интерферометр Майкельсона

Применение когерентного рефлектометра и программно-аппаратного комплекса, с возможностью учета и хранения получаемых характеристик в единой базе данных, позволит усовершенствовать систему мониторинга состояния ВОЛС и паспортизации волоконно-оптической инфраструктуры (ВОИ) операторов связи сети связи общего пользования. Вариант системы мониторинга и паспортизации ВОИ представлен на рис. 4.

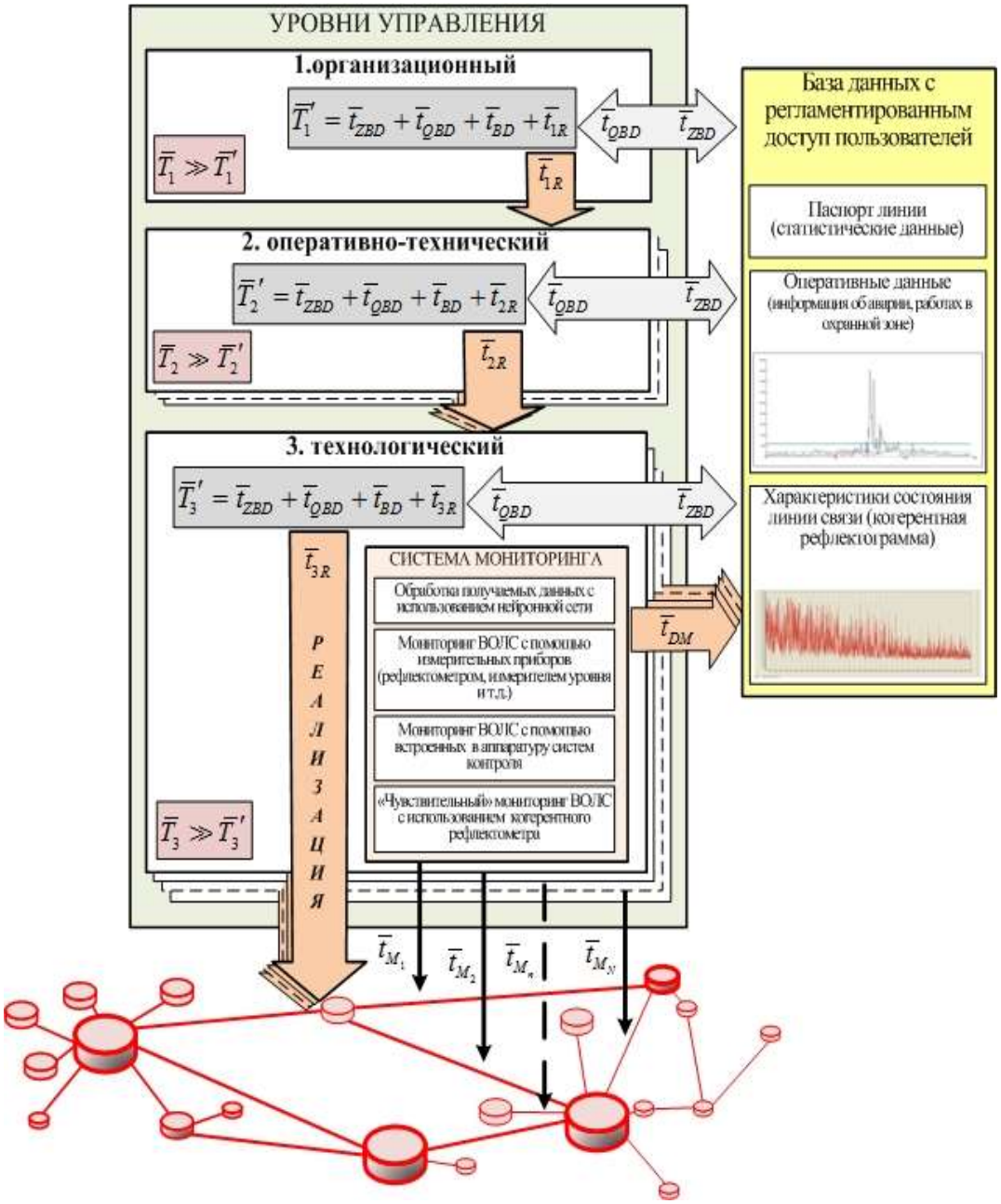


Рис. 4. Графическое представление предлагаемой системы мониторинга и паспортизации ВОИ

На рис. 4 $\overline{T}_1', \overline{T}_2', \overline{T}_3'$ – среднее время прохождения всего цикла управления на организационном, оперативно-техническом и технологическом уровне соответственно, при предлагаемом построении системы мониторинга и паспортизации;

$\overline{t}_{1Z}, \overline{t}_{2Z}$ – среднее время, затрачиваемое на запрос на организационном и оперативно-техническом уровне управления;

$\overline{t}_{2Q}, \overline{t}_{3Q}$ – среднее время, необходимое на ответ от оперативно-технического и технологического уровня управления;

$\overline{t}_{Ds}$ – среднее время, необходимое для обработки имеющихся данных;

$\overline{t}_{DQ}$ – среднее время, необходимое для обработки данных, получаемых по запросу;

$\overline{t}_{DM}$ – среднее время, затрачиваемое на обработку полученных данных мониторинга;

$\overline{t}_{ZBD}$ – среднее время, затрачиваемое на запрос к БД;

$\overline{t}_{QBD}$ – среднее время, необходимое на ответ БД;

$\overline{t}_{BD}$ – среднее время, затрачиваемое на обработку полученных данных из БД;

$\overline{t}_{M1}, \overline{t}_{M2}, ..., \overline{t}_{MN}$ – среднее время мониторинга состояния ВОИ.

В предлагаемом варианте построения системы мониторинга и паспортизации (рис. 4, см. ниже) с внедрением единой БД, содержащей статические и динамические параметры ВОИ, среднее время, затрачиваемое на получение необходимых данных на каждом уровне, будет одинаковым:

$$\overline{t}_{1D}{}' = \overline{t}_{2D}{}' = \overline{t}_{3D}{}' = \overline{t}_{ZBD} + \overline{t}_{QBD}$$

и среднее время, требуемое для анализа данных и принятия решения:

$$\overline{t}_{1p} = \overline{t}_{2p} = \overline{t}_{3p} = \overline{t}_{BD}$$

что позволит существенно уменьшить время прохождения всего цикла управления на каждом уровне управления ВОИ операторов связи ССОП.

Таким образом, применение в системе мониторинга и паспортизации ВОИ операторов связи ССОП когерентных рефлектометров – интерферометров, позволит существенно уменьшить время получения достаточного объема данных, необходимого для принятия управляющего решения, а регистрация обработанных результатов измерения в логически единой территориально распределенной БД обеспечит сокращения цикла управления ВОИ на различных уровнях принятия управляющего решения о состоянии ВОИ.

Список используемых источников

1. Закалкин П. В. Эволюция систем управления киберпространством // Вопросы кибербезопасности. 2022. № 1 (47). С. 76–86.

2. Иванов С. А. Устойчивость сетей связи общего пользования в условиях глобализации // Известия Тульского государственного университета. Технические науки. 2021. № 9. С. 86–90.

3. Степутин А. Н., Николаев А. Д. Мобильная связь на пути к 6G. М.: Инфра-Инженерия, 2021. Т. 1. 384 с.

4. Иванов С. А., Закалкин П. В., Иванов С. А. Состояние и достижения волоконно-оптической связи в России // Состояние и перспективы развития современной науки по направлению «Информационная безопасность»: сборник статей II Всероссийской научно-технической конференции. Федеральное государственное автономное учреждение «Военный инновационный технополис «ЭРА». Анапа, 2020. С 285–291.

5. Иванов С. А., Смирнов И. Ю., Федоров П. Н. Расчет волоконно-оптического делителя мощности на основе фазоконтурных схем замещения // Актуальные проблемы инфотелекоммуникаций в науке и образовании. X Международная научно-техническая и научно- методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2021. С. 240–245.

6. Соколов С. А. Волоконно-оптические линии связи и их защита от внешних влияний: учебное пособие. М.: Инфра-Инженерия, 2019. 172 с.

7. Дашков М. В., Смирнов А. С. Поляризационная рефлектометрия оптических волокон: физические основы, методы и приложения (обзорная статья) // Прикладная фотоника. 2018. Т 5. № 1-2. С. 62–91.

Научный руководитель
Заслуженный деятель науки, доктор военных наук, профессор Ю. И. Стародубцев.

УДК 004.056
ГРНТИ 81.93.29

МЕТОДИКА ПРОТИВОДЕЙСТВИЯ УГРОЗАМ НАРУШЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИНСТАНСОВ И ОБЛАЧНОЙ ИНФРАСТРУКТУРЫ, ОСНОВАН НА ОПИСАНИИ АТАК И МЕТОДОВ ПРОТИВОДЕЙСТВИЯ ИМ, ИСПОЛЬЗУЯ ТЕОРИИ ГРАФОВ

И. Е. Пестов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Методики противодействия угрозам нарушения информационной безопасности на сегодняшний день приобретают все большую популярность, так как автоматизирование данного процесса значительно снизит время реакции на атаку и как следствие время простоя информационной системы [1]. Простой информационной системы влечет не только финансовые потери, но и репутационные, что недопустимо для организации любого типа.

информационная безопасность, анализ атак, теория графов, противодействие угрозам.

Анализ стабильности работы информационной системы проводится на основе параметров, отображенных на рис. 1, каждый из которых включает отдельные характеристики (коэффициенты). Таким образом, выделено 12 коэффициентов, по которым будет проводиться анализ состояния системы. Присвоение оценочных значений каждому из них производится по следующему правилу: состояние параметра системы определено в двоичной системе, где 0 – допустимое значение параметра, 1 – значение, отличное от заданного при стабильной работе системы.

В процессе анализа состояния системы, в случае её нестабильной работы, первостепенно определяется параметр, а после – коэффициент, значением которого обусловлена нестабильность работы.

Для определения методики выявления угрозы и выявления путей её решения, была использована теория графов.

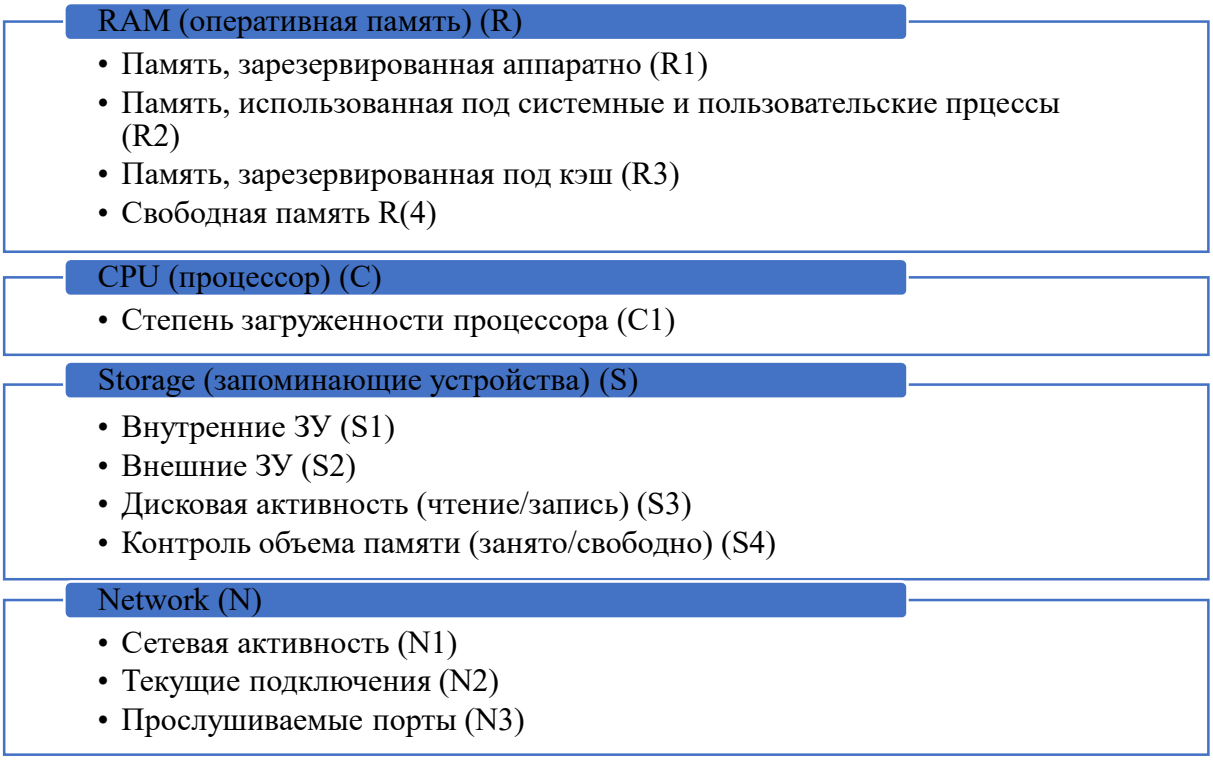


Рис. 1. Параметры информационной системы

Обход графа в ширину использует очередь для отслеживания необработанных соседних вершин. Этот алгоритм обхода графа применяется для поиска компонент связности в графе. Поиск начинается с определенной вершины, обозначенной как начальная, которая обрабатывается, маркируется и

помещается в очередь. После того, как начальная вершина обработана, промаркирована и помещена в очередь, начинается выполнение основной части алгоритма обхода графа в ширину. Основой алгоритма является циклический процесс, в котором обработанная вершина удаляется из очереди, а в очередь помещаются соседствующие с обработанной вершины. Таким образом, тело цикла состоит из двух основных шагов:

- Удалить вершину из головы очереди;
- Для каждой непомеченной вершины, соседней по отношению к предшествующей вершине, обработать данную вершину, маркировать ее и поместить в очередь.

Эти действия выполняются до тех пор, пока очередь не станет пустой.

Обход графа в глубину применяется в различных расчётах на графах. Одним из ярких примеров является алгоритм Диница для поиска максимального потока в транспортной сети. Алгоритм обхода графа в глубину начинает выполнение также с вершины, обозначенной начальной, фиксирует информацию о посещении этой вершины, и, перемещаясь по ребрам, посещает соседние вершины поочередно. По завершении обхода все вершины окажутся пройдёнными – обработанными.

Используем алгоритм обхода графа в глубину для исследования состояния информационной системы, соответственно взяв за основу ориентированный граф.

Составим граф, позволяющий рассмотреть пути принятия решений соответствующей системой. Каждая вершина графа является значением параметров системы в момент проведения исследования. Благодаря этому возможно наглядное представление, каким или какими из четырёх главных параметров обусловлено отклонение системы от стабильного состояния. Граф представлен на рис. 2.

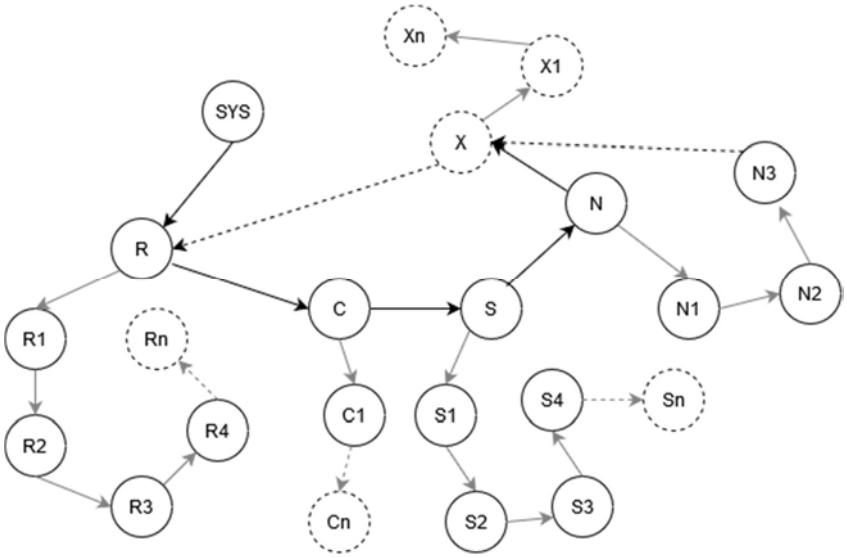


Рис. 2. Общий граф принятия решений

Анализируя граф состояния можно однозначно точно определить тип атаки: переполнения буфера [2], вирусная атака [3], отказ в обслуживании [4].

Данный граф можно описать следующим образом:

$$SYS = K_1 \cup K_2 \cup K_3 \cup \ldots \cup K_n$$

где K – выделенный параметр, n – количество параметров.

При этом:

$$K_i = k_1 \cup k_2 \cup k_3 \cup \ldots \cup k_x$$

где k_i – характеристика параметра, x – количество характеристик параметра.

При прохождении каждой вершины, значение в ней фиксируется. При повторном прохождении через вершину (возвращении в вершину), записанное ранее значение остается неизменным.

Связи между характеристиками, относящимися к разным параметрам, также возможны, но они выстраиваются по мере полноты системы. В работе представлен более обобщенный граф, который можно применить к любой системе. Также стоит учитывать, что количество обрабатываемых параметров и связей между ними влияет на быстродействие системы.

Началом графа обозначим состояние информационной системы на текущий момент. После обработки начальной вершины, алгоритмом выполняется переход к соседней вершине. Далее алгоритмом проводится проверка основных параметров поочередно. При выявлении аномалии в параметре выполняется переход к характеристикам параметров, после обработки которых осуществляется возврат к параметру, после чего осуществляется переход к следующему параметру системы. После проверки параметров, имеющих коэффициент, равный «1», алгоритм переходит к проверке оставшихся параметров и их характеристик.

Данный алгоритм позволит свободно варьировать список проверяемых параметров и их характеристик по требованиям системного администратора: добавлять новые значения, а также исключать невостребованные. Чем больше параметров и характеристик устанавливается для проверки состояния системы, тем точнее происходит дальнейшее определение аномалии.

После прохождения всего графа производится анализ всех полученных характеристик (коэффициентов) с целью выявления проблемных – имеющих логическое значение «1» и их количества.

По итогам выявления всех проблемных характеристик, система принятия решений обращается к базе знаний, содержащей характеристики существующих угроз и методы их устранения.

После проведения сравнения информации из базы знаний с текущими оценочными коэффициентами, система принятия решений составляет список возможных угроз, осуществляющихся в данный момент. На основании этого списка принимаются меры по устранению всех угроз, максимально соответствующих описанию и отмеченных значением «1».

По итогам успешного принятия мер по противодействию угрозам, система принятия решений уведомляет системного администратора о проведённых манипуляциях, состоянии системы, на основании которого эти манипуляции проводились, а также предлагает варианты стабилизации работы информационной системы, в случае необходимости.

В случае, когда система сталкивается с угрозой, отсутствующей в базе знаний, или не может идентифицировать однозначно ситуацию, производится автоматическое отключение устройства от общей сети, а также формируется информационное уведомление о неизвестной угрозе с описанием параметров системы на данный момент. Необходимо отметить, анализируемых инстансов облачной инфраструктуры возможно большое количество, такое что потребуются технологии анализа больших данных[6].

Список используемых источников

1. Волкогонов В. Н., Гельфанд А. М., Деревянко В. С. Актуальность автоматизированных систем управления // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VIII Международной научно-технической и научно-методической конференция : сб. науч. ст. в 4 т. СПб. : СПбГУТ, 2019. С. 262–266.

2. Суворов А. М., Цветков А. Ю. Исследование атак типа переполнение буфера в 64-х разрядных Unix подобных операционных системах // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2018. С. 570–573.

3. Штеренберг С. И., Красов А. В., Цветков А. Ю. Компьютерные вирусы. Ч. 1. СПб.: СПбГУТ, 2015. 62 с.

4. Гельфанд А.М., Косов Н.А., Красов А.В., Орлов Г.А. Защита для распределенных отказов в обслуживании в облачных вычислениях // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VIII Международной научно-технической и научно-методической конференцияи : сб. науч. ст. в 4 т. СПб. : СПбГУТ, 2019. С. 329–334.

5. Красов А. В., Штеренберг С. И., Голузина Д. Р. Методика визуализации больших данных в системах защиты информации для формирования отчетов уязвимостей // Электросвязь. 2019. №. 11. С. 39–47.

Статья представлена заведующим кафедрой ЗСС СПбГУТ, кандидатом технических наук, доцентом А. В. Красовым.

УДК 004.414.22
ГРНТИ 50.01

АНАЛИЗ АРХИТЕКТУРЫ ВИРТУАЛЬНОЙ МАШИНЫ

И. Е. Пестов, З. А. Федорова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Архитектура виртуальной машины определяет ее использование, пользовательские и технические параметры. Виртуализация – основной инструмент разработки компьютерных систем. Появляются архитектурные элементы с новыми или улучшенными характеристиками. Виртуальные машины: преимущества и недостатки.

виртуальные машины, виртуализация, гипервизор, операционная система.

Основные возможности применения виртуальной машины (ВМ), ее технические и пользовательские параметры – все это в значительной степени определяется архитектурой ВМ – ее структурой и принципами построения.

ВМ – это абсолютная копия стандартного компьютера, с требуемой операционной системой (ОС) и рядом установленных программ. Виртуальной машиной можно управлять так же, как физическим сервером или настольным компьютером. Для этого нужно просто подключиться, а для доступа к ВМ использовать специальные сервисы или консоль, предоставляемую облачным провайдером [1, 2]. Главное – иметь доступ к сети и учетную запись с соответствующими правами. Составляющими ВМ являются: память, процессор, виртуальный жесткий диск, видеокарта и другие компоненты. В возможности самостоятельного управления ресурсами ВМ заключается привлекательность виртуализированного подхода: за считаные секунды можно уменьшить или увеличить используемые ресурсы по мере необходимости [3, 4].

Концепция виртуальных машин является наиболее естественным и полным проявлением принципа виртуальности. В качестве средства выделения ресурсов и организации управления процессами по определенным правилам каждая операционная система фактически скрывает реальное оборудование и другие ресурсы от пользователя и приложений, заменяя их абстракцией [5].

В большинстве случаев ВМ копирует конфигурацию реального компьютера, но в этом представлении архитектурные элементы появляются с новыми или улучшенными свойствами и значительно облегчают работу с системой. Параметры могут отличаться, но пользователи хотят получить «идеальную» машину с учетом архитектурных особенностей:

– виртуальная оперативная память неограниченного объёма;

– способные к одновременной работе и взаимодействию любое количество виртуальных процессоров;

– произвольное число внешних (виртуальных) устройств, которые могут работать как параллельно, так и последовательно с памятью ВМ, как асинхронно, так и синхронно с действиями того или иного виртуального процессора, инициирующего работу этих устройств [6].

Степень приближенности к «идеальной» виртуальной машине может быть больше или меньше в каждом случае. Чем больше ВМ, реализованная операционной системой на базе конкретного оборудования, приближается по своим показателям к «идеальной», и чем сильнее ее архитектурные и логические характеристики отличаются от реальных, тем больше достигнутая степень виртуальности. Одним из проявлений виртуализации является организация в данной ОС возможности запуска приложений, разработанных для других операционных систем и это дает преимущество перед похожими ОС, не обладающими такой способностью.

Виртуализация является значимым механизмом разработки компьютерных систем, и ВМ применяются начиная с ОС и заканчивая языками программирования [7, 8]. Освобождая программистов и простых пользователей от ограниченности ресурсов и нарушений интерфейса, ВМ повышают эксплуатационную гибкость аппаратной платформы, улучшают совместимость программного обеспечения (ПО) и снижают уязвимость системы.

Когда создается виртуальная машина, ей присваивается набор виртуального оборудования по умолчанию. У нее есть BIOS, выделенное дисковое пространство, сетевые адаптеры для подключения к реальной машине, другим ВМ или сетевым ресурсам.

Архитектура системы, использующей виртуальные машины, упрощенно выглядит так:

– права контроля над аппаратными компонентами компьютера разделяют монитор ВМ и хостовая ОС, которая распределяет ресурсы между собственными приложениями (включая консоль ВМ);

– монитор виртуальной машины управляет распределением ресурсов между запущенными машинами, создавая видимость доступа к аппаратному уровню напрямую;

– гостевые ОС контролируют работу «своих» приложений в рамках выделенных им ресурсов.

Физическое устройство, на котором работает ВМ, называется хостом, а ВМ – гостевой. В конкретной ВМ гостевая ОС хранится на виртуальном жестком диске – большом файле размером в несколько гигабайт, который находится на реальном жестком диске. Приложение ВМ представляет этот файл гостевой ОС как настоящий жесткий диск.

Гостевую ОС и ее приложения можно настраивать и обновлять по мере необходимости, а также устанавливать или удалять новые приложения, не затрагивая хост или другие ВМ.

ВМ работает, как компьютер и изолирована от остальной части хост-системы. ПО в гостевой системе не может вносить изменения в ПО хост-системы. Таким образом, вирусные файлы можно тестировать с помощью ВМ, не затрагивая основную компьютерную систему. Благодаря использованию виртуальных машин реальный компьютер защищен от любых непреднамеренных действий со стороны пользователей: приложение, запущенное на виртуальной машине, не может нанести вред другим приложениям и реальной ОС. Так решается проблема безопасности [9].

Описанная выше архитектура является очень общей, но доступные сегодня на рынке системы ВМ имеют значительные различия, в основном из-за механизма виртуализации. Системы ВМ могут использовать отличные технологии и строиться на разных платформах. Схема виртуализации зависит от поддерживаемой гостевой ОС, аппаратной платформы и особенностей ОС хоста. Некоторые архитектуры позволяют осуществлять виртуализацию на аппаратном уровне, в то время как другие требуют дополнительных программных технологий [10].

Гипервизором называется создающее и запускающее виртуальные машины компьютерное ПО. Он является неотъемлемой частью системы и делает виртуализацию возможной [11].

Гипервизор – это платформа виртуализации, которая позволяет запускать несколько операционных систем на одном физическом компьютере. Именно гипервизор создает изолированную среду для каждой ВМ и предоставляет ОС ВМ доступ к аппаратному обеспечению реального компьютера.

ВМ, как и другие программы, состоит из набора файлов, хранящихся на жестких дисках физического сервера, в системе гипервизора. Количество файлов может варьироваться в зависимости от конкретной реализации, но ядром каждой ВМ является один и тот же базовый набор: файл конфигурации ВМ и виртуальный жесткий диск. В зависимости от состояния и конфигурации ВМ не все файлы могут присутствовать в каталоге ВМ.

Существует несколько типов файлов, которые связаны с виртуальной машиной и составляют её. Эти файлы расположены в каталоге ВМ в хранилище данных. Также для каждой ВМ создана отдельная папка с её именем, которое присваивается самим пользователем в процессе установки виртуальной ОС.

Описание файлов, из которых состоит ВМ:

– файл конфигурации (<имя ВМ>.vmx) – главный файл, в котором хранятся все параметры ВМ. Это важный файл, содержащий описание эмулируемого оборудования и ресурсов, выделенных ВМ реальным компьютером.

– файл BIOS (<имя ВМ>.nvram) – файл состояния и настроек BIOS ВМ. ВМ должна знать, сколько у нее жестких дисков и другие общие настройки BIOS. Если файл удалить, то он будет восстановлен с настройками по умолчанию при следующем включении ВМ.

– файлы журнала (vmware.log или <имя ВМ>.log) – файл журнала ключевой активности. Он используется для устранения неполадок, в случае их возникновения.

– файл подкачки (<имя ВМ>.vmem) – появится только в том случае, если ВМ запущена или в ней произошел сбой;

– файл диска (<имя ВМ>.vmdk) – файл виртуального диска, в котором хранится содержимое жесткого диска ВМ;

– файл данных моментального снимка (<имя ВМ> .vmsd) – файл, в котором хранится информация и метаданные о снимках.

Знание характеристик различных архитектурных решений позволяет пользователям ВМ оперативно управлять всеми предоставляемыми средствами, делая целенаправленный выбор и тем самым повышая эффективность обработки данных.

Виртуализация меняет способ организации и использования информационной инфраструктурой. Мощный сервер теперь можно разделить на множество виртуальных серверов с собственными разделенными ресурсами. Это позволяет каждому пользователю запускать приложения и собственную ОС. Объем оперативной памяти и ресурсов предоставляется по мере необходимости, кроме того, всегда доступны резервные копии, а если виртуальный сервер выйдет из строя, можно переключиться на другой.

Таким образом, среди неоспоримых преимуществ ВМ:

1. Удобство создания резервной копии ОС.

2. Для перехода на другую операционную систему не нужна перезагрузка.

3. Возможность иметь неограниченное количество ВМ с различными ОС и их состояниями на одном компьютере.

4. Одновременная работа в нескольких системах.

5. Виртуализация ОС, аппаратного обеспечения приложений, систем хранения данных и серверов.

6. Возможность сделать «моментальный снимок» текущего состояния и затем вернуться в него.

Недостатки виртуальных машин можно описать следующим образом:

1. Потребность в достаточном оборудовании для единовременного функционирования нескольких ОС.

2. Работа операционной системы в ВМ медленнее, чем на обычном компьютере.

В настоящее время для организации взаимодействия между прикладными программами, аппаратным обеспечением и операционными системами активно используются виртуальные машины. Можно предположить, что на основе технологий ВМ будут разрабатываться все новые архитектуры, языки программирования и ОС [12].

Список используемых источников

1. Билятдинов К. З., Красов А. В., Меняйло В. В. Теория информационных процессов и систем: учебное издание, Санкт-Петербург, 2019.

2. Гольдштейн Б. С. Инфокоммуникационные сети и системы. СПб.: БХВ-Петербург, 2019. 208 с.

3. Коржик В. И., Красов А. В., Сахаров Д. В., Владыко А. Г., Штеренберг С. И. Основы научных и экспериментальных исследований. СПб.: СПбГУТ, 2019. 80 с.

4. Туманов Д. С. Технологии виртуализации / Федер. агентство связи, ГОУВПО «СПбГУТ им. проф. М. А. Бонч-Бруевича» // Научно-техническая конференция профессорско-преподавательского состава, научных сотрудников и аспирантов, 63-я (21-25 февр. 2011 г.): материалы. Ч. 1. СПб.: СПбГУТ, 2011. С. 246–247.

5. Котенко И. В., Саенко И. Б, Кушнеревич А. Г. Архитектура системы параллельной обработки больших данных для мониторинга безопасности сетей Интернета вещей // Труды СПИИРАН. 2018. № 4 (59). С. 5–30.

6. Гультяев А. К. Виртуальные машины: несколько компьютеров в одном: учебник. Санкт-Петербург: Издательский дом «Питер», 2006. 224 с.

7. Коржик В. И., Кушнир Д. В. Теоретические основы информационной безопасности телекоммуникационных систем: учебное пособие. СПб.: СПбГУТ, 134 с.

8. Красов А. В. Основы информационных технологий. Опорный конспект лекций. СПб.: Изд-во СПбГУТ, 2007. 56 с.

9. Кушнир Д. В. Теоретические основы информационной безопасности телекоммуникационных систем: учеб. пособие. СПб.: СПбГУТ, 2004.

10. Сахаров Д. В., Левин М. В., Фостач Е. С., Виткова Л. А. Исследование механизмов обеспечения защищенного доступа к данным, размещенным в облачной инфраструктуре // Наукоемкие технологии в космических исследованиях Земли. 2017. Т. 9, № 2. С. 40–46.

11. Красов А. В., Штеренберг С. И., Голузина Д. Р. Методика визуализации больших данных в системах защиты информации для формирования отчетов уязвимостей // Электросвязь. 2019. № 11. С. 39–47.

12. Кушнир Д. В. Информационное общество. Инфокоммуникации и бизнес: учебник / под ред. Ю. В. Арзуманяна. СПб.: СПбГУТ, 2005. 480 с.

УДК 004.4'242
ГРНТИ 50.41.17

АНАЛИЗ ПОДХОДОВ К РАЗРАБОТКЕ ОБЛАЧНЫХ СЕРВИСОВ

И. Е. Пестов, Р. О. Христофоров, А. А. Швидкий

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В данной статье представлены результаты исследования подходов к разработке облачных сервисов. В рамках исследования были решены следующие задачи: рассмотрены ключевые модели облачных, проанализированы подходы проектированию архитектуры приложения и методам разработки облачного программного обеспечения.

облачные сервисы, облачная инфраструктура, инструменты разработки.

Облачные сервисы предлагают удобные модели предоставления вычислительных услуг через интернет. Причина, по которой пользователи и компании все чаще выбирают облачное программное обеспечение заключается в простоте и удобстве пользования сервисом из любой точки мира почти на любом устройстве. Вместе с этим возрастает сложность с обеспечения отказоустойчивости приложений, а также с поддержкой инфраструктурной (серверной) стороны сервиса.

Существует 3 основные модели обслуживания облачных сервисов, представленные Национальным институтом стандартов и технологий США [1]: SaaS, PaaS и IaaS. На сегодняшний день к ним добавилось множество других моделей, такие как FWaaS (*Firewall as a service*), KaaS (*Kubernetes as a service*), GaaS (*Game as a service*) и другие. Все они так или иначе входят в группу SaaS, PaaS, IaaS, поэтому в статье будет рассмотрена каждая из основных моделей (рис. 1).

IaaS (*Infrastructure as a Service*) – Инфраструктура как услуга. Заключается в предоставлении пользователям в аренду вычислительных ресурсов в виде виртуальной и физической инфраструктуры, в которую могут входить серверы, системы хранения данных, коммутаторы, маршрутизаторы.

PaaS (*Platform as a Service*) – Платформа как услуга. Она заключается в предоставлении инструментов и сервисов. Такую платформу клиент может использовать, например, для автоматического тестирования программного обеспечения.

SaaS (*Software as a Service*) – Программное обеспечение как услуга. Самая распространенной в мире, так как с ней взаимодействуют практически

все пользователи сети интернет. Заключается услуга в предоставлении пользователям программных продуктов. Такими продуктами могут быть почтовые сервисы, программы для обмена сообщениями, программы для редактирования документов.

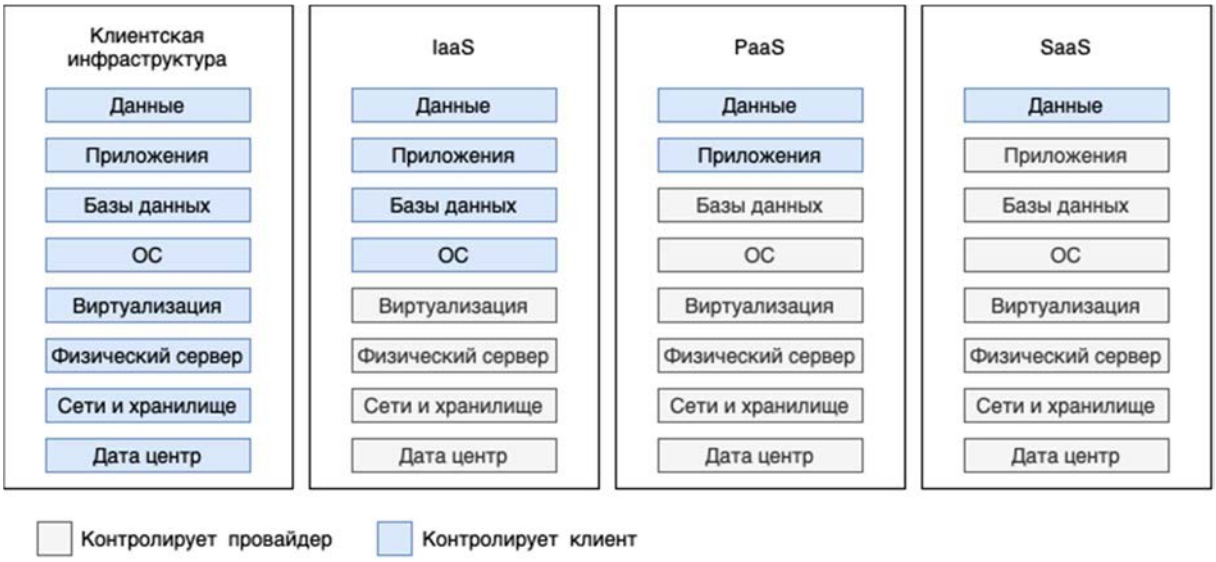


Рис. 1. Модели предоставления облачных сервисов

Для построения архитектуры облачного сервиса следует рассмотреть основные подходы к проектированию облачного программного обеспечения. Для того чтобы выбрать правильную архитектуру следует оценить: область применения облачного сервиса, комплексность будущего приложения, навыки команды разработки. Это создает определенные особенности в выборе технологий, в структуре приложения, в будущем масштабировании приложения. Основными подходами определяют монолитную (единую) и микросервисную (слабосвязянную) архитектуру.

«Монолитная» архитектура (рис. 2) подразумевает наличие общей и единой платформы, на основе которой запущены и взаимодействуют между собой все компоненты приложения. Все компоненты унифицированы. В ходе исследования были выведены следующие преимущества:

– простая разработка,

– простой запуск приложения,

– уменьшение проблем при проектировании взаимодействия модулей.

Недостатки:

– большой объем кода, который сложно модернизируется. В результате чего гибкость изменений сильно ограничена,

– компоненты приложения сложно масштабируются.

Микросервисная архитектура (рис. 2) – вариант архитектуры облачного программного обеспечения, направленный на взаимодействие насколько

это возможно небольших, слабо связанных и легко изменяемых модулей – микросервисов. Плюсы такого подхода:

– модули можно легко заменить в любое время,

– модули могут быть реализованы с использованием различных языков программирования,

– модули приложения легко масштабировать.

Минусы:

– сложности проектирования взаимодействия модулей,

– производительность, связанная с дополнительным слоем для взаимодействия модулей,

– сложность развертывания модулей приложения.

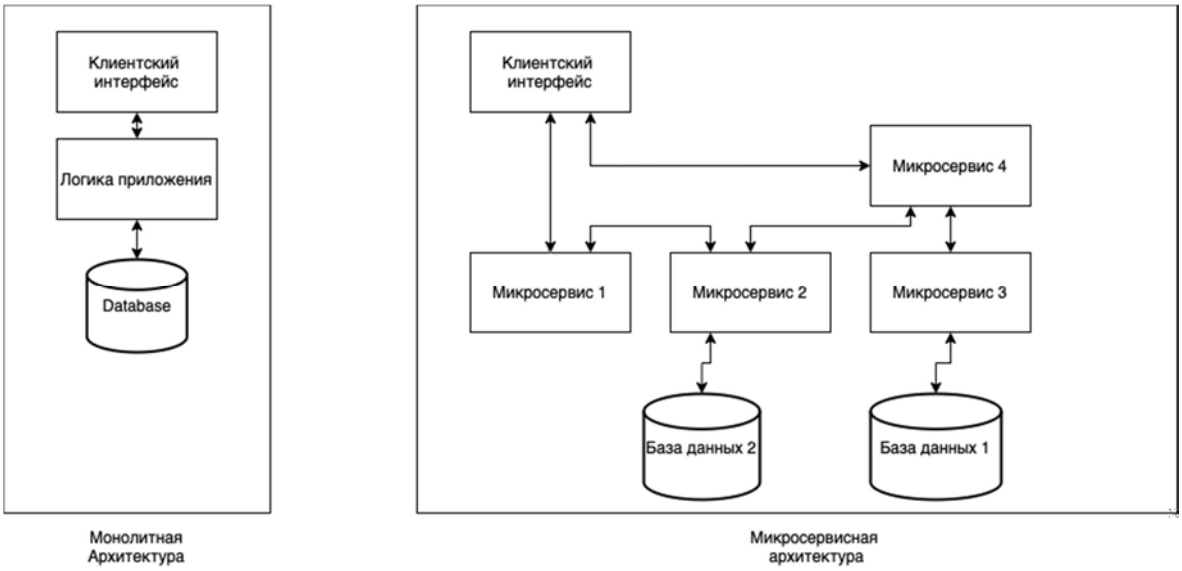


Рис. 2. Архитектура приложения

После определения модели и архитектуры сервиса рассматривается инфраструктурную часть приложения. Для правильного выбора серверной части сервиса необходимо определить какие ресурсы будут необходимы для корректной работы программного обеспечения, а также определиться запускать ПО на выделенном сервере, либо на виртуальном.

Выделенный сервер – отдельный физический сервер. Обычно используется для запуска приложений, которые не могут сосуществовать на одном сервере с другими проектами или имеют повышенные требования к ресурсам.

Виртуальный сервер – представляет из себя размещение сервера на физическом сервере с использованием технологии виртуализации. Самый распространённый вариант размещений ПО, подходит для приложений не требовательным к ресурсам, которые могут быть ограничены из-за использования слоя виртуализации.

Для любого приложения, которое работает в облаке, важно сохранять высокую доступность и обеспечить отказоустойчивость. В основе этих принципов всегда лежит дублирование компонентов облачного сервиса и исключении единой точки отказа (рис. 3). Уровень, на котором будет производиться дублирование определяет степень устойчивости к сбоям. Если сервис будет запущен на одном сервере, то это и будет единой точкой отказа, если разместить несколько дублирующих виртуальных серверов на одном физическом, то точкой отказа станет этот физический сервер, но если распределить приложение по нескольким физическим серверам в разных центрах обработки данных с несколькими сетевыми каналами, то единой точки отказа не будет. Чем более устойчива к отказам инфраструктура, тем она дороже, с точки зрения аренды или покупки серверов и оборудования, и тем сложнее она в обслуживании со стороны инженерных решений. Тем самым целесообразность подходов определяется индивидуально для каждого проекта.

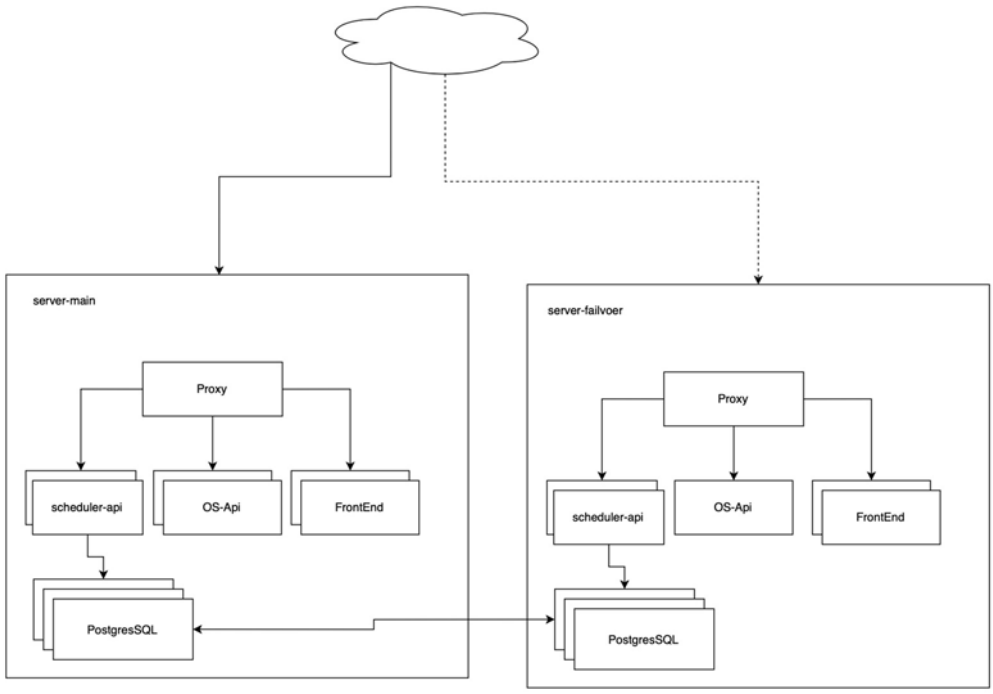


Рис. 3. Пример отказоустойчивой инфраструктуры облачного сервиса

Рассматриваются подходы к организации командной работы при разработке программного обеспечения, самым распространенным инструментом для увеличения производительности при написании кода является git.

Git [2] – утилита для ведения истории изменения исходного кода проекта, а также для конфигурационных файлов, картинок и прочих файлов. Точкой сохранения состояния файлов является коммит (commit). У каждой точки сохранения есть уникальных хэш и комментарий. Ветка – это цепочка

из точек сохранений. Репозиторий – хранилище веток, которое может быть как локальным, так и находящимся на удаленном сервере.

Это позволяет протестировать код в любой ветке и даже в любом доступном коммите, а также наблюдать за изменениями всех файлов проекта, чтобы вернуться в предыдущее состояние с случае ошибки. Когда разработка в отдельной ветке завершена, разработчик инициирует слияние точек сохранений (коммитов) между ветками (рис. 4).

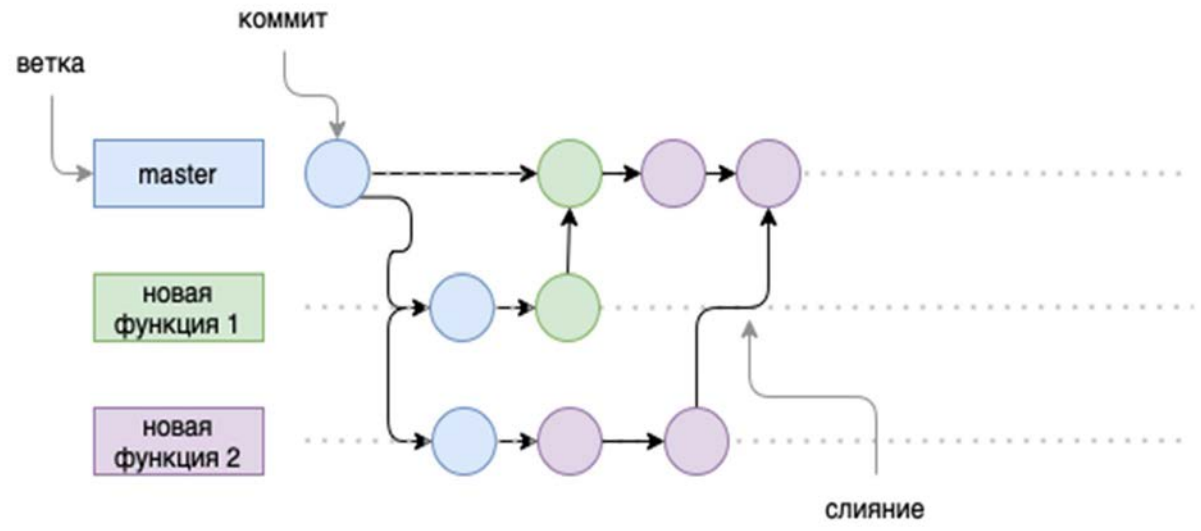


Рис. 4. Пример работы с инструментом git

Чтобы сократить время на сборку, тестирование кода, а также развертывание приложения используют набор принципов и практик непрерывной интеграции (*Continuous Integration*, CI) [3] и непрерывной поставки (*Continuous Delivery*, CD) [3]. Цель непрерывной интеграции обеспечить автоматизировать сборку, упаковку и тестирование кода. Непрерывная поставка начинается там, где сразу после непрерывной интеграции, она позволяет автоматизировать развертывание сервиса в различные окружения. Сборочные линии или Pipelines (рис. 5) – сконфигурированный цикл CI/CD, включающий в себя сборку, тестирование, развертывание приложения.

Рис. 5. Пример сборочный линии облачного сервиса

В статье проведено исследование основных подходов к разработке облачных сервисов на основе использования современных методов и практик. Рассмотрены возможные решения в области выбора архитектуры для облачного приложения, вариантов проектирования инфраструктурной части сервиса, а также инструментов и подходов для ускорения и повышения качества написания исходного кода приложения.

Список используемых источников

1. Peter Mell (NIST), Tim Grance (NIST) The NIST Definition of Cloud Computing. // NIST Special Publication 800-145. PP. 2–3.
2. Git about. URL: https://git-scm.com/about (дата обращения: 20.03.2022).
3. CI/CD concepts. URL: https://docs.gitlab.com/ee/ci/introduction/index.html #continuous -delivery (дата обращения: 20.03.2022)

Статья предоставлена заведующим кафедрой ИКС СПбГУТ, кандидатом технических наук, доцентом А. А. Зарубиным.

УДК 654.021
ГРНТИ 49.33.29

ГРАФИЧЕСКОЕ ИЗОБРАЖЕНИЕ МНОГОМЕРНЫХ ЗАВИСИМОСТЕЙ ПОКАЗАТЕЛЕЙ КАЧЕСТВА ОБСЛУЖИВАНИЯ ТРАФИКА ОТ ПАРАМЕТРОВ ЕГО РАСПРЕДЕЛЕНИЯ ПО НЕСКОЛЬКИМ МАРШРУТАМ

М. И. Рафальская

Военная орденов Жукова и Ленина Краснознаменная академия связи имени Маршала Советского Союза С. М. Буденного

Одним из механизмов обеспечения качества обслуживания трафика является его распределение по нескольким маршрутам. Рассматриваются способы наглядного графического изображения многомерных зависимостей показателей качества обслуживания трафика от параметров его распределения по нескольким маршрутам путем сведения этих зависимостей к функциям одного и двух аргументов.

многомерные графики, распределение трафика, качество обслуживания трафика.

Управление распределением трафика по нескольким маршрутам является одним из действенных механизмов повышения качества его обслуживания. При этом процедуры распределения трафика проявляются на стыке смежных уровней сетевой архитектуры в виде совместных решений о том,

какие доли ресурсов нижнего уровня использовать для обслуживания очередной порции данных верхнего уровня [1].

В качестве обобщенного показателя качества обслуживания трафика, передаваемого в некотором отдельном направлении связи по нескольким маршрутам $i = 1,..,n$, с интенсивностями потоков данных $\{\lambda_i\}_n$ и пропускными способностями $\{\mu_i\}_n$ обычно рассматриваются усредненные показатели качества обслуживания трафика в каждом из маршрутов:

$$Q = \sum_{i=1}^{n} \alpha_i \cdot Q_i(\lambda_i, \mu_i), \qquad (1)$$

где $Q_i(\lambda_i,\mu_i)$ – частный показатель качества обслуживания трафика в i-м маршруте; α_i – весовой коэффициент, в роли которого обычно выступает доля трафика, направляемого по i-му маршруту:

$$\alpha_i = \lambda_i \Big/ \sum_{j=1}^{n} \lambda_j = \lambda_i / \lambda,$$

где λ – суммарная интенсивность трафика в рассматриваемом направлении.

Функциональные зависимости $Q_i(\lambda_i,\mu_i)$ показателей качества обслуживания трафика в отдельных маршрутах от параметров их пропускной способности (канального ресурса) μ_i и трафика λ_i, как правило, являются нелинейными и существующими лишь в ограниченном диапазоне изменения аргументов, что затрудняет выбор метода решения задач оптимизации распределения потоков данных и канального ресурса по критерию минимума целевой функции (1), являющейся обобщенным показателем задержек и/или потерь пакетов, которые обычно стремятся уменьшить, чтобы выполнить требования к качеству обслуживания [2].

Важным средством предварительного анализа функциональных зависимостей (1) от управляемых параметров распределения трафика $\{\lambda_i\}_n$ и канального ресурса $\{\mu_i\}_n$ является графическое изображение этих зависимостей, которое позволяет наглядно представить эти зависимости и обнаружить их особенности, существенные для дальнейшего выбора метода строгого решения задачи оптимизации управления трафиком.

Однако графически на плоскости наиболее полно и точно можно представить функции только одного аргумента. Менее полно и точно можно представить функции двух аргументов, используя различные проекции трехмерного изображения таких функций на плоскость. Функции же трех и более аргументов в виде одного графического изображения представить вообще невозможно, но можно отображать по частям – в виде отдельных сечений и их проекций на плоскость с подходящей системой координат. При

этом наглядность и информативность подобного графического представления многомерных функциональных зависимостей существенно зависит от выбора указанных сечений, проекций и системы координат.

В настоящей статье рассматриваются способы наглядного графического отображения многомерных зависимостей показателей качества обслуживания трафика от параметров его распределения по нескольким маршрутам путем сведения к функциям одного и двух аргументов.

В качестве примера функции (1) далее рассматривается зависимость средней задержки T передачи пакетов по нескольким маршрутам $i = 1,..,n$, от соответствующих каждому маршруту долей $\{\alpha_i\}_n$ суммарной интенсивности потока данных λ и долей $\{\gamma_i\}_n$ суммарной пропускной способности μ, причем в каждом из маршрутов задержка T_i соответствует модели одноканальной системы массового обслуживания M/M/1 [3]:

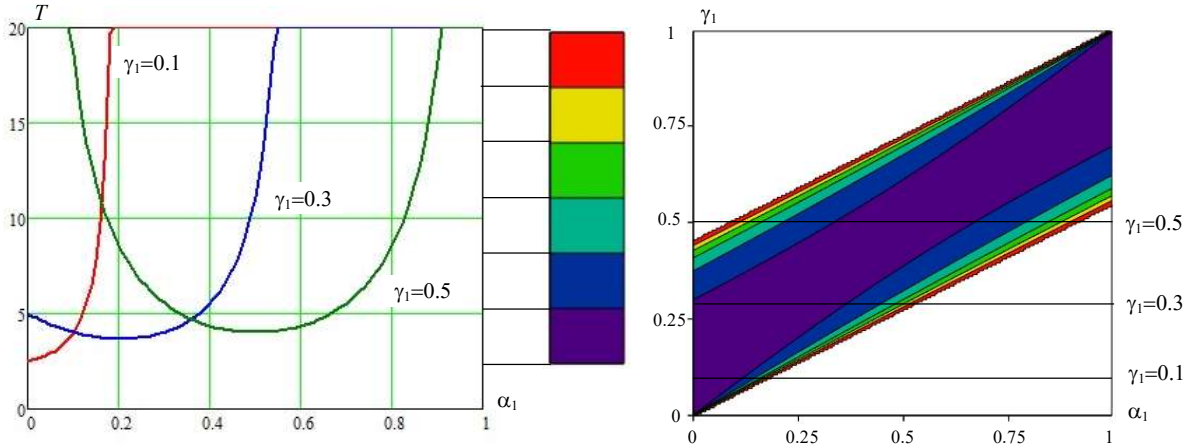
$$T(\{\alpha_i\}_n,\{\gamma_i\}_n,\lambda,\mu)=\sum_{i=1}^{n}\alpha_i\cdot T_i(\lambda\cdot\alpha_i,\mu\cdot\gamma_i)=\sum_{i=1}^{n}\frac{\alpha_i}{\mu\cdot\gamma_i-\lambda\cdot\alpha_i}. \qquad (2)$$

Как следует из выражения (2), в общем случае функция $T(\cdot)$ является многомерной и зависит от $2\cdot n + 2 > 2$ аргументов, т. е. графически представить зависимость $T(\cdot)$ от всех аргументов сразу невозможно.

Основными очевидными способами понижения размерности функции (2) являются: фиксация значений отдельных аргументов и учет их взаимозависимости. В данном случае фиксированные значения в первую очередь можно задать для неуправляемых (заданных) параметров интенсивности пакетов λ и пропускной способности μ. Очевидная взаимозависимость между собой долей $\{\alpha_i\}_n$ и отдельно долей $\{\gamma_i\}_n$ определяется их физическим смыслом, согласно которому их сумма должна равняться 1, а, следовательно, по одной доле из этих двух групп долей можно выразить через остальные. В итоге размерность функции (2) можно свести к $2\cdot(n - 1)$ аргументам. Но и это количество позволяет графически представить функцию (2) только при $n = 2$ и только в двумерном виде.

В случае, когда аргументами функции (2) выступают одна из долей $\{\alpha_1,\alpha_2\}$, например, α_1, соответственно, $\alpha_2 = 1–\alpha_1$, и одна из долей, $\{\gamma_1,\gamma_2\}$, например, γ_1, соответственно, $\gamma_2 = 1–\gamma_1$, функцию (2) можно также представить в виде набора графических зависимостей от одного аргумента α_1 или γ_1, задавая значения другого в виде нескольких дискретных значений. На рис. 1 для примера приведены зависимости $T(\alpha_1,\gamma_1)$ при $n = 2$, $\lambda = 0.5$, $\mu = 1$ в виде одномерной зависимости (рис. 1а) от одного аргумента α_1 при трех дискретных значениях второго аргумента γ_1 и двумерной зависимости (рис. 1а) от двух аргументов (α_1,γ_1) с дискретными значениями функции

$T(\alpha_1,\gamma_1)$, соответствующими границам цветных областей, согласованным с семью градациями задержек на вертикальной оси графика на рис. 1а.



а) б)

Рис. 1. Графическое изображение зависимостей обобщенного показателя задержки T от двух независимых параметров распределения трафика α_1 и канального ресурса γ_1 при использовании двух маршрутов

В другом случае, когда аргументами функции (2) выступают две из трех долей $\{\alpha_1,\alpha_2,\alpha_3\}$, например, α_1 и α_2, соответственно, $\alpha_3 = 1 - \alpha_1 - \alpha_2$, появляется возможность графического изображения зависимости показателей качества обслуживания от параметров распределения трафика между тремя маршрутами. На рис. 2 по аналогии с рис. 1 для примера приведены зависимости $T(\alpha_1,\alpha_2)$ при $n = 3$, $\lambda = 0.5$, $\mu = 1$, $\gamma_1 = 0.5$, $\gamma_2 = 0.3$, $\gamma_3 = 0.2$ в виде одномерной зависимости (рис. 2а) от одного аргумента α_1 при трех дискретных значениях второго аргумента α_2 и двумерной зависимости (рис. 2а) от двух аргументов (α_1,α_2) с дискретными значениями функции $T(\alpha_1,\alpha_2)$, соответствующими границам цветных областей, согласованным с семью градациями задержек на вертикальной оси графика на рис. 2а.

Некоторым неудобством анализа двумерных графических зависимостей показателя задержки T от двух параметров (α_1,α_2) является отсутствие возможности наглядного представления, как меняется и, соответственно, как влияет на величину данного показателя третий зависимый параметр $\alpha_3 = 1–\alpha_1–\alpha_2$. В предыдущем случае, когда рассматривалась зависимость T от одного параметра распределения трафика α_1, изменение и влияние зависимого параметра $\alpha_2 = 1–\alpha_1$ было очевидным – зеркально симметричным относительно графиков на рис. 1.

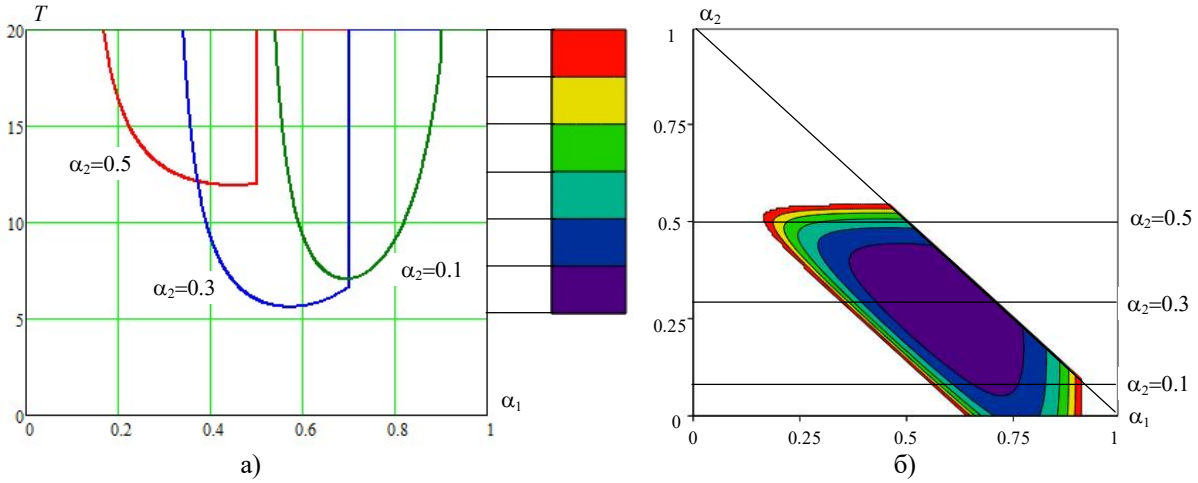


Рис. 2. Графическое изображение зависимостей обобщенного показателя задержки T от двух взаимозависимых параметров распределения трафика α_1 и α_2 при использовании трех маршрутов

Для построения симметричных графических зависимостей показателя задержки T относительно трех параметров распределения трафика (α_1,α_2,α_3) можно использовать следующее преобразование прямоугольной ортогональной системы двух координат (x,y) в косоугольную неортогональную систему трех координат (α_1,α_2,α_3):

$$\begin{cases} \alpha_1 = y, \\ \alpha_2 = 1 - 0.5 \cdot (y + x \cdot \sqrt{3}), \\ \alpha_3 = -y + 0.5 \cdot (y + x \cdot \sqrt{3}). \end{cases}$$

На рис. 3 приведены примеры графического изображения зависимостей обобщенного показателя задержки T от трех взаимозависимых параметров распределения трафика α_1, α_2 и α_3 в косоугольной неортогональной системе координат при использовании трех маршрутов для трех случаев распределения канального ресурса с постоянной долей $\gamma_1 = 0.5$ в первом маршруте и тремя вариантами долей канального ресурса во втором и третьем маршрутах. Причем первый вариант (рис. 3а) соответствует варианту на рис. 2 ($\gamma_2 = 0.3$, $\gamma_3 = 0.2$), а третий вариант является противоположным первому ($\gamma_2 = 0.2$, $\gamma_3 = 0.3$), что подтверждается симметричным изменением графика на рис. 3в относительно графика на рис. 3а. Второй вариант соответствует одинаковым значениям долей канального ресурса во втором и третьем маршруте ($\gamma_2 = 0.25$, $\gamma_3 = 0.25$), что подтверждается симметричным графиком на рис. 3б относительно долей трафика α_2 и α_3, направляемого по этим маршрутам.

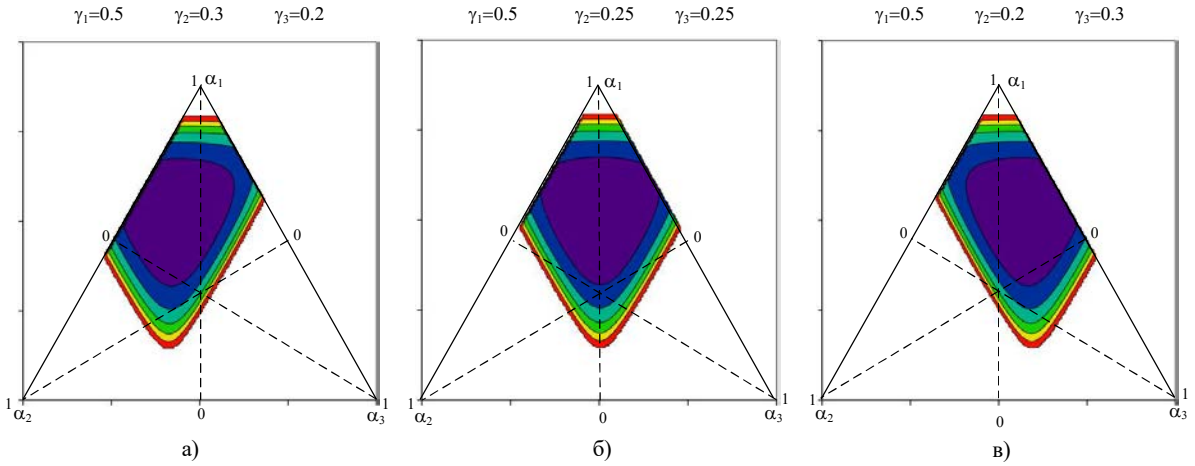


Рис. 3. Графическое изображение зависимостей обобщенного показателя задержки *T* от трех взаимозависимых параметров распределения трафика α_1, α_2 и α_3 в косоугольной неортогональной системе координат при использовании трех маршрутов

Таким образом, в настоящей статье рассмотрены способы графического изображения многомерных зависимостей показателей качества обслуживания трафика от параметров его распределения по нескольким маршрутам путем сведения этих зависимостей к функциям одного и двух аргументов. Приведены примеры, демонстрирующие возможность графического изображения зависимостей обобщенного показателя задержки от параметров распределения трафика и канального ресурса по двум и трем маршрутам с целью выявления особенностей данных зависимостей, существенных для дальнейшего выбора метода строгого решения задачи оптимизации управления трафиком.

Список используемых источников

1. Одоевский С. М., Яровикова О. В. Оптимизация управления распределением трафика на смежных уровнях сетевой архитектуры // Актуальные проблемы инфотелекоммуникаций в науке и образовании. III Международная научно-техническая и научно-методическая конференция: сб. науч. ст. СПб: СПбГУТ, 2014. С. 323–328.

2. Рекомендация МСЭ-Т Y.1541 (02/2006). Требования к сетевым показателям качества для служб, основанных на протоколе IP.

3. Крылов В. В., Самохвалова С. С. Теория телетрафика и её приложения. СПб.: БХВ-Петербург, 2005. 288 с.

Статья представлена научным руководителем, доктором технических наук, профессором С. М. Одоевским.

УДК 004.725.7
ГРНТИ 49.46.29

УЯЗВИМОСТИ ОПТИЧЕСКИХ КАНАЛОВ ПЕРЕДАЧИ ДАННЫХ

Б. К. Резников, Г. В. Степаненков, И. Ф. Тарабанов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В наше время все большую популярность приобретают системы связи с применением оптических каналов передачи данных. В данной статье обзорно рассмотрены основные уязвимости сетей с применением оптических технологий связи и возможные решения для выявления появляющихся угроз в системе связи.

оптические системы связи, защита информации, безопасность оптических систем передачи данных, уязвимость.

Перед изучением существующих уязвимостей волоконно-оптических систем связи можно перечислить их основные преимущества:

– Минимальное влияние побочных электромагнитных излучений и наводок;

– Высокая скорость передачи информации по каналу связи с минимальным коэффициентом ошибок (частота появления ошибочной информации меньше 10^{-10}, что дает большое преимущество для работы в сетях связи);

– Незначительны шумы оптического канала;

– Материалы для изготовления оптического кабеля, имеют в себе диэлектрические свойства, что в свою очередь увеличивает сложность нахождения такого кабеля, без точного понимания, где он был расположен;

– Долговечность, средний срок службы оптического кабеля составляет 25 лет.

В волоконно-оптических сетях связи основные действия нарушителя, направлены на воздействия на трафик (информацию), передаваемые по оптическим сетям, которые в свою очередь создают:

– Угрозу доступности передаваемой информации по каналам связи;

– Угрозу открытия информации несанкционированным лицам путем перехвата трафика;

– Угроза искажения передаваемой информации, путем ее фальсификации, искажения, подмены или уничтожения информации путем внедрения технических средств в канал связи.

Основные типы воздействий на волокно-оптические линиях связи можно разделить на:

– Тепловое воздействие;
– Радиационное воздействие;
– Электромагнитное поле;
– Акустическое излучение.

В цифровых каналах с бинарным кодированием чаще всего оценивается качество связи с помощью вероятности появления ошибочного бита BER (BIT Error Rate) [1], т. е. отношения числа неправильно распознанных битов к общему числу принятых битов за заранее определенный промежуток времени.

$$BER \simeq \frac{1}{2}\left[1 - erf(\frac{SNR}{2\sqrt{2}}\right],$$

– это функция ошибок, где в свою очередь

$$(x) = \frac{2}{\sqrt{\pi}}\int_0^x \quad exp\ exp\ (-t^2)\ dt.$$

Таким образом, при увеличении уровня шума в канале связи будет падать отношение сигнал\шум (SNR) и расти вероятность появления BER.

Шум в канале связи можно вычислять по формуле:

$$N = N_m + N_a = \eta S + N_A.$$

В этой формуле под N_M – мощность мультипликативных шумов (искажений), а N_A – мощность аддитивных шумов (помех), а S в свою очередь мощность полезного сигнала, основную роль играют мультипликативные шумы (искажения) N_M, а мощность аддитивных (помех) N_A стремятся к 0.

Вторая угроза конфиденциальности подразумевает под собой перехват трафика с помощью различных технических средств. Технический канал утечки информации для реализации перехвата на сети волокно-оптической линии зависит от множества факторов, таких как тип информативного сигнала (трафика), места перехвата, вида сети, и построенной инфраструктуры. Задача при защите информации состоит в анализе трафика на участке прохождения трафика в оптической линии (оптоволоконном кабеле, коммутационных узлах и на других элементах оптической сети [2]. Одной из самых сложных задач связаны не только с учетом трафика, но и с обработкой перехваченной информации и возвращением его исходный канал связи, из-за этого появляется необходимость созданием несанкционированного узла связи, такое действие возможно только при прямом подключении, такое действие очень сложно осуществить без прерывания в обслуживании линии, что могут обнаружить инженеры обслуживающие данную линию связи.

Рисунок. Внедрение в канал связи

Под перехватом трафика понимается неправомерное получение информации с помощью различных технических средств, осуществляющих обнаружения, обработку и прием трафика. Сценарий перехвата трафика разбивается на 5 основных этапов:

1. Выявление архитектуры и топологии сети, включающей выявление размещения кабеля, кабельной инфраструктуры, нахождение коммутационных узлов;

2. Определение типа оптического кабеля, волокна и выявления характерных неоднородностей кабельной системы, разъемных соединений и мест сварки, типа коммутационных элементов и его производителя;

3. Получения физического доступа к сети и подбор технических средств для подключения к волокну и реализации съема трафика с волокна;

4. Проведение мероприятий, направленных на повышение эффективности съема трафика с волоконно-оптической линии;

5. Регистрация сигнала утечки информации и осуществления перехвата трафика.

Во время перехвата информации в волоконно-оптических сетях, действия нарушителя и используемые средства в чаще всего опираются на вид телекоммуникационной сети (подземная, подводная, подвесная, городские коммуникации). Так в сетях абонентского доступа технические средства определяется расположением кабельных каналов, коммутационных элементов и топологией кабельной сети [3]. Прохождения трафика в виде оптического излучения по волокну может быть двумя способами:

– Непосредственный – подключение к оптической сети или получения вывода части оптического излучения:

  ○ Перехват с разрывом оптической линии и вставкой,

  ○ Перехват с доступ к волокну;

– Удаленный – регистрация проходящих оптических излучений и связанных с информационных полей в виде сопровождающих и побочных излучений:

  ○ Перехват с регистрацией побочных и сопутствующих эффектом,

  ○ Перехват на основе параметрических методов.

Стоит упомянуть, что возможности для удаленного съема трафика имеют ограничения. Для уверенного перехвата трафика требуется максимальная близость к оптическому каналу (менее 1 метра). Использование не оптических информативных полей без специальных воздействий затруднено. Из-за этого основным способом съема трафика чаще всего используют непосредственный съем информации с доступом к кабелю.

Также можно изменить доступ к каналу связи с помощью физического воздействия на кабель, так нагревание может вызвать изменение геометрических размеров кабеля, возникновение механических напряжений, изменение показателя преломления, коэффициентов поглощения, дисперсионных параметров волокна. Из-за этого происходит искажение сигнала и увеличение рассеивания излучения. Также стоит учитывать, что кабель может вернуть свои свойства после окончания на него воздействия.

Возможны изменения свойства кабеля с помощью воздействия на него гамма-излучения, что способствует появлению точечных дефектов, которые увеличивают количество потерь в оптическом волокне ведущие к потере пропускной способности. При больших потоках ядерных излучений появляются аддитивные помехи. Стоит упомянуть, что более критичным является долгое облучение малыми дозами, они вызывают больше потемнение, чем при более коротком облучении с такой же дозой. При таком типе воздействий реакция обратима и волокно возвращает свои свойства спустя некоторое время

Также возможно воздействие с помощью акустических волн, при использовании высоких частот акустическая волна вызывает рассеяние света вследствие акустооптического эффекта, при низких частотах механическое действие на кабель и волокно, вызывающее изменения геометрических параметров с помощью механических колебаний кабеля.

С помощью изменения электромагнитного поля можно вызвать появление оптической анизотропии, что приводит к искажению распространения света и дополнительному рассеянию света в волокне.

Также стоит упомянуть химическое воздействие на кабель, к примеру, проникновение воды в кабель неизбежно приводит к необратимому значительному росту потерь.

Список используемых источников

1. What is Bit Error Rate: BER tutorial // Electronics Notes. URL: https://www.electronics-notes.com/articles/radio/bit-error-rate-ber/what-is-ber-definition-tutorial.php (дата обращения: 02.12.2021).

2. Оптические каналы утечки информации // СёрчИнформ. URL: https://searchinform.ru/analitika-v-oblasti-ib/utechki-informatsii/sluchai-utechki-informatsii/opticheskie-kanaly-utechki-informatsii/ (дата обращения: 07.12.2021).

3. Гришачев В. В. Выявление угроз утечки речевой информации через волоконно-оптические коммуникации // Фотоника. 2011. № 4 (28). С. 32–39.

Статья представлена доцентом кафедры ЗСС СПбГУТ, кандидатом технических наук, доцентом Д. В. Кушниром.

УДК 004.657
ГРНТИ 50.41.21

АНАЛИЗ СИНХРОНИЗАЦИИ БАЗ ДАННЫХ В УСЛОВИЯХ ОТСУТСТВИЯ ДЕТЕРМИНИРОВАННЫХ ЗАПРОСОВ

И. Б. Саенко, А. В. Удальцов

Военная орденов Жукова и Ленина Краснознаменная академия связи
имени Маршала Советского Союза С. М. Буденного

В статье рассматриваются вопросы синхронизации баз данных в условиях отсутствия детерминированных запросов. Проведен анализ возможных видов синхронной репликации. Обоснованы условия выбора того или иного формата фиксации изменений в базу данных.

база данных, синхронизация, репликация.

С развитием информационных технологий и ростом объемов обрабатываемой информации во всех сферах деятельности все большую значимость приобретают распределенные автоматизированные информационные системы, в том числе облачные, в основе работы которых положено использование баз данных [1, 2]. По своей сути, базы данных – это структурируемые данные, которые собраны в одном или нескольких удаленных местах [3]. В распределенных базах данных информация хранится на различных компьютерах, соединенных коммуникационными сетями. В целях поддержания актуальности и согласованности распределенных баз данных выполняется процесс синхронизации баз данных, который принято называть репликацией. Репликация – это поддержание двух и более идентичных копий данных на разных узлах распределенной базы данных [4].

Реплика может включать всю базу данных (полная репликация), одно или несколько взаимосвязанных отношений (таблиц базы данных) или фрагмент отношения. Репликации различают:

по степени синхронизации – синхронная, асинхронная, комбинированная;

по количеству серверов записи – мастер-реплика, мастер-мастер;

по формату применения изменений – покомандная, построчная, комбинированная;

по модели передачи изменений – push («толкать»), pull («тянуть»).

При выборе варианта синхронной репликации проведем анализ покомандной (*Statement Based Replication*, SBR) и построчной (*Row Based Replication*, RBR) репликации.

Структура процесса синхронной репликации показана на рис. 1. На мастер-узел приходит транзакция от пользователя. Мастер записывает ее в свой журнал и передает на реплику-узел.

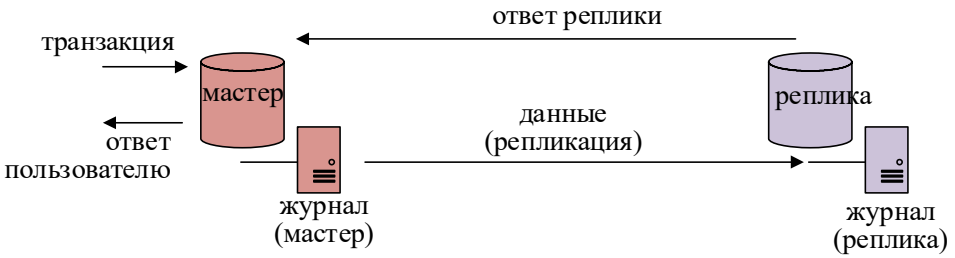


Рис. 1. Синхронная репликация

Реплика считывает транзакцию из журнала мастера и выполняет ее у себя. После выполнения транзакции ответ отправляется мастеру. Мастер фиксирует изменения, после чего обновленные данные становятся видны пользователю.

При репликации вида SBR на реплику приходит транзакция в формате запроса. Реплика должна выполнить транзакцию у себя и зафиксировать изменения. Основная проблема в этом случае состоит в том, что если в транзакции были детерминированные запросы, то может возникнуть рассинхронизация баз данных. Причиной тому является то, что реплика всегда отстает от мастера. Как правило, мастер по техническим характеристикам лучше реплики. Поэтому время выполнения запроса на нем ниже, чем на реплике. Если на мастере запрос выполнялся длительное время, то на реплике он будет выполнятся еще дольше.

При репликации вида RBR на реплику приходят не запросы, а уже сами изменения строк данных, которые реплика применяет у себя. Основная проблема в этом случае состоит в том, что если результатом выполнения запроса будет очень большой объем информации, то по коммуникационным сетям журнал будет передаваться длительное время. В этом случае на реплике будет осуществляется достаточно большое количество операций записи. Тем самым будет значительно возрастать нагрузка на жесткий диск.

Проведем анализ рассмотренных выше способов репликации и определим, в каких случаях наиболее эффективно использовать SBR или RBR репликацию. Будем полагать, что канал связи является надежным, он обеспечивает необходимую пропускную способность. Запросы не являются детерминированными.

Данные для анализа были получены с помощью средств мониторинга СУБД MySQL [5].

На рис. 2 показаны данные по нагрузке на процессор (% CPU) и жесткий диск (% HDD) в случае реализации SBR либо RBR репликации. Данные, поступающие из мастера на реплику, представляют небольшой объем информации. На рис. 2а представлен случай, когда запрос осуществляет изменение большого количества записей, а на рис. 2б – небольшого количества. Во всех случаях от мастера не требуется больших вычислительных мощностей.

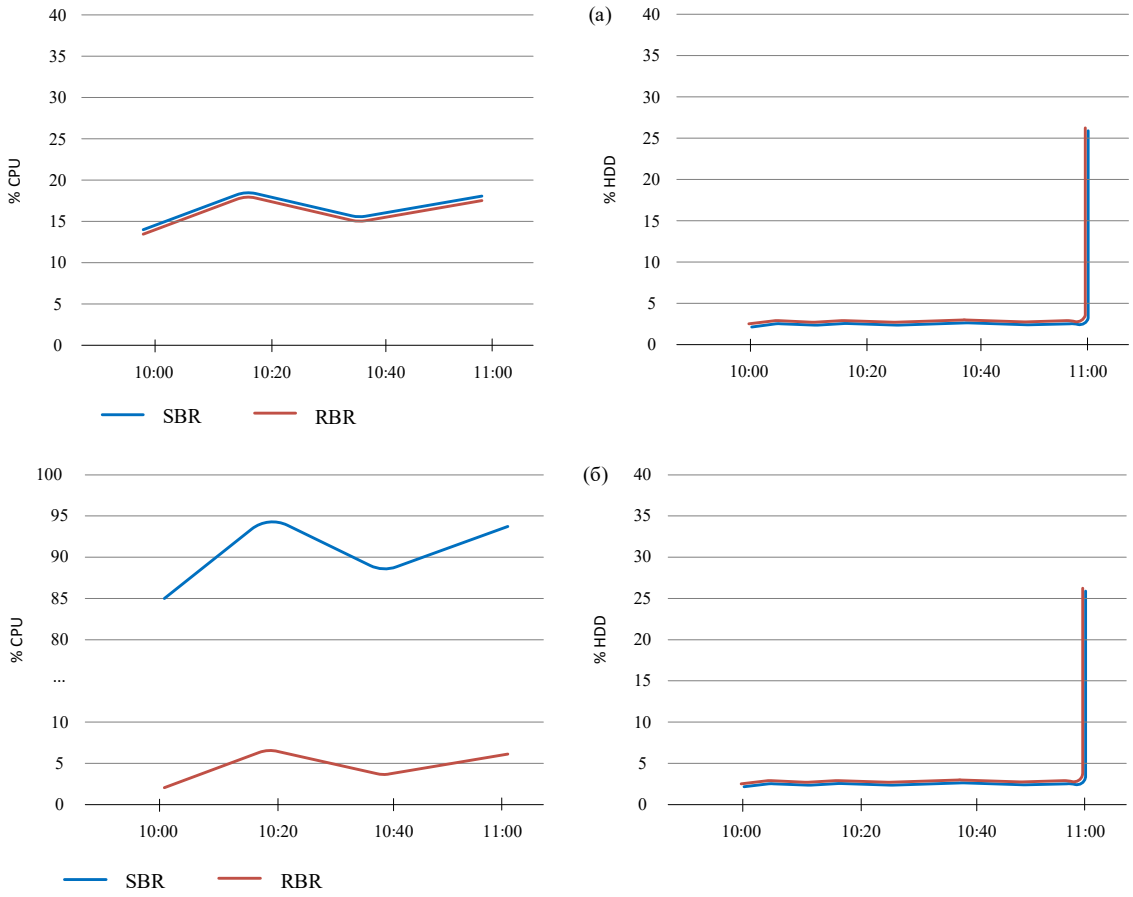


Рис. 2. Нагрузка на CPU и HDD при небольшом объеме данных в репликации

Ситуация, при которой данные, поступающие из мастера на реплику, имеют большой объем, отображается на рис. 3.

Во всех выше указанных случаях использовалась синхронная репликация, то есть изменения на мастере не применяются до тех пор, пока реплика не отправит подтверждения о фиксации изменений у себя. Таким образом, из приведенных выше графиков видно, что при синхронной репликации способ репликации RBR показывает себя более эффективным в случаях, когда синхронизация баз данных происходит при большом количестве транзакций, но при этом сами данные имеют небольшой объем. В случае, когда допускается внесение изменений с определенной задержкой, более эффективным является способ SRB при минимальной нагрузке на процессор. При этом полагалось,

что канал связи являлся надежным и обеспечивал высокую пропускную способность. При способе RBR, наличии проблем с каналом связи и больших объемах данных фиксация изменений на реплике будет занимать значительное время.

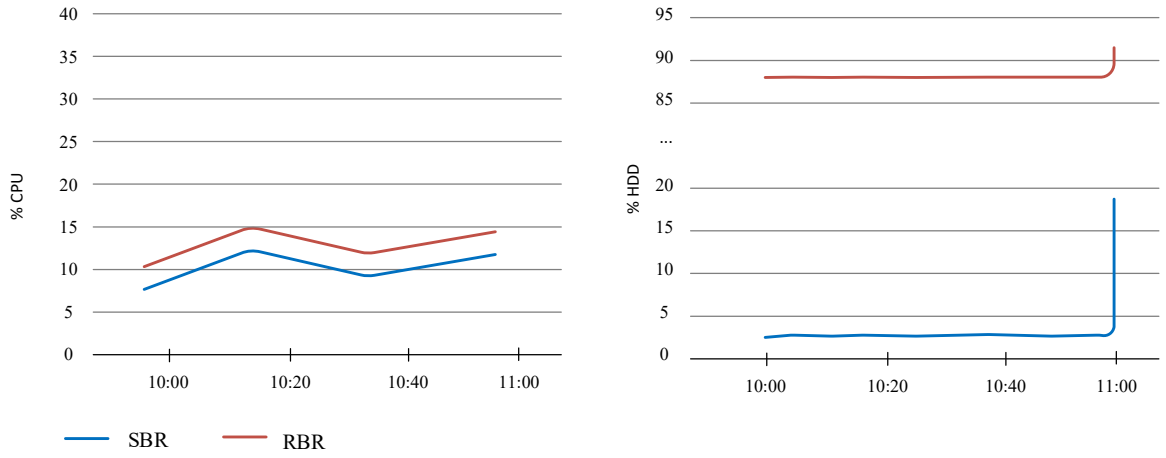


Рис. 3. Нагрузка на CPU и HDD при большом объеме данных в репликации

Следует отметить, что в настоящее время информационные технологии позволяют вмещать базы данных целиком в оперативную память, а дисковые устройства имеют высокие показатели по скорости записи и чтения. В то же время, репликация SBR нагружает, в основном, процессор, а RBR репликация нагружает жесткий диск. Кроме того, при проведенном анализе не рассматривались случаи, когда происходят сбои на мастере или реплике либо происходил откат изменений. Это рассматривается на направления дальнейших исследований.

Таким образом, SBR репликацию лучше использовать, когда необходимо синхронизировать базы данных при неустойчивом канале связи, большом объеме информации и в отсутствии детерминированных запросов. RBR репликацию лучше использовать, когда запросы требуют больших вычислительных мощностей, но при этом результатом запроса будет небольшое количество данных.

Список используемых источников

1. Котенко И. В., Федорченко А. В., Саенко И. Б., Кушнеревич А. Г. Технологии больших данных для корреляции событий безопасности на основе учета типов связей // Вопросы кибербезопасности. 2017. № 5 (24). С. 2–16.

2. Саенко И. Б., Бирюков М. А., Ясинский С. А., Грязев А. Н. Реализация критериев безопасности при построении единой системы разграничения доступа к информационным ресурсам в облачных инфраструктурах // Информация и космос. 2018. № 1. С. 81–85.

3. Основы технологий баз данных: учеб. пособие / Б. А. Новиков, Е. А. Горшкова, Н. Г. Графеева; под ред. Е. В. Рогова. 2-е изд. М.: ДМК Пресс, 2020.

4. Wiesmann M., Pedone F., Schiper A., Kemme B., Alonso G. Database replication techniques: a three parameter classification // Proceedings of the 19th IEEE Symposium on Reliable Distributed Systems SRDS-2000, 2000, pp. 206–215.

5. Ping Y., Hong-Wei H., Nan Z. Design and implementation of a MySQL database backup and recovery system // Proceeding of the 11th World Congress on Intelligent Control and Automation, 2014, pp. 5410–5415.

УДК 621.391
ГРНТИ 49.03.03

ОЦЕНКА ВОЗМОЖНОСТИ ОТКРЫТОГО ФОРМИРОВАНИЯ НЕСКОЛЬКИХ КЛЮЧЕЙ В СЕТИ СВЯЗИ

А. Д. Синюк, А. А. Тарасов

Военная орденов Жукова и Ленина Краснознаменная академия связи
имени Маршала Советского Союза С. М. Буденного

Сетевая криптосвязность корреспондентов в наибольшей степени подвержена разрушению при компрометации общего ключа нарушителем. Актуализируется поиск условий открытого и одновременного формирования нескольких ключей в сети связи. Производится теоретико-информационная оценка возможности формирования нескольких ключей в процессе открытого сетевого многоключевого согласования путем оценки информационных базисов для формирования ключей. Приводятся направления дальнейших условий.

широковещательный канал связи, нарушитель, ключ, энтропия, взаимная информация, совместная информация, информационная скорость, открытое сетевое многоключевое согласование.

Устойчивость к компрометации сетевого ключа (СК) считается минимальной, т. к. ключ известен всем корреспондентам [1, 2] и компрометация СК у одного из них приводит к невозможности безопасной передачи информации по сети связи. Задача безопасной доставки сетевого ключа обладает высокой сложностью [2]. Альтернативой представляются методы открытого ключевого согласования [3].

Ключевая сеть, объединяющая трех и более корреспондентов с общим ключом в наименьшей степени устойчива к компрометации нарушителем [1, 2]. Закрытый информационный обмен между корреспондентами с нарушенной криптосвязностью становится невозможным и требует незамедлительного решения задачи формирования, распределения и доставки нового сетевого ключа корреспондентам. Известные методы формирования сетевого ключа позволяют получить один ключ [4–7]. Исследуется метод, который позволяет, открыто формировать вместе с СК дополнительно несколько

парных ключей (ПК) между корреспондентами сети, что позволит быстро восстановить сетевой ключ. Поэтому, актуализируется теоретико-информационная оценка возможности (условий) формирования нескольких ключей от качества каналов сети связи в процессе открытого сетевого многоключевого согласования [8].

Рассмотрим процесс передачи информации по сети связи, в которой связность корреспондентов определяется моделью широковещательного канала связи [9, 10]. Имеется источник информации и один передатчик у корреспондента связи (КС) *A* и три независимо работающих приемника у КС *B*, *C* и нарушителя *E*, на входы которых поступают выходные сигналы разных каналов. На вход передатчика КС *A* поступает информация от источника, которую он должен передать одновременно *B*, *C* и *E*.

Пусть источник сообщений описывается моделью двоичного стационарного источника без памяти [10–12]. Алфавит источника задается ансамблем $\{X, p(x)\}$. Источник в единицу времени выбирает i-ю букву из алфавита с равномерным законом распределения [12, 13]. Пусть задано достаточно большое n. Источник генерирует сообщение $\overline{x}$, представляющее собой последовательность длиной *n* букв, причем $\overline{x} \in X^n$, где X^n – *n*-я декартова степень множества X [12, 13]. Совокупность, состоящая из двух каналов с общим входом описывается моделью дискретного широковещательного канала без памяти (ДШК) [10, 12]. Передача сигналов производится по двум составляющим каналам (СК) с алфавитом *X,* выходными алфавитами *Y* (для первого СК (СК1) связи) и M (второй СК (СК2)). Алфавиты *X, Y* и M конечны и любые последовательности удовлетворяют условию: $\overline{x} \in X^n, \overline{y} \in Y^n, \overline{m} \in M^n$. Пусть СК1, описывается моделью двоичного симметричного канала связи без памяти (ДСК) с вероятностью ошибки p_y, а второй СК2 – ДСК с p_m. Канал связи между выходом источника КС *A* и входом приемника 3 нарушителя *E* представляет собой канал перехвата (КП) с выходным алфавитом Z и описывается моделью ДСК с вероятностью ошибки p_z. Составляющие ДШК и КП являются независимыми каналами [10–12]. Алфавиты источника, входов и выходов ДШК и КП, совпадают.

Произведем оценку ситуации после передачи $\overline{x}$ от КС *A* по ДШК: КС *B*, *C* и нарушитель *E* принимают $\overline{y} \in Y^n$, $\overline{m} \in M^n$ и $\overline{z} \in Z^n$, соответственно. КС сети связи *A*, *B* и *C* получают информацию измеряемую информационной мерой (ИМ) совместной информации (СИ) ДШК $F(X^n; Y^n; M^n)$ [14], КС сети связи *A*, *B* - ИМ взаимной информации (ВИ) СК1 $I(X^n; Y^n)$ [10, 11], а КС сети связи *A*, *C* - ИМ ВИ СК2 $I(X^n; M^n)$. С учетом того, что СК ДШК описываются моделями ДСК [15] определим информационные скорости (ИС) $F(X;Y;M)$ – СИ между соответствующими символами на входе и выходе ДШК [14], $I(X;Y)$ – ВИ между символами на входе и выходе СК1 [11, 12, 15] и $I(X;M)$ –

ВИ СК2. Отличие оценки ИС от нуля позволяет создать условия для формирования ключа. В качестве информационной основы для формирования ключа ПК K_{AB} (информации КС *B* и *A* не известной КС *C* и нарушителю *E*) может быть выбрана ИС условной ВИ $I(X;Y/M,Z)$. По аналогии для ПК K_{AC} – условная ИС $I(X;M/Y,Z)$, а СК K_{ABC} – ИС условной СИ $F(X;Y;M/Z)$.

ТАБЛИЦА. Оценка информационной скорости

p_y		p_y=0			$0 < p_y < 0.5$			p_y=0.5		
p_z	ИС	p_m=0	$0 < p_m < 0.5$	p_m=0.5	p_m=0	$0 < p_m < 0.5$	p_m=0.5	p_m=0	$0 < p_m < 0.5$	p_m=0.5
$0 < p_z < 0.5$	*F*(*X*;*Y*;*M*/*Z*)	*H*(*X*/*Z*)	*I*(*X*;*M*/*Z*)	0	*I*(*X*;*Y*/*Z*)	>0	0	0	0	0
	I(*X*;*Y*/*M*,*Z*)	0	*I*(*X*/*M*,*Z*)	*H*(*X*/*Z*)	0	>0	*I*(*X*;*Y*/*Z*)	0	0	0
	I(*X*;*M*/*Y*,*Z*)	0	0	0	*H*(*X*/*Y*,*Z*)	>0	0	*H*(*X*/*Z*)	*I*(*X*;*M*/*Z*)	0
p_z=0.5	*F*(*X*;*Y*;*M*/*Z*)	*H*(*X*)	*I*(*X*;*M*)	0	*I*(*X*;*Y*)	>0	0	0	0	0
	I(*X*;*Y*/*M*,*Z*)	0	*H*(*X*/*M*)	*H*(*X*)	0	>0	*I*(*X*;*Y*)	0	0	0
	I(*X*;*M*/*Y*,*Z*)	0	0	0	*H*(*X*/*Y*)	>0	0	*H*(*X*)	*I*(*X*;*M*)	0

Оценим граничные условия определяющие возможность осуществления согласования ключей в зависимости от качества СК1 (p_y), СК2 (p_m) и КП (p_z). Заметим, что согласование не возможно, если $p_z = 0$, т. к. $H(X/Z) = 0$, где $H(X/Z)$ – условная энтропия *X* при известном *Z* [12]. Согласование также не возможно, если $p_y = p_m = 0{,}5$ т. к. ИС $F(X;Y;M/Z) = 0$, $I(X;Y/M,Z) = 0$, $I(X;M/Y,Z) = 0$. Другие оценки ИС сведем в табл.

Анализ табл. показывает, что возможность формирования ключей определяется разными ситуациями по вероятностям ошибок в каналах сети, т. к. согласование невозможно в обоих граничных случаях, когда все каналы идеальны, так и, состояния, когда каналы находятся в режиме «обрыва». Имеют место сложные взаимосвязи. Так, например, при идеальных СК1 и СК2 по логике должны быть сформированы все три ключа, а возможность имеется только для одного. Есть сочетания вероятностей, при которых возможно формирование только СК K_{ABC} ($p_m = 0$, $p_y = 0$, $0 < p_z < 0{,}5$), только ПК K_{AB} ($p_m = 0.5$; $p_y = 0$; $0 < p_z < 0{,}5$), только ПК K_{AC} ($p_m = 0$, $p_y = 0.5$, $0 < p_z < 0{,}5$). Имеют место сочетания, при которых возможно формирование двух ключей СК K_{ABC} и ПК K_{AB} ($0 < p_m < 0.5$, $p_y = 0$, $0 < p_z < 0{,}5$) и др. Наиболее детального исследования требуют условия, которые позволяют создать максимальную криптосвязность с ключами K_{ABC}, K_{AB}, K_{AC} в интервальных сочетаниях вероятностей $0 < p_m < 0.5$, $0 < p_y < 0.5$, $0 < p_z \le 0{,}5$ в рамках взаимных соотношений p_y, p_m и p_z обеспечивающие успешное формирование трех ключей. В роли других направлений исследований представляются оценка информационной эффективности, синтез конструктивных протоколов открытого сетевого многоключевого согласования, и др.

Список используемых источников

1. Шнайер Брюс Прикладная криптография. Протоколы, алгоритмы и исходные тексты на языке С / пер. с англ. М.: Издательский дом "Вильямс", 2003. 568 с.

2. Алферов А. П., Зубов А. Ю., Кузьмин А. С., Черемушкин А. В. Основы криптографии: Учебное пособие. 3-е изд., испр. и доп. М.: Гелиос АРВ, 2005. 480 с.

3. Maurer U. Secret Key Agreement by Public Discussion Based on Common Information // IEEE Trans. on IT. Vol. 39, May 1993. PP. 733–742.

4. Sinjuk A. D., Ostroumov O. A. Theorem about key capacity of a communication network // Information and Control Systems. 2018;(5):79-87. https://doi.org/10.31799/1684-8853-2018-5-79-87.

5. Group Key Agreement with Local Connectivity Shaoquan Jiang IEEE Transactions on Dependable and Secure Computing Year: 2016, Volume: 13, Issue: 3 Pages: 326 – 339

6. Group Key Agreement Protocol Based on Privacy Protection and Attribute Authentication // Zhang Qikun; Li Yongjiao; Gan Yong; Zheng Chuanyang; Luo Xiangyang; Zheng Jun IEEE Access (Volume: 7) Page(s): 87085–87096. Date of Publication: 02 July 2019. DOI: 10.1109/ACCESS.2019.2926404

7. Zhouzhou Li, Honggang Wang, Hua Fang. Group-Based Cooperation on Symmetric Key Generation for Wireless Body Area Networks // IEEE Internet of Things Journal. 4 (6) 2017. pp. 1955–1963.

8. Синюк А. Д., Тарасов А. А. Оценка условий открытого сетевого многоключевого согласования // Актуальные проблемы инфотелекоммуникаций в науке и образовании. X Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2021. С. 409–413.

9. Cover T. Broadcast Channels // IEEE Trans, on Inf. Theory. 1972. vol. 18. № 1.

10. Колесник В. Д., Полтырев Г. Ш. Курс теории информации. М.: Наука. Главная редакция физико-математической литературы, 1982. 416 с.

11. Галлагер Р. Теория информации и надежная связь. США, 1968 г. Пер. с англ , под ред. М. С. Пинскера и Б. С. Цыбакова, М , «Советское радио», 1974. 720 с.

12. Чисар И., Кернер Я. Теория информации: теоремы кодирования для дискретных систем без памяти / пер. с англ. М.: Мир, 1985. 400 с.

13. Вентцель Е. С. Теория вероятностей: учеб. для вузов. 9-е изд. стер. М.: Издательский центр «Академия», 2003. 576 с.

14. Остроумов О. А., Синюк А. Д. Исследование совместной информации // Информация и космос. 2017. № 3. С. 55–58.

15. Фано Р. Передача информации. Статистическая теория связи. М.: Мир, 1965. 366 с.

УДК 004.75
ГРНТИ 49.34.01, 49.33.01

РАЗРАБОТКА ИМИТАЦИОННОЙ МОДЕЛИ СИСТЕМЫ БЛОКЧЕЙН

А. В. Спиркина

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В данной статье описана разработка имитационной модели системы блокчейн, включающая обобщенную модель трафика и учитывающая свойства процессов подсистемы.

Предложенные автором модели представляют собой простые, но мощные средства для выявления многих важных показателей, таких как интенсивность появления транзакций в секунду, размер блоков, и др. влияющие на определенные характеристики, например, время ожидания в пуле памяти, время пребывания пакетов в системе, задержка транзакций.

Distributed registry, blockchain, QoS, Quality of service.

Введение

Система AnyLogic поддерживает различные подходы к имитационным моделям, позволяет моделировать различные аспекты системы на разных уровнях детализации и имеет графический интерфейс. Предложенная модель представляется для демонстрации работы блокчейна, а также изучения и прогнозирования масштабируемости, взаимодействия участников системы, использования ресурсов и вариации принятия различных реализаций параметров. Необходимо уточнить, что модель направлена на проверку характеристик сети при распределении транзакций и блоков и не включает оценку ряда параметров, таких как общий размер цепочки блокчейна, величина вознаграждения, и других. При этом масштабируемость системы блокчейн зависит от лежащего в основе консенсуса, сетевой синхронизации и архитектуры [1, 2].

Описание имитационной модели

Представленная в статье модель выполнялась в программе AnyLogic 8 Professional 8.7.9 Сборка: 8.7.9.202112171627 x64 и состоит из 3 типов агентов: Block, Main и User.

1. Block. Каждый блок содержит параметры, описывающие общий размер блока в килобайтах и метку времени пребывания в системе в секундах.

2. Main. Является основным типом агентов и содержит совокупность транзакций, блоков, пользователей, верификаторов и валидаторов, отображение агента Main в среде AnyLogic представлено на рисунке 1. Включает параметры, переменные, функции, распределения и диаграммы.

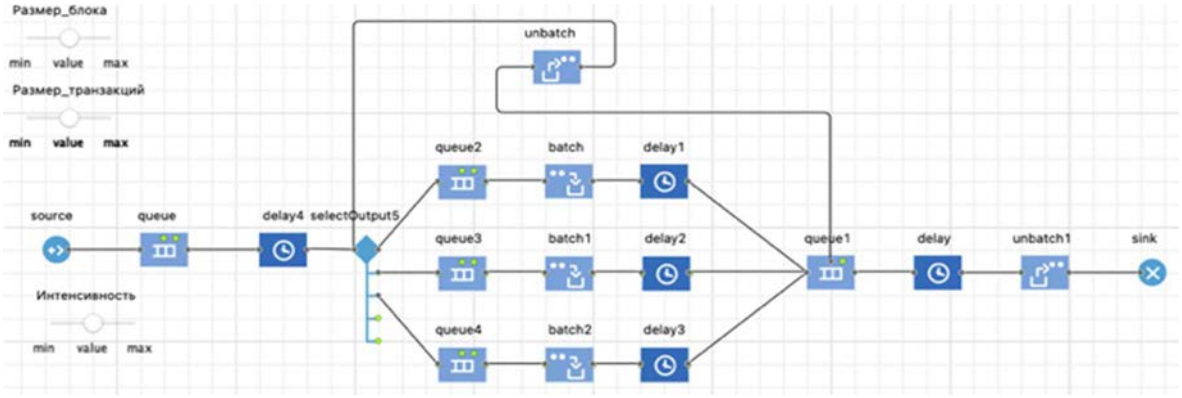


Рис. 1. Графическое отображение агента Main в среде Anylogic

Блок source выполняет роль пользователя, который инициирует появление транзакций (заявок) с определенной интенсивностью. Блоки queue и delay4 представляют проверку транзакции на корректность и отправку валидаторам. Блок selectOutput5 направляет входящих агентов в один из трех выходных портов с равной вероятностью. Устройства валидирующие транзакции представляют собой устройство, состоящее из нескольких блоков: блоки queue2, queue3, queue4 моделируют пулы памяти, принадлежащие валидатору, в которых происходит накопление транзакций, которые ждут добавления в блок и валидацию; блоки batch, batch1, batch2 преобразуют заданное количество поступающих в блок агентов (транзакций), определенных параметром sizet, в одного агента-партию (блок) с постоянным размером, определенным параметром sizeb, и передают в блок, ответственный за выполнение алгоритма консенсуса; блоки delay1, delay2, delay3 задерживают агентов на время обработки пакета. В блоках queue и delay происходит разделение блоков между теми которые отправляются для добавления в основную цепочку и теми, кто был отклонен, отклоненные блоки направляются на устройство unbatch, которое извлекает всех агентов, содержащихся в поступающей партии агентов, и пересылает их далее по одной через выходной порт, сохраняя порядок, в котором они хранились в партии и направляются на устройство валидации. Блоки, которые были подтверждены проверяются со скоростью обработки, которая затребована для проверки текущего состояния блокчейна, вычисляя хэш блока и проверку его согласованность с хэшем, присутствующим в предыдущем блоке, в блоке delay. Как только отдельная транзакция подтверждена или удалена из пула памяти по истечении времени ожидания, отдельный агент транзакции уничтожается блоками unbatch1 и sink.

3. User.

Каждый агент User содержит параметры, описывающие размер транзакции в килобайтах и метку времени пребывания транзакции в системе в секундах, также включает диаграмму состояний и переходов, необходимую в случае расширения количества пользователей.

Результаты моделирования

В рамках моделирования был проведен ряд экспериментов, позволяющий рассмотреть различные конфигурации системы.

Результаты моделирования на рисунке 2 дают представление о влиянии интенсивности формирования транзакций на размер пула памяти, значения, указанные на рис. 2 являются средними для трёх узлов и снимались в течении 604 800 секунд.

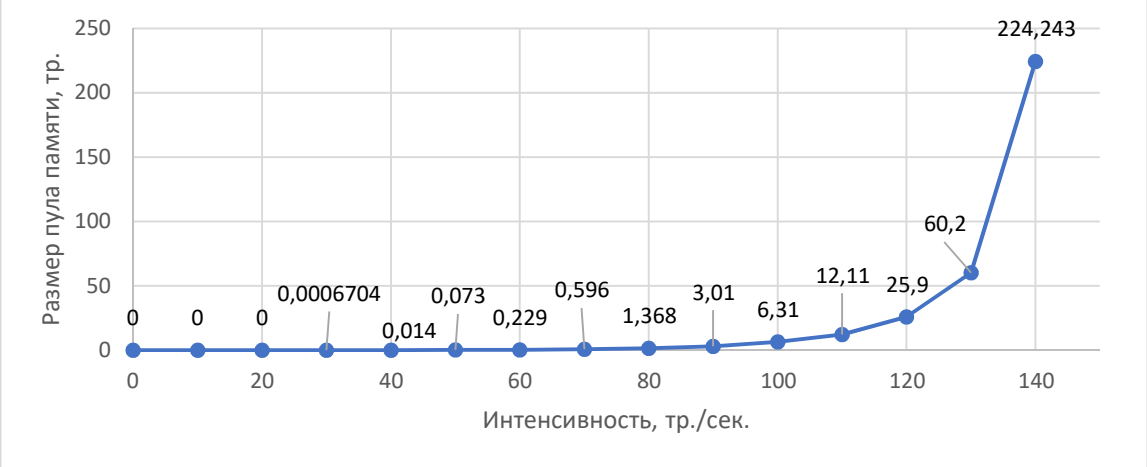


Рис. 2. Результаты моделирования влияния интенсивности формирования транзакций на размер пула памяти

Результаты моделирования на рис. 3 дают представление о влиянии размера блока на задержку транзакции и снимались в течении 604800 секунд, с интенсивностью 100 транзакций в секунду.

Результаты, представленные на рис. 3, позволяют сделать вывод о том, что, когда размер блока мал (в данной конфигурации, < 600), средняя задержка чрезвычайно высока, что связано с тем, что узлы, получающие блоки, не могут сразу начать их проверку, поскольку блоки генерируются слишком быстро из-за малого размера блока и постепенно накапливаются в очереди. По мере увеличения размера блока до определенного значения средняя задержка уменьшается, так как время на этапах проверок становится меньше. Стоит отметить, что при превышении определенных значений (в данной конфигурации, >1000), начинается рост средней задержки, так как увеличивается среднее время ожидания транзакциями полного

наполнения блоков на этапе валидации из-за большего размера, важно отметить, что значение также будет иметь интенсивность формирования транзакций.

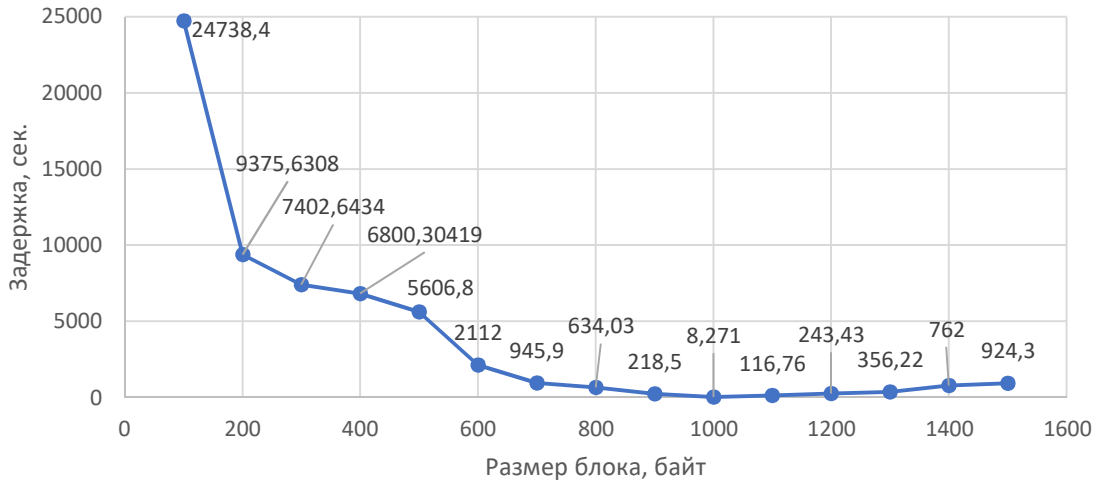


Рис. 3. Результаты моделирования влияния размера блока на задержку транзакции

Результаты моделирования на рисунке 4 дают представление о влиянии интенсивности формирования транзакций на задержку и снимались в течении 604 800 секунд.

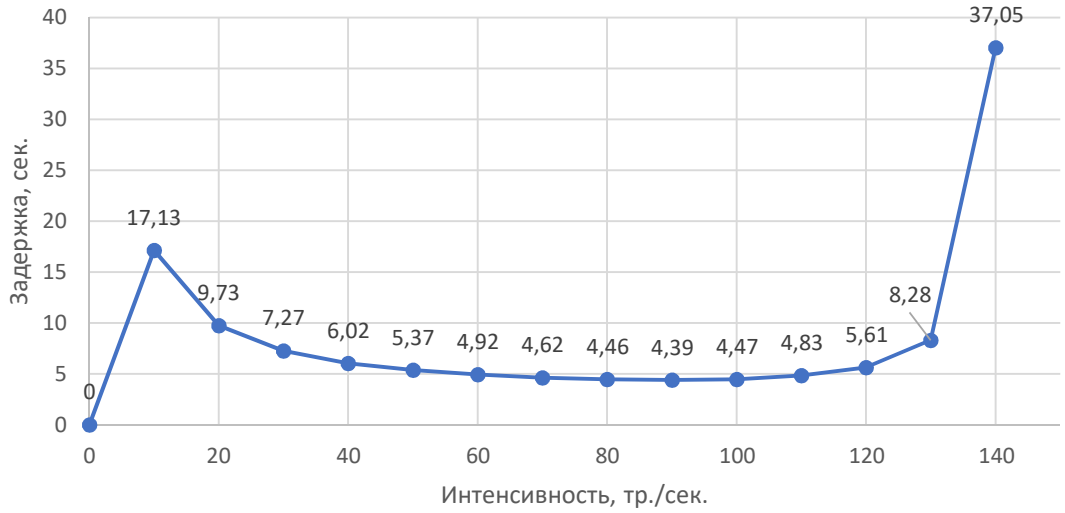


Рис. 4. Результаты моделирования влияния интенсивности формирования транзакций на задержку транзакции

Результаты, представленные на рис. 4, позволяют сделать вывод о том что, когда интенсивность формирования транзакций при фиксированном

размере блока мала (в данной конфигурации, < 20), средняя задержка высока, что связано с тем, что узлы, получающие блоки, не могут сразу начать их проверку, так как увеличивается среднее время ожидания транзакциями полного наполнения блоков на этапе валидации. Стоит отметить, что при превышении определенных значений (в данной конфигурации, > 130), начинается рост средней задержки, так как скорость обработки транзакций валидатором ниже скорости поступления транзакций в пул памяти.

Сравнение полученных результатов и выводы

Сетевая задержка играет ключевую роль при распространении транзакции и блока по сети, так существенная задержка будет влиять на постановку в очередь в пул памяти, что отразится на времени добавления транзакции в блок, и подтверждение выполнения задачи валидатора, так как узел должен прекратить работу над своими блоками, как только будет объявлен новый блок, чтобы сэкономить вычислительные ресурсы, однако узлы могут получать вновь созданные блоки слишком поздно из-за задержки распространения и продолжать работать с уже устаревшими транзакциями. Поэтому с точки зрения эффективной обработки транзакций и работы системы в целом необходимо уделять ключевое значение сетевым параметрам узлов. Также эксперимент показал, что работоспособность сети зависит от интенсивности появления транзакций, при этом для корректной работы технологии блокчейн представленного типа можно варьировать значения интенсивности узлов и значения размера буфера.

Следует отметить, что моделирование технологии блокчейн с помощью системы Anylogic для оценки производительности производительности возможно и удобно для анализа при изменении различных параметров. Анализ моделей показал применимость отдельных систем имитационного моделирования для оценки влияния технологии блокчейн на сети передачи данных [3, 4].

Данные результаты показали, что правильная настройка параметров системы блокчейн важна для снижения задержки, оптимального построения сетей и экономии средств. Для модели с заданными характеристиками и средней интенсивностью формирования транзакций 100 транзакций в секунду оптимальным будет выбор таких параметров: размер пула, рассчитанный на 7–10 транзакций, размер блока около 1 кбайт, однако при изменении средней интенсивности формирования транзакций параметры следует оптимизировать.

Список используемых источников

1. Spirkina A.V. et al. Approaches to Modeling Blockchain Systems // 2020 12th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT). pp. 242–247.

2. Vladyko A. et al. Distributed Edge Computing with Blockchain Technology to Enable Ultra-Reliable Low-Latency V2X Communications // Electronics. 2022. Vol. 11. N. 2. P. 173.
3. Vladyko A. Towards Practical Applications in Modeling Blockchain System // Future Internet. 2021. N. 13. P. 125.
4. Спиркина А. В. Научные аспекты структурно-параметрического моделирования блокчейн-систем // Труды учебных заведений связи. 2021. № 7 (1). С. 122–131.

Статья представлена научным руководителем, доцентом кафедры ИКС СПбГУТ, кандидатом технических наук, доцентом В. С. Елагиным.

УДК 004.451.87
ГРНТИ 50.41.15

РАЗРАБОТКА АЛГОРИТМА ВЫЯВЛЕНИЯ ROOTKIT УРОВНЯ ЯДРА НА ОСНОВЕ ПЕРЕХВАТА СОБЫТИЙ ЯДРА ОПЕРАЦИОННОЙ СИСТЕМЫ

О. В. Фёдорова, А. Ю. Цветков

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Руткиты – тип программного обеспечения, который специализируется на сокрытии сущностей в компьютерных системах, обеспечивая непрерывный контроль или доступ к ним, его – особенно трудно обнаружить по сравнению с другими видами программного обеспечения. Существуют различные инструменты для детектирования руткитов, использующие широкий спектр методов и механизмов обнаружения. Однако эффективность таких инструментов не вполне доказана, особенно в современных академических исследованиях и в контексте операционной системы Linux.

ядро Linux, Модуль ядра системы Linux, RootKit, права суперпользователя, системные вызовы, аппаратные прерывания, механизм защиты, виртуальный лабораторный стенд.

Существует не так много методов, которые позволяют обнаруживать скрытый процесс. В основном они сводятся к перебору всего множества возможных идентификаторов процессов с помощью системных вызовов, таких как:

– setsid;
– getpid;
– kill;
– stat;
– opendir.
– etc.

Одной из проблем существующих реализаций методов обнаружения руткитов является то, что большинство средств по обнаружению руткитов располагаются в пространстве пользователя, тем самым в большинстве своем полагаясь на побочную информацию (к примеру метод перебора идентификаторов процесса).

Процесс выявления скрытых руткитом процессов имеет множество особенностей, затрудняющих работу по поиску. Основной из них является то, что возможное наличие руткита в ядре, которое в данный момент работает, позволяет ему (руткиту) производить всевозможные действия для того, чтобы не быть обнаруженным. Из этого следует, что необходимо осуществлять действия по обнаружению руткитов из режима ядра. При этом стоит отметить, что не всегда имеется возможность проверять наличие руткитов в системе после перезагрузки с другим ядром, либо даже с загрузочного образа, так как даже если возможность и имеется, данные действия приводят к простою в работе машин, что особенно важно для серверов.

Для того, чтобы найти точку, где гарантированно возможно обнаружить скрытый процесс, необходимо выяснить, в какой точке каждый процесс гарантированно окажется, и эта точка однозначно определяема. В качестве одного из вариантов такой точки можно рассмотреть планировщик задач, так как для того, чтобы в скрытии процесса имелся смысл, этот процесс должен работать, а значит процесс его исполнения будет проходить через планировщика задач ядра операционной системы.

Рассмотрим процесс работы планировщика ядра Linux.

Главной точкой входа в планировщик задач является функция «schedule()».Эта функция используется для вызова планировщика задач, решения о том, какой процесс следует запустить, после чего запустить этот процесс. Основной целью является поиск следующей задачи для запуска, после чего выполняется переключение контекста для новой задачи. Если задача не найдена, то функция «schedule()» ничего не изменяет.

Существуют три основные причины вызова «schedule()»:

– регулярное обновление текущей задачи. Функция «scheduler_tick()» вызывается регулярно по прерыванию таймера. Обновляется таймер выполнения, счетчики текущей задачи. Если обнаруживается, что существует задача, которую необходимо запланировать, то устанавливается флаг «need_resched», который сообщает ядру о том, что необходимо вызвать «schedule()» как только это станет возможным;

– текущая задача приостанавливается;

– текущая задача возобновляет выполнение. Код, который вызывает со-бытия для спящих задач ожидает, как правило, вызов «wake_up()» на соответствующей очереди, и в конечном итоге приводит в функцию планировщика «try_to_wake_up()».

Схема планировщика задач ядра Linux представлена в приложении Г.

Таким образом наиболее эффективным выглядит перехват функции «try_to_wake_up», основной задачей которой является пробуждение спящего процесса.

Функция работает следующим образом:

– помещает задачу в очередь выполнения задач;

– изменяет состояние задачи на «TASK_RUNNING» (задача в процессевыполнения);

– если пробуждаемая задача имеет приоритет выше текущей задачи, топроизводит вызов планировщика с целью перепланирования задач.

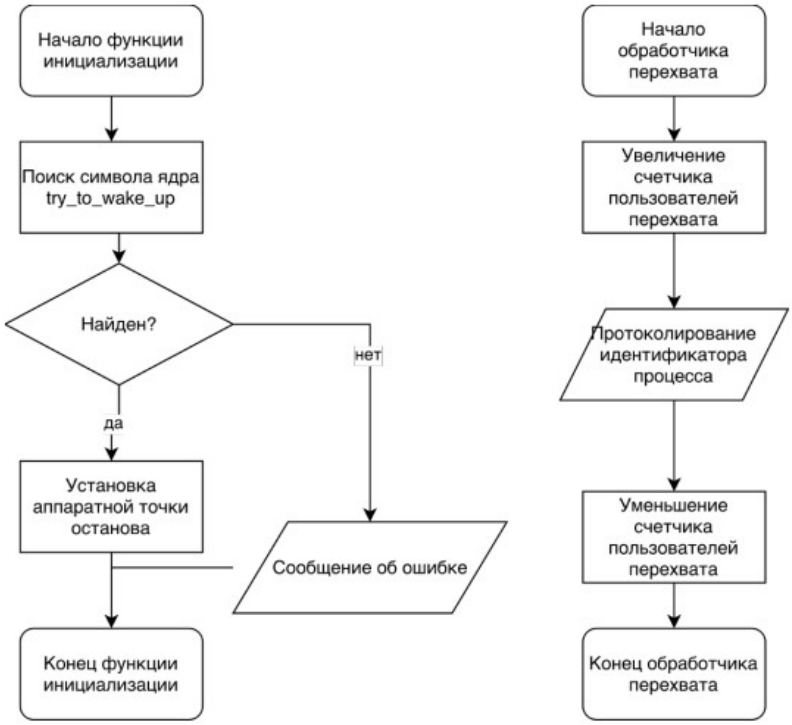


Рисунок. Алгоритм функционирования метода выявления скрытых процессов

Непосредственная реализация на уровне ядра (за исключением побочного кода, который отвечает за механизм перехвата функций на уровне ядра) сводится к перехвату данной функции и протоколирования информации из доступных структур данных ядра.

Перехват функции пробуждения спящего процесса совершает единственное действие, которое является минимально необходимым для решения задачи: выводить в лог ядра название процесса, на которое произошло переключение. Таким образом для завершения работы по выявлению скрытого руткитом процесса достаточно сопоставлять пробуждаемые задачи с теми задачами, которые видно со стороны пользовательского пространства, тем самым позволяя обнаруживать нелигитимные задачи. Алгоритм схематично представлен на рис.

Заключение

Таким образом продемонстрирован алгоритм, позволяющий выявлять скрытые процессе в ядре. Данные процессы могут быть инициализированы зловредным программным обеспечением, что позволяет установить факт присутствия нелегитимного ПО на рабочей станции, а так же понять скомпрометированные процессы.

Список используемых источников

1. Долгих Д. Учимся писать модуль ядра (Netfilter) или Прозрачный прокси для HTTPS. URL: https://habr.com/ru/post/138328/

2. Кирилова К. С., Цветков А. Ю. Анализ существующих методов реализации rootkit // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VIII Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4 т. СПб. : СПбГУТ, 2019. С. 492–497.

3. Кирилова К. С., Цветков А. Ю., Волкогонов В. Н. Проблема обезвреживания руткитов уровня ядра в системах специального назначения //] I-methods. 2020. Т. 12. № 3. С. 1–9.

4. Матвейчиков И. В. Простая маскировка модуля ядра Linux с применением DKOM. URL : https://habr.com/ru/post/205274/

5. Фёдорова О. В., Цветков А. Ю. Детектирование вредоносного программного обеспечения ядра системы на основе анализа запущенных программ // Инновации. Наука. Образование. 2021. № 31. С. 118–124.

6. Цилюрик О. Практикум: модули ядра Linux. Конспект с примерами и упражнения с задачами. URL: https://losst.ru/wp-content/uploads/2016/08/BOOK_PRACTIS_245.pdf

7. Щербакова Т. Фишинговые письма – самый распространенный способ взлома почты. URL: https://www.kaspersky.ru/blog/email-account-stealing/23433/

8. Alavoor Vasudevan The Linux Kernel HOWTO. URL: http://www.faqs.org/docs/ Linux-HOWTO/Kernel-HOWTO.html

9. Andreas Bunten UNIX and Linux based Rootkits. Techniques and Countermeasures // DFN-CERT Services GmbH, 2004. URL: http://repository.root-me.org/Virologie/EN%20-20UNIX%20and%20Linux%20based%20Rootkits%20Techniques%20and%20Countermeasures%20-%20Andreas%20Bunten.pdf

10. Кирилова К. С., Цветков А. Ю. Анализ существующих методов реализации rootkit // Актуальные проблемы инфотелекоммуникаций в науке и образование. VIII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. СПб.: СПбГУТ, 2019. С. 492–497.

11. Таргонская А. И., Цветков А. Ю. Разработка защищенного веб-интерфейса для управления устройствами в сети // Актуальные проблемы инфотелекоммуникаций в науке и образование. VIII Международная научно-техническая и научно- методическая конференция: сб. науч. ст. СПб.: СПбГУТ, 2019. С. 734–739.

12. Темченко В. И., Цветков А. Ю. Проектирование модели информационной безопасности в операционной системе // Актуальные проблемы инфотелекоммуникаций в науке и образование. VIII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. СПб.: СПбГУТ, 2019. С. 740–745.

13. Цветков А. Ю. Исследование существующих механизмов защиты операционных систем семейства Linux // Актуальные проблемы инфотелекоммуникаций в науке и образование. VII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2018. С. 657–662.

14. Цветков А. Ю., Шалаева М. Е., Юрченко М. А. Обеспечение безопасности в клиент-серверном Java приложении для учета и автоматической проверки лабораторных работ // Актуальные проблемы инфотелекоммуникаций в науке и образование. VIII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. СПб.: СПбГУТ, 2019. С. 756–761.

15. Багомедова А. Р., Ушаков И. А., Цветков А. Ю. Разработка методов проверки соответствия серверов виртуализации требованиям безопасности согласно стандарту ГОСТ Р 56938-2016 // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2018. С. 58–63.

УДК 004.946
ГРНТИ 28.17.33

ИССЛЕДОВАНИЕ МЕТОДОВ ПОЗИЦИОНИРОВАНИЯ В ДОПОЛНЕННОЙ РЕАЛЬНОСТИ

М. В. Шарлаева

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В данной статье рассмотрены существующие способы определения местоположения объектов с целью выбора наиболее эффективного при создании приложений дополненной реальности. К навигации в дополненной реальности предъявляются более серьезные требования по сравнению с трекингом мобильных роботов. Необходимо обеспечить высокий уровень точности в реальном времени и расширить дальность действия, учитывая многообразие окружающих объектов. Дальнейшее использование наиболее эффективного алгоритма заключается в создании приложения дополненной реальности для слабовидящих.

маркерная технология, безмаркерная технология, методы определения местоположения объектов, дополненная реальность.

С появлением дополненной реальности одну из ключевых ролей среди элементов обеспечения корректной работы создаваемых приложений заняла задача трекинга. Под термином «трекинг» в контексте данной работы понимается процесс отслеживания некоторого объекта реального мира или текущего местоположения устройства дополненной реальности относительно окружающих объектов. Следует учитывать, что к навигации в дополненной реальности предъявляются серьезные требования ввиду того, что цель применения этой технологии способна оказать огромную пользу обществу, а вероятность ошибки может повлечь за собой неизгладимые последствия.

Попытки совершенствования трекинга ведутся с прошлого века в различных сферах, касающихся навигации. На текущий момент в качестве ключевых направлений развития можно выделить обеспечение более высокого уровня точности в реальном времени и расширение дальности действия распознавания и отслеживания объектов.

Одной из сфер применения дополненной реальности является медицина, и применение различных подходов к трекингу наблюдается в двух основных направлениях: проведение хирургических операций с участием «виртуального помощника»; поддержка людей, имеющих проблемы со зрением.

Существующие методы и подходы, позволяющие определить местоположение объектов окружающего мира, можно разделить на несколько основных групп [1]:

– Акустические.
– Радиочастотные.
– Магнитные.
– Оптические.
– Инерционные.

Используя акустические методы, приборы фиксируют показатель ToA (*Time of Arrival*) – абсолютное время, за которое звуковая волна преодолевает расстояние от источника до приемника [2] или разность фаз звуковой волны при приёмо-передаче. Однако, низкая скорость звука в воздухе не способна поддерживать высокую скорость обновления местоположения устройства, а также она зависима от внешних факторов, температуры, давления, влажности, что не гарантирует стабильное качество работы алгоритма.

Радиочастотные методы во многом схожи с акустическими, отличие заключается в природе волны. Однако, ни один из используемых стандартов, таких как UWB, Wi-Fi, WiMax, MiWi, ZigBee, NFER, NanoLOC, DECT, GSM, Bluetooth [8], не способны обеспечить высокую точность определения местоположения. Лучшие показатели, порядка 10-30 см, достигаются при позиционировании с использованием широкополосного доступа посредством повышения частоты, что влечет за собой снижение радиуса действия [3].

Системы, использующие магнитный трекинг, базируются на измерении интенсивности магнитного поля, излучаемого базовыми станциями: с увеличением расстояния между местом измерения и базовой станцией, уменьшается сила магнитного поля. Данный метод способен продемонстрировать высокую точность работы в условиях, где обеспечивается защита от помех токопроводящих материалов и магнитных полей, создаваемых другими устройствами и материалами на территории отслеживания.

Инерциальные системы способны обеспечить высокую точность и минимальные задержки, однако использование данных акселерометра, гироскопа, магнетометра, барометра или компаса без комбинирования источников данных и других методов в результате дает сильные помехи, зашумления, а также квадратичное увеличение ошибки с течением времени.

Оптическое позиционирование возможно благодаря наличию камеры на устройстве ДР, обладает хорошей совместимостью с алгоритмами машинного обучения с целью распознавания окружения, а также может быть использовано в любой точке мира за счет отсутствия необходимости использования дополнительных устройств, таких как приемо-передатчики звука, базовые станции, BLE-маяки, Bluetooth-антенны и т. п. За счет чего использование данного подхода можно назвать наиболее перспективным среди конкурентов.

В зависимости от использования специальных оптических маркеров выделяют отдельно безмаркерную и маркерную технологии. «Безмаркерная» технология подразумевает под собой сканирование окружения на предмет обнаружения плоскостей, дальнейшего размещения виртуальной сетки и алгоритмического поиска опорных точек для точного отображения виртуального объекта. Преимущество данного подхода заключается в восприятии объектов реального мира в качестве маркеров, из чего следует вывод, что отсутствует необходимость создания визуальных идентификаторов. Использование данного подхода поддерживается целым рядом программных комплексов, позволяющих реализовать приложения дополненной реальности: ARCore, ARKit, Vuforia, Kudan [4]. Смысл маркерной технологии прослеживается, исходя из её названия: камера устройства дополненной реальности распознает определенные метки в реальном мире посредством использования специальных алгоритмов. Метки предварительно заданы и хранятся либо в памяти устройства, либо в облачной базе данных. По содержимому метки выполняется поиск 2D или 3D виртуального объекта, который должен быть расположен на поверхности маркера. При этом поддерживается возможность перемещения виртуального объекта по траектории движения маркера.

Переходя к экспериментальной части работы, создано несколько приложений с использованием платформы Unity 3D, использующей C# для обработки поведения объектов сцены, и Python. Безмаркерная и маркерная технологии поддерживаются благодаря встроенным возможностям библиотеки Vuforia Engine. Предполагается, что маркерами выступают изображения из заранее созданной облачной базы данных.

Элементы инерциальной навигации интегрированы с механизмами отслеживания положения захваченного объекта. Для отображения виртуальной модели потребовалось организовать передачу в Unity посредством UDP-сокета, а в качестве метки выступает рамка отслеживаемого объекта.

Для сравнения перечисленных подходов решено использовать замеры времени с момента запуска приложения ДР в одинаковом положении камеры устройства ДР, при этом изменяя угол поворота, что позволяет сравнить скорость вычислений. Благодаря изменению уровня рассогласования между объектами на изображении можно определить также число ложных срабатываний, что определяется как среднее количество неверно распознанных опорных точек по результатам 50 тестов. Высокий показатель напрямую влияет на вероятность отклонения виртуального указателя от истинной позиции. В качестве показаний наклона исходного изображения использованы значения 45 и 90 градусов. Выбор максимального значения обусловлен тем, что более высокие показатели являются зеркальными отражениями наклона от 0 до 90 градусов. Зафиксированные показатели экспериментов представлены в таблице.

ТАБЛИЦА. Результаты, полученные при использовании разных технологий

Технология	Угол наклона			Количество ложных опорных точек		
	0°	45°	90°	0°	45°	90°
Безмаркерная	3,44 с.	3,83 с.	3,72 с.	-	-	-
Маркерная	3,42 с.	3,86 с.	3,65 с.	7,91	12,15	8,11
Инерциальная + маркерная	2,84 с.	2,98 с.	3,02 с.	0	2,9	0

Полученные результаты свидетельствуют о наилучших показаниях времени вычисления при выполнении поиска расположения и отображения виртуальной модели при совместном использовании инерциального подхода и маркерной технологии, несмотря на необходимость передачи данных местоположения из внешнего Python-модуля. Реализованные примеры строго маркерного подхода и безмаркерной технологии демонстрируют близкие результаты, следовательно, их применение должно быть обусловлено условиями задачи.

На основании результатов времени отображения модели при изменении угла наклона метки или поверхности можно судить о том, что промежуточные значения между 0 и 90° увеличивают время распознавания области.

Безмаркерная технология не предусматривает поиск опорных точек. Метка, используемая при маркерном способе, обладает высоким рейтингом качества уникальности, но несмотря на это в результате выполнения алгоритма распознавания, встроенного в Unity, присутствуют ошибочные точки идентификации Image Target.

В случае совместного использования инерциального и маркерного подходов практически отсутствует ложное определение опорных точек можно объяснить самостоятельным выделением области поиска метки, вследствие

чего сокращается область поиска, а значит часть пространства не учитывается.

Список используемых источников

1. Обзор методов и технологий отслеживания положения для виртуальной реальности. URL: https://habr.com/ru/post/397757/
2. Time of arrival. URL: https://en.wikipedia.org/wiki/Time_of_arrival
3. Indoor Positioning With Ultra-Wideband. URL: https://www.infsoft.com/basics/positioning-technologies/ultra-wideband/
4. Дополненная реальность - AR. URL: https://digitaloxy.ru/ru/services/sozdanie-dopolnennoy-real-nosti-ar/

Статья представлена профессором кафедры ССиПд СПбГУТ, доктором технических наук, доцентом М. А. Маколкиной.

УДК 004.273
ГРНТИ 50.41.17

АНАЛИЗ МЕТОДОВ ОПРЕДЕЛЕНИЯ ХАРАКТЕРИСТИК СИСТЕМ ХРАНЕНИЯ ДАННЫХ РП РАЗЛИЧНЫХ ТИПАХ НАГРУЗКИ

А. А. Швидкий

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье приводится анализ методов определения характеристик распределенных систем хранения данных с помощью определения различных параметров для шаблонов нагрузки. Отдельно рассмотрены вопросы влияния на производительность архитектуры распределенной системы хранения данных, так как особенности её построения не позволяют применять к анализу те же методы, что использовались при анализе работы классических СХД [1]. *На основании анализа предлагаются шаблоны генерации нагрузки, которые отражают основные требования к проведению нагрузочного тестирования.*

система хранения данных, программно-определяемая СХД, распределенная СХД.

При использовании распределенной, программно-определяемой СХД Ceph, выбор которой был обоснован в отчете по результатам работы над этапом 1 данной НИР, следует учитывать архитектурные требования данной распределенной СХД [2], которые рекомендуют размещать раздел с журналом на высокоскоростных дисках. Так как основное направление работы данной НИР связанно с повышением производительности распределённой

СХД средствами нейронной сети, то требование к типам дисков должно учитывать все типы дисков, для разных компонентов архитектур.

Согласно проведённому исследованию стоимости дисковых накопителей (анализ производился для 206 моделей дисков, представленных в настоящее время на рынке), средняя стоимость HDD дисков в ~4.12 раза ниже стоимости SSD дисков [3, 4], что говорит о том, что при равном объёме финансовых затрат на развёртывание инфраструктуры хранения, инфраструктура, построенная на HDD дисках, позволит хранить в 4.12 раза больший объём информации, в ситуации, когда будет обеспечен достаточный уровень производительности.

При этом архитектура распределённой СХД Ceph позволяет повысить производительность распределённой СХД за счёт установки дополнительных высокоскоростных дисков, обеспечивающих кэширование данных.

Так же, при работе с распределёнными СХД следует учитывать особенности режимов работы с данными. важно определить параметры работы приложения с дисковой подсистемой, изменение которых может влиять на производительность:

•Случайность операций ввода/вывода. Определяется в процентном соотношении случайных операций к последовательным. При абсолютно случайном характере работы с диском, каждая новая операция при работе с подсистемой ввода/вывода требует определения блока дисковой подсистемы для работы с ним, произведение операций и переключение к следующему блоку и следующей операции.

•Характер операций ввода/вывода. Определяется в процентном соотношении операций чтения и операций записи. Операции записи всегда являлись наиболее затратными операциями по времени, так как после любой операции записи приложению требуется некое подтверждение, что блок данных был записан. Поэтому эти операции значительно влияют на производительность, а в случае распределенных систем блок данных обычно считается записанным только после подтверждения всеми участниками распределённой системы, иначе, в случае восстановления кластера, появляется риск получения ситуации Split-Brain, в которой на разных узлах будет записана разная информация.

•Глубина очереди записи. Определяется в единицах количества одновременных запросов к подсистеме ввода/вывода. Перед записью на диск данные могут формировать цепочку блоков, и быть записанными хоть с некоторой задержкой, зато со значительно большей скоростью. Для систем, требующих высокой скорости отклика, таких как базы данных, где важна минимизаций времени отклика, глубина очереди равна 1, что значит, что каждый блок сразу записывается на диск, без хранения в промежуточном кэширующем устройстве. Для систем, которым важен объём записываемой

информации, такие как системы видеонаблюдения, глубина очереди может достигать 256.

•Размер блока данных. Может изменяться от 4КБ до 512КБ. Данный размер указывает, блоками какого размере оперирует приложение. Чем больше размер блока, тем меньшее их количество будет принято дисковым устройством в единицу времени, при этом выше будет общий объём переданных данных.

•Количество потоков чтения и записи. Наличие нескольких поток одновременно могут как повышать общую производительность дискового устройства, за счёт наличия в нём нескольких модулей чтения записи, так и замедлять работу дискового устройства, из-за конкурентной борьбы между приложениями за ресурсы дисковой подсистемы.

Нагрузку, создаваемую пользовательским приложением, можно обозначить совокупностью следующих характеристик (1):

$$L_i = \{A_i, B_i, N_i, D_i, B_i\}, \quad (1)$$

где i – пользовательское приложение,

A – величина, определяющая соотношение случайных операций чтения и записи к линейным операциям чтения и записи,

B – величина, определяющая соотношение количества операций чтения к операциям записи для конкретного приложения,

N – значение глубины очереди записи, которое использует данное приложение,

D – дисциплина записи на дисковое устройство. Означает либо прямую запись, либо разрешение использования кэширующего устройства самого диска,

B – размер блока данных, которым оперирует пользовательское приложение.

Все эти параметры будут непосредственно влиять на производительность подсистемы хранения данных, которая будет определена следующей совокупностью характеристик (2):

$$P_{L_i} = \{k_i, V_t, \Delta tR_i, \Delta tW_i\}, \quad (2)$$

где t – минимальный промежуток времени доступа к данным, требуемым при данном типе нагрузки,

k – количество операций ввода и вывода в секунду для определенного тип нагрузки на систему хранения данных,

V – количество информации, записанное и считанное с хранилища данных за единицу времени, требуемое для конкретного типа нагрузки,

ΔtR – среднее время чтения блока данных с системы хранения данных,

ΔtW – среднее время записи блока данных на систему хранения данных.

Для проведения тестирования была спрофилирована нагрузка, позволяющая измерить значения P_{L_i}.

Для измерения максимальной задержки использовался следующий тест (табл. 1).

ТАБЛИЦА 1. Шаблон нагрузки для измерения максимальной задержки

```
[global]
bs=4K
iodepth=1
direct=1
ioengine=rbd
group_reporting
log_avg_msec=1000
time_based
runtime=600
numjobs=1
name=latency–test
rw=randwrite
[job1]
pool=bench–pool01
rbdname=testimg01
```

При реализации данного теста, основной задачей было выяснить минимальное время исполнения одной операции записи на диск. Используя блок данных минимального размера, глубину очереди записи на диск равной 1 и отключив все возможности кэширования данных, при проведении тестирования был получен минимальный результат времени задержки.

Для измерения количества операций ввода вывода использовался следующий тест (табл. 2).

ТАБЛИЦА 2. Шаблон нагрузки для измерения максимальной задержки

```
[global]
bs=4k
iodepth=128
direct=1
ioengine=rbd
group_reporting
time_based
log_avg_msec=1000
runtime=600
numjobs=10
name=iops_test
rw=randwrite
invalidate=1
ramp_time=30
write_lat_log=/root/fio–tests/iops/cpu_RDMA_offload_hdparm/lat–result.log

[job1]
pool=bench–pool01
rbdname=testimg01
```

При реализации данного теста был взят блок минимального размера, глубина очереди в 128 операций, а также были сконфигурированы 10 задач, для параллельного исполнения.

Данные шаблоны нагрузки позволяют образом отобразить производительность распределенной СХД, для оценки конкретных требований P_{L_i}.

Основная проблема распределенных систем хранения данных в том, что на все операции чтения и записи оказывают значительное влияние на сетевые задержки.

При взаимодействии пользовательского приложения с дисковым устройством в классической модели происходит обращение к модулю ядра, отвечающему за работу с устройством хранения (рис.). При таком подходе обращение к диску идет через один и тот же драйвер, что минимизирует накладные расходы при работе с такой системой.

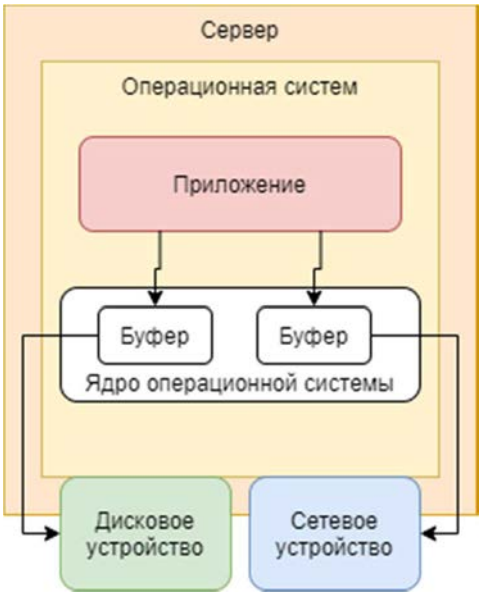


Рисунок. Классический интерфейс работы с дисковым устройством

В случае работы приложения с дисковым устройством, организуемым распределенной системой хранения данных, запись на дисковое устройство происходит в несколько этапов:

1) Обращение приложения к модулю ядра, отвечающего за хранение данных,

2) Обращение модуля ядра, отвечающего за хранение данных к приложению, управляющему работой РСХД,

3) Обращение приложения, отвечающего за работу РСХД к модулю ядра, отвечающему за работу с дисковыми устройствами (для записи локальной копии данных), и сетевому устройству (отвечающему за запись на удаленный узел),

4) Обращение модулей ядра к соответствующим дисковым устройствам и сетевым устройствам,

5) Передача данных на удаленный узел, где все эти операции повторяются.

При этом, так как данной производительности хватает большинству современных систем, распределенные системы хранения данных пользуются значительным спросом.

Так как основным компонентом распределенной системы является приложение, работающее в пространстве пользователя и обращающееся напрямую к дисковым устройствам, от его работы зависит производительность всей системы. На основании проведенного анализа, для комплексного тестирования производительности распределенной программно-определяе-

мой СХД были разработаны типы профилей нагрузки, позволяющей получить значение значения производительности (P_{Li}) для разных типов нагрузки.

Список используемых источников

1. Зарубин А. А., Елагин В. С., Савельева А. А., Швидкий А. А. Подходы к моделированию нагрузки на распределенную систему хранения данных // Системы синхронизации, формирования и обработки сигналов. 2018. Т. 9, № 3. С. 90–95.

2. CEPH hardware recommendations. URL: https://docs.ceph.com/en/latest/start/hardware-recommendations/ (дата обращения: 09.03.2022).

3. Internal SSD prices. URL: https://diskprices.com/?locale=us&condition=_new&disk_types=internal_ssd (дата обращения: 10.03.2022).

4. Internal HDD prices. URL: https://diskprices.com/?locale=us&condition=new&disk_types=internal_hdd (дата обращения: 10.03.2022).

Статья предоставлена заведующим кафедрой ИКС СПбГУТ, кандидатом технических наук, доцентом А. А. Зарубиным.

УДК 004.056(075.8)
ГРНТИ 81.96

ФОРМАЛИЗАЦИЯ МОДЕЛИ ФИЗИЧЕСКИ НЕКЛОНИРУЕМОЙ СИСТЕМЫ НА ОСНОВЕ УНИВЕРСАЛЬНОГО КЛАССА ХЭШ-ФУНКЦИЙ

В. А. Яковлев

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Физически неклонируемой функцией (ФНФ) называется характеристика физической (цифровой) системы, неподдающейся клонированию (воспроизведению, копированию) на других физических системах. Одним из важных параметров ФНФ является непредсказуемость отклика для заданного запроса. Проблема формализации параметров ФНФ состоит в том, что при ограниченных физических (линейных) размерах ФНФ, количество ФНФ полиномиально ограничено, поэтому выходные характеристики разных ФНФ при одинаковых запросах становятся повторяющимися. Предлагается формализация параметра ФНФ на основе использования класса строго универсальных$_2$ хеш-функций, что позволяет количественно оценить параметр непредсказуемости ФНФ и сформулировать требования к ФНФ, используемых в различных приложениях.

физически неклонируемые функции, универсальные хэшфункции, непресказуемость.

Физически неклонируемые функции приобрели широкую популярность в последние 10–15 лет для решения различных аспектов информационной безопасности и в первую очередь решения задач аутентификации. Обзор достижений в этой области и описание принципов построения ФНФ приведены в работах [1–5].

По определению, данному в [1], физически неклонируемой функцией - ФНФ (от англ. PUF - Physical Unclonable Function) является характеристика физической (цифровой) системы, которая не поддается клонированию (воспроизведению, копированию) на других физических системах. Физически неклонируемые функции наследуют свою неклонируемость от того факта, что они состоят из множества случайных компонентов, которые присутствуют в производственном процессе и не поддается контролю.

ФНФ можно описать значениями пар входных и соответствующих им выходных параметров (сигналов): $R = f(C)$, где входной сигнал $C = c_1, c_2, ..., c_t$ называется запросом, выходной сигнал $R = r_1, r_2, ..., r_k$ называется ответом (откликом). Пара, состоящая из входного физического параметра (запроса) и выходного параметра (отклика), называется парой запрос – оклик (*Challenge-Response Pair* – CRP).

ФНФ должны удовлетворять следующим требованиям [1]:

1. Сигнал отклика R может быть извлечен неоднократно и надежно путем проведения измерений для запроса C .

2. Число возможных запросов C_i должно быть настолько большим, что все соответствующие ему отклики R_i не могут быть получены путем перебора за обозримое время.

3. Так как в физической системе расположено чрезвычайно большое количество данных, определяющих ответ на поданный запрос, рассчитать, смоделировать или любым другим способом вычислить пару запрос – отклик (C, R) при знании другой пары (C', R') или некоторого количества таких пар должно быть вычислительно невозможным.

4. Клонирование заданной физической системы другой физической системой, которая описывается аналогичным множеством пар запрос-отклик, или ее физическое воспроизведение должно быть чрезвычайно сложным.

В настоящее время предложено много типов ФНФ: оптические ФНФ, покрывающие ФНФ, ФНФ арбитрового типа, ФНФ на основе кольцевых генераторов, ФНФ на основе статического оперативного запоминающего устройства, ФНФ типа бабочка (защелка, мультивибратор), ФНФ на основе сбоев, комбинированные ФНФ. Их сравнительный анализ приведен в [5].

Для применения ФНФ в различных приложениях необходимо из множества видов выбрать те, которые удовлетворяют требованиям в конкрет-

ном приложении. Для более точного описания ФНФ и формулирования требований к ним целесообразно рассмотреть формализованную модель ФНФ. В одной из первых работ по ФНФ [3] эти функции назывались физически однонаправленные функции. В [4] использовалось название физически случайные функции, в [2] введены понятия сильных физически неклонируемых функции и физически неклонируемые функции с обфускацией. Наиболее полная характеристика ФНФ дана в монографии [5], в которой авторы наряду с определением физически неклонируемой функции ввели понятия, физически неколонируемой системы и физически неклонируемой инфраструктуры. В [5] характеристики ФНФ определяются такими свойствами: робастность; неклонируемость; непредсказуемость.

Робастность можно определить, как способность ФНФ сохранять свои свойства, в частности, однозначность отображения $C \to R$ при изменении условий функционирования ФНФ (температуры, влажности, напряжения питания и пр.) Для повышения устойчивости к дестабилизирующим факторам используют дополнительные меры, например, помехоустойчивые коды. В этом случае говорят о системе ФНФ [5].

Неклонируемость. Понятие неклонируемости в [5] рассматривается в двух видах:

Экзистенциальная неклонируемость. По ней понимается невозможность нарушителя создания двух ФНФ с одинаковыми свойствами.

Селективная неклонируемость. Под которой понимается невозможность создания новой ФНФ, которая является клоном исходной при доступе злоумышленника к исходной ФНФ. При этом предполагается, что выполняется ряд ограничений, например, время доступа к ФНФ ограничено, злоумышленник не может физически воздействовать на ФНФ, чтобы себя не обнаружить, злоумышленник может воспользоваться побочными каналами и т. п.

Применительно к системам аутентификвации наиболее важным свойством является непредсказуемость отклика ФНФ [6].

Введем следующие обозначения:

$\{C\}$ – множество запросов на входе ФНФ; $\{R\}$ – множество откликов на выходе ФНФ; $\{C,R\}_s$ – множество пар запрос-отклик s-й ФНФ; $\{F\}$ – множество ФНФ для выбранной технологии изготовления с заданными парами отображений $R = f(C)$; $\{F_{ij}\}$ – подмножество ФНФ для заданной пары (C_i, R_j); $|A|$ – мощность произвольного множества А.

Непредсказуемость ФНФ можно определить в узком и широком смысле.

Непредсказуемость в узком смысле определяется для отдельной ФНФ следующим образом. При любом случайном равновероятном выборе запроса C_i вероятность появления отклика R_i близка к вероятности $\frac{1}{|R|}$. Если задано некоторое подмножество откликов $\{\hat{R}\} \subset \{R\}$, которые используются в каком-либо приложении ФНФ, то вероятность успеха атаки угадывания нарушителем любого отклика из $\{\hat{R}\}$ будет равна $\frac{|\hat{R}|}{|R|}$.

Если выполняется условие $|\hat{R}| \ll |R|$, то вероятность угадывания отклика на случайный запрос пренебрежимо мала.

В широком смысле непредсказуемость определим, как невозможность формирования одинаковых откликов разными ФНФ. Как известно, количество вариантов отображений вида $X^k \to Y^k$, где $X, Y \in (0,1)$ определяется количеством булевых *k*-мерных функций и равно $(2^{2^k})^k$. Откуда следует, что даже при умеренных *k* вероятность появления двух одинаковых отображений ничтожно мала. Однако, такая идеализация ФНФ не подтверждается практикой. В [2] отмечается, что для любой физической системы число ее состояний полиномиально зависит от ее линейных размеров. Поэтому приведенная оценка количества ФНФ не может быть достигнута на практике. Следовательно, необходимо допустить, что количество ФНФ полиномиально зависит от мощности множества откликов, то есть $|F| = Poly(|R|)$. Это означает возможность существования подмножеств $\{F_{ij}\}$, которые имеют одинаковые CRP в некотором количестве.

В этой связи нужно иметь возможность оценки мощности таких подмножеств и количества совпадающих CRP в них.

Применим для моделирования взаимосвязи CRP разных ФНФ класс строго универсальных$_2$ хэш-функций, предложенных Вегманом и Картером [7].

Определение. Классом *строго универсальных* хеш-функций называется такое множество отображений $H : X \to Y$, что:

1) для любых $x \in X, y \in Y$: $\#\{h \in H : y = h(x)\} = \frac{|H|}{|Y|}$,

где $|H|$ – общее количество хеш-функций h, $|Y|$ – общее количество хеш-кодов Y, #{..} – количество хеш-функций, удовлетворяющих условию, представленному в фигурных скобках;

2) для любых $x_1, x_2 \in X$, $x_1 \neq x_2$ и $y_1, y_2 \in Y$

$$\#\{h \in H : h(x_1) = y_1, h(x_2) = y_2\} = \frac{|H|}{|Y|^2}.$$

Применительно к ФНФ введем понятие класса ФНФ, под которым будем понимать множество ФНФ, выполненных по одинаковой технологии и имеющих фиксированные параметры сигналов запроса и отклика.
Тогда из условия 1) следует, что для любой CRP

$$\left|F_{ij} : C_i \to R_j\right| = \frac{|F|}{|R|}. \quad (1)$$

Выполнение условия 2) для ФНФ означает, что количество ФНФ для которых $(C_i \xrightarrow{F_{ir}} R_r, C_j \xrightarrow{F_{js}} R_s), C_i \neq C_j$ определяется мощностью пересечения двух подмножеств $F' = F_{ir} \bigcap F_{js}$ и обратно пропорционально квадрату мощности множества откликов $|R|$

$$|F'| = \frac{|F|}{|R|^2}. \quad (2)$$

В частном случае, когда сигнал отклика ФНФ R – двоичная последовательность длиной k символов, количество возможных ответов равно числу всевозможных двоичных комбинаций длины k, то есть $|R| = 2^k$, из (1) и (2) следует

$$\left|F_{ij} : C_i \to R_j\right| = \frac{|F|}{2^k}, \quad |F'| = \frac{|F|}{\left(2^k\right)^2}.$$

Из (1), (2) несложно увидеть, что если $|F'| = 1$, то количество ФНФ $|F| = |R|^2$, то есть имеет полиномиальную (полином второй степени) зависимость от $|R|$.

В предлагаемой модели ФНФ количество возможных ФНФ полиномиально (степень полинома равна двум) зависит от числа выходов ФНФ то есть от ее размеров, что не противоречит практике и позволяет сделать количественную оценку параметров системы защиты, например, системы аутентификации, в которой она будет применяться. Таким образом можно предложить следующую модель физически неклонируемой системы:

– количество разрядов двоичного представления отклика – k (размерность ФНФ) линейно зависит от ее физического размера;

– количество пар (CRP) имеет экспоненциальную зависимость от размерности ФНФ $|R| = 2^k$;

– количество ФНФ полиномиально зависит от мощности отклика $|F| = Poly(|R|) = |R|^2$.

В дальнейшем планируется использовать данную модель для аутентификации ключей, распределяемых по методу Диффи-Хеллмана [6, 8].

Список используемых источников

1. Ярмолик В. Н., Вашинко Ю. Г. Физически неклонируемые функции // Информатика. 2011. N 2. С. 92–104.

2. Rührmair U., Sölter J., Sehnke F. On the Foundations of Physical Unclonable Functions. 2009.

3. Tuyls P., Skoric B., Kevenaar T. Security with Noisy Data: Springer, 2007. 344 pp.

4. Gassend B., Physical Random Functions, MSc Thesis, MIT, 2003

5. 1Maes R. Physically Unclonable Functions: Constructions, Properties and Applications: Katholieke Universiteit Leuven, 2012. 234 pp.

6. Яковлев В. А., Хворова И. О. Аутентификация ключей, распределяемых на основе EVSkey-схемы и использования физически неклонируемых функций // Актуальные проблемы инфотелекоммуникаций в науке и образовании. IX Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2020. Т. 1. С. 802–807.

7. Carter J.l., Wegman M.N. New Hash functions and Their Use in authentication and Set Equality.//Journal of Computer and System Sciences. 1981; 22: pp. 265−278.

8. Diffie M., Hellman M. New directions in cryptography // IEEE Transactions on Information Theory. 1976; 22(6):644–654. DOI:10.1109/TIT.1976.1055638.

УДК 004.056(075.8)
ГРНТИ 81.96

СИСТЕМА РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ ПО ПОСТОЯННЫМ КАНАЛАМ НА ОСНОВЕ ПРОТОКОЛА ОБМЕНА ЧИСЛАМИ МЕЖДУ КОРРЕСПОНДЕНТАМИ

В. А. Яковлев

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Рассматривается сеть связи из M корреспондентов. Для работы корреспондентов каждый с каждым в защищенном режиме они формируют парные ключи следующим образом. Каждый корреспондент, например, A формирует: a – секретное гауссовское случайное число с параметрами (0,1); $(a+n_a)$ – открытое случайное число, где n_a – гауссовское случайное число с параметрами $(0,\sigma^2)$. Открытые случайные числа все корреспонденты помещают в хранилище, доступ в которое имеет каждый корреспондент, в том числе злоумышленник E (без права модификации чисел). Если корреспонденты A и B хотят сформировать общий ключ, то они обращаются в хранилище открытых чисел и получают в нем числа $b+n_b$ (корр.) A и $a+n_a$ (корр.B) соответственно и формируют биты «сырого» ключа: $K_A = p(g+n_B)$ корр. A и $K_B = q(p+n_A)$ корр.B. Злоумышленник E может сформировать оценку ключа пары корреспондентов $K_{E(AB)} = (a+n_a)(b+n_b)$. Доказаны следующие утверждения:

1. Ключи любой пары корреспондентов A и B некоррелированы с ключем третьего корреспондента C.

2. Оценки ключа, нарушителя относительно ключей двух пар корреспондентов K_{EAB} и K_{EAC}, некоррелированы.

криптография, распределение ключей, бесшумные каналы.

Рассматривается сеть связи из M корреспондентов. Корреспонденты должны работать каждый с каждым в защищенном режиме. Для этого они формируют парные ключи следующим образом (рис.).

Каждый корреспондент, например A, формирует:

– a – секретное гауссовское случайное число с параметрами (0,1);

– $(a+n_a)$ – открытое случайное число, где n_a – гауссовское случайное число с параметрами $(0,\sigma^2)$.

Открытые случайные числа все корреспонденты помещают в хранилище, доступ, в которое имеет каждый корреспондент, в том числе злоумышленник (без права модификации чисел).

Если корреспонденты A и B хотят сформировать общий ключ, то они обращаются в хранилище открытых чисел и получают в нем числа $b + n_b$

корреспондент А и $a + n_a$ корреспондент В соответственно. Далее корреспонденты формируют значения так называемого «сырого» ключа:

$$\text{A: } K_{AB} = a(b + n_b)$$
$$\text{B: } K_{BA} = b(a + n_a)$$

(здесь и далее первый символ в обозначении ключа соответствует корреспонденту, использующему свое секретное число, второй символ соответствует корреспонденту, чье открытое число используется). Если корреспондент С будет работать с А, то они будут формировать ключи:

$$\text{A: } K_{AC} = a(c + n_c), \text{ C: } K_{CA} = c(a + n_a)$$

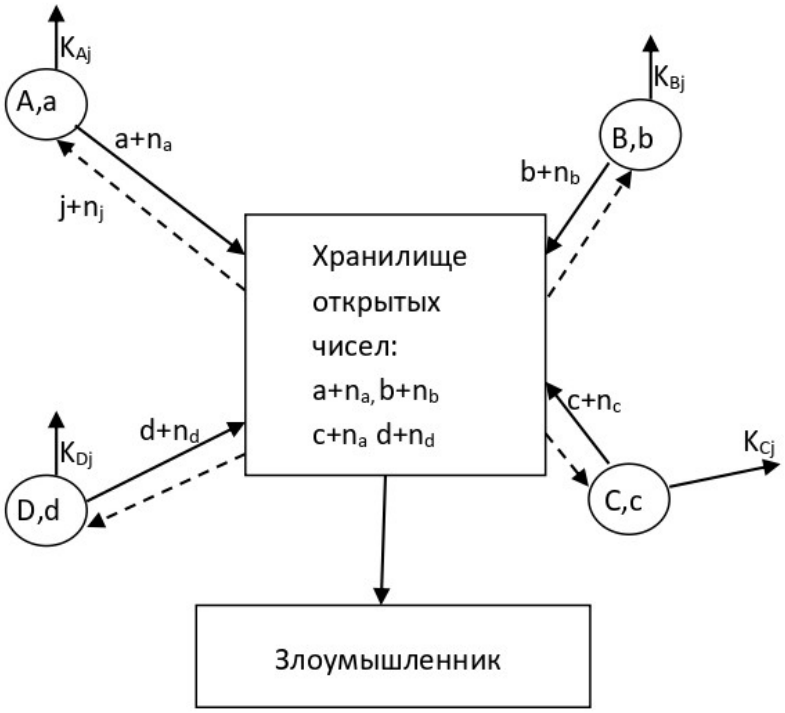


Рисунок. Система распределения парных ключей
с открытыми индивидуальными числами

То есть, если корр. А формирует ключи с разными корреспондентами, он использует одно и то же случайное число *a*. И соответственно все корреспонденты берут из хранилища открытое число $a + n_a$.

Злоумышленник имеет доступ ко всем открытым числам корреспондентов, и знает, кто с кем формирует ключ. Поэтому, если А и В формируют ключ, то нарушитель выбирает из хранилища числи $a + n_a$ и $b + n_b$ и формирует ключ

$$K_{EAB} = (a + n_a)(b + n_b),$$

если А и С формируют ключ, то нарушитель выбирает из хранилища чисел $a + n_a$ и $c + n_c$ и формирует ключ

$$K_{EAC} = (a + n_a)(c + n_c).$$

Пусть $\tilde{K}_{AB}, \tilde{K}_{BA}, \tilde{K}_{AC}, \tilde{K}_{CA}$ квантованные на два уровня по знаку числа значения соответствующих СВ. Обозначим

$p_m = \tilde{K}_{AB} \neq \tilde{K}_{BA}$ – вероятность несовпадения ключей у А и В,
$p_e = \tilde{K}_{AB} \neq \tilde{K}_{EAB}$ – вероятность несовпадения ключей у А и Е.

Для доказательства работоспособности системы нужно доказать выполнение по крайней мере трех утверждений:

1. Любая пара корреспондентов может организовать протокол взаимного обмена, в результате которого будут созданы условия:

$p_m \leq \tilde{p}_m$ – условие очистки ключа от ошибок за счет помехоустойчивого кодирования;

$p_e \geq \tilde{p}_e$ – условие применения *теоремы усиления секретности* [1], выполнение которой обеспечивает безусловную стойкость системы (здесь $\tilde{p}_m, \tilde{p}_e$ – некоторые пороговые значения).

2. Ключи, формируемые корреспондентами и рассматриваемые как случайные величины, независимы в парах, то есть K_{AB} *и* K_{AC} независимы, K_{BA} *и* K_{CA} независимы.

3. Ключи, формируемые нарушителем, независимы в парах, то есть K_{EAB} *и* K_{EAC} независимы.

Утверждение 1 можно считать доказанным, см. [2, 3] и статью в настоящем сборнике [4].

Для доказательства утверждения 2 докажем следующую лемму.

Лемма 1. *Ключи* K_{AB} *и* K_{AC}*, формируемые корр. А для связи с корр. В и С некоррелированы. Ключи* K_{BA} *и* K_{CA}*, формируемые корр. В и С для связи с А соответственно, некоррелированы.*

Доказательство.

Запишем выражение для коэффициента корреляции СВ K_{AB} **и** K_{AC}

$$R(K_{AB}, K_{AC}) = \frac{E(K_{AB} \cdot K_{AC}) - E(K_{AB}) \cdot E(K_{AC})}{\sqrt{D(K_{AB}) D(K_{AC})}},$$

где *E()* – матожидание, *D()* – дисперсия.

Запишем

$$E(K_{AB}) = E(a(b + n_b)) = E(ab + an_b) = E(ab) + E(an_b) =$$
$$E(a)E(b) + E(a)E(n_b).$$

Последнее равенство следует из независимости СВ a,b,n_a,n_b. Так как по условию матожидание всех СВ равно нулю, то $E(K_{AB}) = 0$. Аналогично можно показать, что $E(K_{AC}) = 0$.

Найдем $E(K_{AB} \cdot K_{AC})$.

$$E(K_{AB} \cdot K_{AC}) = E(a(b + n_b)a(c + n_c)) = E((ab + an_b)(ac + an_c)) =$$
$$E(aba\,c + an_b a\,c + aban_c + an_b an_c) = E(a^2(bc + n_b\,c + bn_c + n_b n_c)) =$$
$$E(a^2)E(bc + n_b\,c + bn_c + n_b n_c) = E(bc + n_b\,c + bn_c + n_b n_c) = 0$$

Таким образом, числитель в (1) равен 0, следовательно, ключи K_{AB} и K_{AC} некоррелированы. Аналогично доказывается, что ключи K_{BA} и K_{CA} некоррелированы. Лемма 1 доказана.

Для доказательства третьего утверждения докажем лемму.

Лемма 2. *Ключи K_{EAB} и K_{EAC}, формируемые нарушителем, как аналоги ключей K_{AB} (корр. А для связи с корр. В) и K_{AC} (корр. А для связи с корр. С) некоррелированы.*

Доказательство.

В силу того, что исходные СВ a,b,n_a,n_b имеют нулевые матожидания и независимы, можно записать:

$$E(K_{EAB}) = E(a + n_a)(b + n_b) = E(ab + bn_a + an_b + n_a n_b) = 0$$
$$E(K_{EAC}) = E((a + n_a)(c + n_c)) = E(ac + cn_a + an_c + n_a n_c) = 0$$
$$E(K_{EAB} \cdot K_{EAC}) = E((a + n_a)(b + n_b)(a + n_a)(c + n_c)) =$$
$$E((a + n_a)^2(b + n_b)(c + n_c)) = E(a + n_a)^2 E((b + n_b)(c + n_c)).$$

Несложно увидеть, что $E((b + n_b)(c + n_c)) = 0$, Поэтому $E(K_{EAB} \cdot K_{EAC}) = 0$. Таким образом, ключи, которые формирует злоумышленник, как аналоги ключей двух корреспондентов для связи с третьим корреспондентом являются некоррелированными. Лемма 2 доказана.

Как известно, из некоррелированности СВ не следует их независимость. Поэтому необходимо доказать, что сформированные значения сырого ключа независимы. Эта часть работы составляет перспективу дальнейшего исследования предлагаемой системы распределения ключей.

Список используемых источников

1. Maurer U., Secret key agreement by public discussion from common information, IEEE Transactions on Information Theory, 39:3 (1993). pp. 733–742.

2. Яковлев В.А, Коржик В. И. Вероятности ошибок при распределении ключей по бесшумным постоянным каналам с использованием добавления искусственного шума // Актуальные проблемы инфотелекоммуникаций в науке и образовании. IX Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2020. Т. 1. С. 802–807.

3. Yakovlev V., Korzhik V., Akhmetshina A., Zhuvikin M. Key Sharing Protocol Using Exchange by Integers over Public Noiseless Channels Between Users that Provides Security without Cryptographic Assumptions // The 31th Conference of Open Innovations Association FRUCT Helsinki, Finland .

4. Яковлев В. А, Коржик В. И. Протокол распределения ключей по постоянным каналам на основе совместного применения интерактивных протоколов обмена данными // Актуальные проблемы инфотелекоммуникаций в науке и образовании. XI Международная научно-техническая и научно-метод. конференция: сб. научн. ст. СПб.: СПбГУТ, 2022. (В настоящем сборнике).

A N N O T A T I O N S

PLENARY MEETING

Shestakov A. Perspective Directions on the Results of Science and Technology in the Russian Federation and SPbSUT. – PP. 5–21.
The scientific activity of the St. Petersburg State University of Telecommunications named after Professor Bonch-Bruevich is developing in accordance with global trends in applied scientific research of breakthrough digitalization technologies in all spheres of human activity, including in organizing and providing training for new-formation specialists according to national programs and federal projects of the Russian Federation. The main vectors of the promising scientific problems of the university and changes in the concept of harmonization of regulatory regulation in the country are considered, taking into account the international activities of university representatives at specialized sites of various United Nations institutions, such as the Study Commissions of the ITU and the ISO. The activities of the Organization for International Cooperation in Education, Science and Communications (UNESCO) present the results of theoretical and practical approaches to the implementation of the concept of mobile learning of the university, which are based on the author's models of digital transformation of educational content, accessibility technologies to digital educational resources, taking into account modern international factors and risks.
Key words: science, technology, applied research, telecommunications, digital transformation, mobile learning, educational and didactic content.

Muthanna A. S. A. Migration of Intelligence Services in a Distributed Environment as One of the Key Directions in the Development of Infocommunications. – PP. 22–29.
The 5G and next generation networks are designed to integrate all mobile and fixed networks to provide ultra-high data rates, enabling a range of new services with new cloud computing structures such as fog computing and edge computing. An important direction in the development of communication network technologies is URLLC (Ultra-Reliable Low Latency Communication), which is created in order to achieve the lowest possible latency indicators while maintaining high transmission reliability. This article will focus on the URLLC technology. This task should be solved through the use of artificial intelligence and live migration tools, taking into account modern trends in the field of communications.
Key words: 5G, service migration, edge computing

INFORMATION AND COMMUNICATION NETWORKS AND SYSTEMS

Шестаков А. В., Ураго А. В., Гордеев М. А. Разработка программного обеспечения для аутентификации по QR-коду как интернет-сервиса. – С. 30–35.

Распространение информационных технологий в течение последних десятилетий в нашей повседневной жизни стремительно расширяется, одновременно с потребностью в более совершенных мерах кибербезопасности. При этом наиболее критичная часть кибербезопасности – люди и процедуры их аутентификации. Представлены результаты анализа существующих методов аутентификации и предложенное оригинальное решение проблемных вопросов – разработанное программное обеспечение, которое значительно упрощает работу с учетными данными, повышает их безопасность в пользовательском оборудовании и реализует более сложные комплексные механизмы учетных данных. Представлена структура и характеристики оригинального программного обеспечения: мобильного приложения (менеджера паролей), веб-приложения и средств разработки для сторонней интеграции.

Ключевые слова: QR-код, аутентификация, интернет-сервис, кибербезопасность, защита данных, пароли.

Михайличенко А. В., Паращук И. Б. Интеллектуальные системы для анализа технической надежности мобильных центров обработки данных. – С. 35–40.

Рассматриваются вопросы автоматизированного анализа технической надежности современных мобильных центров обработки данных, реализовано формальное описание состава интеллектуальных систем анализа их технической надежности. Данные интеллектуальные системы содержат элементы, призванные в автоматизированном режиме количественно оценивать показатели технической надежности современных мобильных центров обработки данных. Они призваны выступить в роли системы поддержки принятия решений в интересах гарантированного обеспечения безотказности, долговечности и ремонтопригодности центров обработки данных, что позволит повысить объективность управления такими центрами, а также достоверность и оперативность решения задачи анализа технической надежности систем такого класса.

Ключевые слова: интеллектуальная система, анализ, техническая надежность, центр обработки данных, нечеткость, долговечность, ремонтопригодность.

Abbasov M., Dagaev A. Network Load Balancing. – PP. 40–46.

The article provides a brief overview of the basic principles of balancing global and local networks. The stages of solving the load balancing problem are proposed. The levels of Network Load Balancing are considered, as well as its main algorithms: DNS, Round Robin, Weighted Round Robin, Random, IP Hash, which can be implemented depending on the specifics of a particular project to achieve a further goal.

Key words: Load Balancing, Load Balancing, OSI network model, DNS, Round Robin, Weighted Round Robin, Random, IP Hash, equally probable balancing.

Abramenko G., Vitkova L., Melnik M. Overview of Tools for Monitoring Local Information Security Events. – PP. 46–49.
Today, more than ever, information that is processed, stored and transferred between various information systems is of key importance. It is critically important for the state and business to continuously and correctly perform all processes, and ensure confidentiality, integrity and availability. The article discusses the functional characteristics of the ISMS and compares SIEM systems from foreign and domestic manufacturers.
Key words: analysis of local incidents, information security monitoring, SIEM, information security.

Abramenko G., Lansere N., Fadeev I. Analysis of the Features of Subjects of the Critical Information Infrastructure of the Russian Federation Functioning in the Field of Science. – PP. 49–54
The article discusses typical objects of the critical information infrastructure of the Russian Federation (CII), CII subjects operating in the field of science, determines the specifics of critical processes for this area, analyzes typical CII objects, assesses vulnerabilities for the software and hardware used.
Key words: critical information infrastructure, CII, vulnerabilities, current threats, import substitution, science.

Abramov S., Abramova E., Pavlov I., Pavlova M. Methods of Synthesis of Invariant Message Transmission Systems with Constant Parameters and Invariant to Additive Interference. – PP. 54–61.
The article discusses the methods underlying the synthesis of message transmission systems with constant parameters invariant to additive interference. The first method consists in finding an invariant operator, which has a number of significant disadvantages. The second method is to find the optimal signal, with this method the lowest probability of error is achieved.
Key words: absolute invariance, additive interference, modulation, demodulation, invariant system, invariant message transmission systems.

Aleksandrov I., Fomin V. Using Bagging Technology to Improve the Efficiency of Data Classification Based on Metric Proximity. – PP. 61–65.
The problem of pattern recognition is considered as a classification problem based on supervised learning. The possibility of using bagging for decision function methods is investigated, the possibility of using the bootstrap aggregating method to improve the accuracy of classification in the framework of the problem of diagnosing diabetes is checked. The measurements were carried out according to two efficiency criteria - the metrics of completeness and accuracy. Experimental results are presented that prove the expediency of integrating individual methods into an ensemble in order to improve the accuracy of classification.
Key words: pattern recognition, decision function methods, data classification, bagging.

Alekseeva N., Redrugina N., Saveleva A., Tarabanov I. Mathematical Modeling of Data Transfer Between Nodes in Software Defined Storage. – PP. 65–70.
This article describes the process of constructing a functional model of a software defined storage (SDS) in terms of the process of writing data blocks to system disks. The procedure for

writing data to disks in a distributed storage system differs in the need for data replication. A comparative analysis of synchronous and asynchronous approaches to data replication and their impact on QoS and QoE is made. Operating with input data made it possible to predict the behavior of the system and analyze approaches to solving possible problems.
Key words: software defined storage, analytical modeling, queuing system.

Alekhin R., Krasov A., Makarova A., Orlov G. Cloud Services. The Principle of Operation, Classification and Service Models. – PP. 70–74.
Nowadays, with constant volumes of storage, received and stored information, the requirements for data storage methods in data processing are increasing. The demand for the use of cloud services is growing. This article discusses the basic information on processing data for processing data centers and considering the types of cloud infrastructures, characteristics and classification of service models from the side of cloud service operations.
Key words: cloud services, Cloud infrastructure, SaaS, PaaS, DaaS, IaaS, Cloud service's operator, Data processing center.

Al-Sweity Malik A. M., Muthanna A. S. A. Comparative Analysis of C-V2X and DSRC Technologies. – PP. 75–79.
This paper investigates the effect of vehicle speed on C-V2X-4 mode characteristics based on an open-source simulator. The effects of speeds on detection window functions and resource conservation probabilities are also analyzed accordingly. The study finds that low speeds negatively affect the performance of C-V2X while decreasing the performance more steadily at high speeds. Faster vehicles can tolerate higher packet frequencies because the effect of speed can be compensated. Also, data was collected to compare DSRC and Cellular V2X (C-V2X) radio technologies for their application to deliver broadcast V2X security messages.
Key words: modeling, migration, multimedia tasks, V2X networks, DSRC.

Al-Sweity Malik A. M., Muthanna A. S. A. Scenarios and Methods of Application of the UAV in the Concept of Autonomous Guided Transport. – PP. 79–82.
The UAV are a network node in Vanet's infrastructure, just like the other nodes. The UAV create communication channels both with the vehicles (obu) and with its services and applications. While in flight, the biplanes can provide long-term communications for most vehicles due to the fact that they are high up and interact with the vehicles within line of sight. The use of UAV also allows a significant increase in communication distance between network nodes. The distance is increased because the UAV are much higher above the ground and buildings than the obu equipment, so the signals disappear and are absorbed by the surrounding objects and landscape to a lesser extent.
Key words: UAV, AV, VANET, DSRC

Andreeva E. Metods of Measuring the Parameters of Ultrashort Optical Pulses for High-Speed Fiber-Optical Data Transmission Systems. – PP. 83–86.
Methods for measuring ultrashort optical pulses used in high-speed optical fiber DWDM systems are studied. The need for accurate measurement of a set of parameters of ultrashort optical pulses, including their time-frequency and energy characteristics, is shown.
Key words: optical fiber systems, optical fiber, ultrashort optical pulses, lasers, nonlinear effects.

Andreeva E., Ermolaev A., Hitrov P. Methods for Forming Ultrashort High-Power Optical Pulses Taking Into Account the Linear and Nonlinear Fiber Properties. – PP. 86–91.
Methods for the formation of high-power ultrashort optical pulses in optical fibers have been studied. It is shown that the process of self-compression of an optical chirped pulse can be used in the linear propagation mode. The greatest effect is achieved in the case of nonlinear "multi-soliton" self-compression of the optical pulse. Numerical estimates are given for such a case.
Key words: fiber optics systems, optical fiber, ultrashort optical pulses, lasers, optical solitons.

Andreeva E., Yakovlev N. The Research of Influence of Four-Wave Mixing Effect on Telecommunication Systems Transmission Quality and Ways to Weaken it. – PP. 91–94.
Comprehensive development of communication systems, fiber-optic communication lines, in particular, are in count of main directions of modern scientific and technological progress. Nowadays FOCL's have large information capacity with a length of regeneration sections of up to 200 km and more. This became possible thanks to WDM technology. While using this technology, one has to deal with nonlinear optical effects which show up in active environment. This article will discuss influence of nonlinear effect of four-wave mixing (FWM) on transmission quality in WDM systems.
Key words: telecommunication systems, four-wave mixing, nonlinear optic effects.

Andryunin A., Bylina M. Virtual laboratory installation for studying the effect of a quantum eraser. – PP. 95–100.
Currently, modern technologies based on the phenomena of quantum physics have acquired particular importance. Now it is one of the most promising areas of science and technology, relating to end-to-end digital technologies. Graduates of the faculties "Infocommunication Technologies and Communication Systems" and "Photonics and Optoinformatics" should receive basic knowledge and skills in this promising area, so SPbSUT is actively working to introduce disciplines related to quantum technologies into the curricula. These disciplines require a laboratory workshop. This paper presents a virtual laboratory setup for studying the quantum eraser effect, simulating an interference experiment that demonstrates quantum entanglement and the principle of complementarity.
Key words: interference, single photon, quantum state, Mach-Zehnder interferometer, quantum eraser, virtual laboratory work.

Antonenko A., Gerasimova Y., Dunaytsev R. A Study on the Efficiency of Transmit Beamforming in IEEE 802.11ac Networks. – PP. 100–105.
Adaptive beamforming technology, also known as transmit beamforming, involves the formation of the electromagnetic field of antennas of the transmitting device in the form of a narrowly focused main lobe oriented towards the receiving device with the ability to change its direction when needed. This technology first appeared in the IEEE 802.11n standard and has been further developed in the subsequent IEEE 802.11ac and IEEE 802.11ax standards. The paper presents the results of an experimental study on the efficiency of transmit beamforming in IEEE 802.11ac networks. The effective data rate, retry rate, and received signal strength are analyzed with and without the use of this technology.
Key words: IEEE 802.11ac, TxBF, transmit beamforming.

Akhmetshina M., Mankaev R., Yakovlev V. Experimental Study of Key Distribution Protocol over Constant Channels with the Addition of Artificial Noise. – PP. 105–109.
An experimental study of the key distribution protocol over permanent silent channels, consisting of a numerical raw key bit distribution protocol and a basic channel predominant enhancement protocol, has been conducted. A set of programs was developed to simulate the formation of key bits by legitimate users and an intruder and to perform statistical analysis of error distribution in the symbols of the key sequence. The experimental results are in good agreement with theoretical calculations.
Key words: key distribution protocols, cryptographic transformations, S-blocks.

Akhrameeva K., Gerling E., Kulikov I. Possibilities of Using Linguistic Steganography Depending on the Genre of Computer Games. – PP. 110–113.
This article discusses the possibility of using linguistic steganography and creating steganographic systems using linguistic steganography based on modern computer games and game mechanics. Modern computer games are divided into many different genres with their own features, as well as gaming, cooperative and communication mechanics. This article discusses ways to create steganographic systems, depending on the game genre and features of game mechanics of certain genres of computer games. The article also discusses ways to create steganographic systems based on communicative mechanics and methods of in-game interaction between players.
Key words: steganography, content-aware steganography, computer games.

Akhrameeva K., Kuznetsov S., Kulikov I., Fominykh A. Implementation of Honeypot Auto-assembly on Linux Operating Systems using Vagrant Software. – PP. 114–118.
This article discusses the problematic issue of implementing honeypot auto-assembly on Linux operating systems using Vagrant software. Existing off-the-shelf image builds are often built on outdated OS versions and, in essence, are only suitable for educational purposes. This article describes how to install a honeypot on modern operating systems of the Linux family and how to adapt the PenTBox security package to ensure its stable operation on the latest operating systems. The article also discusses the possibility of automatically installing the necessary security packages on an "empty" OS and auto-assembly of the OS using Vagrant software to create a ready-made OS image with a pre-installed honeypot.
Key words: honeypot, vagrant, linux, pentbox.

Babaev A., Javarova E., Ibrahimov B., Ismayilova S. Analysis Methods and Means Increasing the Noise Immunity Fiber-Optical Transmission Systems Based on Spectral Technologies. – PP. 118–124.
Methods and means increasing the reliability optical signal transmission in fiber-optic transmission systems (FOTS) using WDM (Wavelength Division Multiplexing) and DWDM (Dense WDM) spectral technologies in multiservice telecommunication networks are analyzed. On the basis of the study, a new approach to the construction methods for calculating the indicators noise immunity for receiving streams optical signals operating under the influence unintentional sources of interference is proposed. Important analytical expressions are obtained that evaluate the noise immunity characteristics optical signal reception taking into account the transfer characteristics.
Key words: noise immunity, bit error probability, WDM unintentional interference, signal-to-noise ratio, DWDM, optical signal, FOTS.

Babkov I., Kazakov N., Karelsky P., Minyaev A. Determination of efficiency indicators of monitoring systems and correlation of information security events. – PP. 125–129.
Information security event management, from analyzing attacks and threats to selecting appropriate countermeasures, has become a major challenge for security professionals and IT administrators. To eliminate this problem in a timely manner and minimize the onset of information security risks, many companies create centers for monitoring and managing information security. One of the most important components of such centers are security information and event management (SIEM) systems, which allow aggregating events and identifying information security incidents from them. The article defines the performance indicators of SIEM systems.
Key words: security operations center, SIEM, information security incident.

Bakatov V., Martynuk A., Murashkin N., Pomogalova A. Creation of a Decentralized Messenger Using Blockchain Technologies. – PP. 129–132.
Blockchain technology is considered to be the most innovative and promising technology of our time. Nowadays, this technology is gaining momentum in a variety of areas. One of which is the sphere of business communication. The relevance of the technology application is justified by the need for a safe and convenient way of communication and concluding transactions in a corporate sector. This work is devoted to the development of a decentralized platform that performs the functions of a messenger with integrated smart contracts. As a result a decentralized solution was developed on the basis of the Ethereum blockchain platform.
Key words: Blockchain, Ethereum, smart contract, decentralized applications, matrix.

Batenkov K. Assessment of General Quality Indicators of Analog Terminals of Telecommunication Networks. – PP. 132–136.
The general indicators of the quality of analog terminals are considered: the band of efficiently transmitted frequencies, residual attenuation, asymmetry attenuation, symmetrical voltage and general asymmetric voltage. It is noted that for tonal frequency channels formed by digital transmission systems and mixed channels, it is necessary to ensure that the frequency of the measuring signal is not a subharmonic of the sampling frequency of 8 kHz in order to avoid additional error or beats.
Key words: communication network, telecommunication network, quality indicator, analog termination, tone frequency channel.

Beckel L., Maximenko M. Network Activity Analysis as a Security Tool. – PP. 137–142.
The article explores the problem of protecting a device from malicious software and network attacks by analyzing the behavior of the network and network structure, and provides an example of the work of programs such as nmap and Wireshark. The paper focuses on the fact that the use of licensed anti-virus software, although the most reliable way to protect the device, is often ignored by users due to its high cost. The issue of network traffic analysis is considered separately. The article provides comparison and comparison data of network attacks with the filters of the Wireshark program, which help to detect them.
Key words: traffic analysis, network attacks, malware, data transfer protocols.

Belaya T., Berezin A. Review of Neural Network Hardware Acceleration Platforms. – PP. 142–146.
This article will consider different hardware acceleration platforms for computing and training neural networks, such as GPUs, ASICs, FPGAs. Also, the nuances of the implementation of neural networks on hardware acceleration platforms. Hardware gas pedals are used to increase the speed of data processing. Modern neural networks are usually very large, which leads to increased processing time. Also, trends in network development show that the size of networks grows exponentially. Modern tasks require the fastest possible output. Even modern high-performance CPUs may not be able to handle large amounts of neural networks, usually due to data transfer delays between memory and the CPU itself.
Key words: HW Acceleration, AI, hardware, neural networks.

Biryukov M., Zentsov A., Remdenok P. Organization of an Automated Campus Delivery Network with the Help of Unmanned Aerial Vehicles. – PP. 147–150.
The article is devoted to the organization of an automated campus delivery network using unmanned aerial vehicles. The existing methods of campus delivery, their advantages and disadvantages are considered. Described: the order of delivery, a new way of landing a UAV, using computer vision, an approach to building a route.
Key words: unmanned aerial vehicles, automated delivery, campus delivery, runway, automated landing system, automated routing system, marking on the runway.

Biryukov M., Makukha A., Saenko I. Comparative Evaluation of Options for Organizing Information Interaction in a Distributed Control System. – PP. 150–154.
The paper deals with the issues of database synchronization in the absence of deterministic queries. The analysis of possible types of synchronous replication has been carried out. The conditions for choosing the most preferred option, taking into account the conditions for the functioning of a distributed control system, are substantiated.
Key worlds: informational space; information interaction; information storage; evaluation criteria.

Biryukov M., Mikhailichenko A., Nikolaev V., Saenko I. About the Problem of Information Resources Allocation in a Single Information Space. – PP. 154–159.
Possible options for building a single information space and the architecture of data storage systems used in their construction are considered. A comparative description of the options for access to information resources is given. The problem statement of the problem of optimal information resources allocation in a single information space based on the existing topologies of data storage systems are proposed.
Key words: information space, data storage systems, information resource.

Biryukov M., Yakubova O. Overview of Methods to Increase Web Page Loading Speed. – PP. 160–165.
Optimizing the loading of HTML pages ensures comfortable work with the site, increases network bandwidth. The used computing power is reduced, which means that energy consumption is reduced.

A long loading page increases the likelihood that the user will leave it without waiting for the content to appear, lowers it in the search results in search engines. It is believed that the optimal loading time is no more than 3 seconds.
Developers should know ways to optimize and lay them down at the design stage.
Key words: web development, optimization, loading speed.

Bobrova K., Zakharov I., Saharova M. Mathematical Model of a Multiservice Data Network Fragment for Evaluation of the Network Resources Utilization. – PP. 165–169.
In the context of development of the next generation multi service networks which provides access to services for different customers ensuring the required quality of service is quite a difficult task.
Next generation multi service data networks (MSDN) are rapid developing nowadays. Such networks are aimed to provide access to services for different types of customers. In the context of rapid development and claimed aims ensuring the required quality of service is quite a difficult task.
Private solutions of the task for different data types are relevant and in demand.
The authors suggest mathematical models that allow calculating and predicting operation efficiency for MSDN taking into account the imposed restrictions. The article presents developed mathematical model for network resources utilization performance evaluation taking into account the characteristics of the telecommunication channel used.
The result of the modeling is network probability-time characteristics that are necessary for successful message delivery in diverse network conditions.
Key words: multi service data network, mathematical model, performance, network resource, probability-time characteristics.

Bogomaz M., Mihailova L., Polyanicheva A. Security Tools VoIP. – PP. 170–172.
The relevance of the article is due to the advantages of using IP telephony as a tool for improving the data transmission network in an enterprise, and as a result, the growing need to protect information from unauthorized access and leaks in VoIP networks. This article will discuss some of the security tools that are designed to protect information in IP telephony technology. As a result of the work on the article, a comparison was made of promising and effective methods for protecting IP telephony networks, on the basis of which recommendations for ensuring security in the VoIP environment are presented.
Key words: telephony, IP telephony security, Voice over IP, VPN, IPsec.

Bogomolova M., Kazenkin A. The Concept of Business Process Reengineering for a Franchisee of a Domestic Software Vendor. – PP. 173–176.
Modern business management tools, among which business process reengineering stands out, allow you to rebuild company processes to speed up technical procedures, reduce costs, and introduce a corporate culture. In the context of the transition to domestic software, this tool is especially relevant for optimizing the activities of partner organizations operating under the single brand "1C: Franchising", which have received vendor confirmation of the provision of high-quality automation services using 1C software products.
Key words: business reengineering, business process reengineering, 1C: Franchisee, 1C, cloud software products.

Bogomolova M., Ushakov K. Development of a Virtual Reality Application "VR-projection" for Driving Education. – PP. 176–179.
In the process of developing the VR-projection software product, it is necessary to create an application for teaching driving using virtual reality: develop training routes based on real roads, as well as a student assessment system to reduce the burden on the teacher. The application will be developed using the Unreal Engine game engine.
Key words: VR application, driving training, virtual reality, VR headset.

Borovskaya Y., Grebeshkov A. Application of Semantic Technologies in Information Centric Networking ICN. – PP. 179–183.
The architectural and informational integration of fifth generation communication networks and information-centric networking ICN (5G-ICN) provides a number of advantages in delivering content to the user. An analysis of the architectural capabilities of 5G-ICN in terms of the possibility of data caching shows the need to use new semantic technologies to manage content caching. The basic task is to build a generalized information model, taking into account the considered parameters of the cached named object.
Key words: information-centric networking, content, caching, fifth generation networks, semantic technologies.

Branitskiy A., Manukyan A. Exploring the Evolution of Information Protection Mechanisms of the Windows 11 Operating System. – PP. 183–187.
The article shows the evolution of information security mechanisms using the Windows 11 operating system as an example. The authors analyze such characteristics as Zero Trust, hardware security, application security, user security and secure identification, operating system security and cloud services. It also provides a table of information security mechanisms of the Windows 11 operating system about innovations and updates.
Key words: privacy, security, system, Microsoft, operating system, development, app.

Bugrova E., Pestov I., Tarabanov I., Shvidky A. Analysis of Fault Tolerance Improving Methods of Cloud Infrastructure using Monitoring and Predicting the State of Components. – PP. 188–192.
The purpose of the paper is to study methods for improving the fault tolerance of cloud infrastructure. Particular attention is paid to the monitoring process, the consideration of the health status of cloud components. The paper reveals the problem of insufficient functionality of single monitoring tools. Based on the study, various monitoring methods are identified, as well as a search for options that provide prediction of possible failures for their prompt elimination.
Key words: monitoring system, cloud infrastructure, metrics, fault tolerance.

Bugrova E., Redrugin N., Tarabanov I., Shvidky A. Analysis of Machine Learning Methods for State Tracking of Distributed Storage Systems. – PP. 193–197.
This paper analyses machine learning methods applicable to distributed storage systems. Different machine learning methods were considered and the most appropriate one for the Ceph data storage system was selected. After selecting the training method, machine learning tools were selected. These were analysed to track anomalies in the performance of the storage system

Key words: opensearch, data storage systems, diagnostic information.

Burdin V., Gureev V., Sosunov D., Shaban O. Monitoring of the Condition of Microtubule Channels of Transport Multichannel Communication of Fiber-Optic Line. – PP. 197–201.
The paper suggests a method for monitoring the state of inspection chambers of transport multichannel communication using a distributed vibroacoustic monitoring system. The results of experimental measurements at the test site are presented. The measurements were made on a polymer inspection chamber, which contains a stock of two types of fiber-optic cable.
Key words: fiber-optic cable, inspection chamber, multichannel communication, condition monitoring, vibroacoustic monitoring system.

Bourdine A., Dmitriev E., Zaitseva E., Pashin S. Model of Piece-Wise Regular Fiber Optic Link Operating in a Few-Mode Regime Into Account the State of Connector Ferrule End-Face. – PP. 201–206.
This work is present model of piece-wise regular fiber optic link operating in a few-mode regime into account the state of connector ferrule end-face. We present comparison results of computed optical pulse response envelops, distorted during propagation over 10GBase-LX MM 50/125 cat. ISO/IEC OM2 network fiber optic links, containing, depending on various conditions of transceiver laser source connector ferrule end-face contamination.
Key words: few-mode regime, differential mode delay, multimode optical fibers, structural cable systems.

Bukharin V., Nikitin A., Dolgireva E. An Approach to the Formation of Filtering Rules in the Protection System of Information and Telecommunication Networks. – PP. 207–210.
The article considers an approach to the formation of filtering rules in the information and telecommunications network system, due to additional analysis of the "Black" list of IP addresses using time parameters, when implementing destructive program influences.
Key words: information and telecommunication network, destructive program impacts, filtering rules.

Bylin A., Bylina M., Nikolaenko O. Controlled Variable Attenuator of Reflective Type. – PP. 211–215.
The paper models a variable optical attenuator, the main element of which is a microelectromechanical system (MEMS), which is a matrix of micro mirrors, each of which can be in one of two positions. The radiation from the input optical fiber is collimated and falls on an array of micro mirrors. Mirrors, depending on their current position, reflect radiation so that it either falls (position 1) or does not fall (position 2) into the output optical fiber. If all mirrors are in position 1, the attenuator introduces minimal self-attenuation. By moving part of the mirrors to position 2, you can increase the attenuation. The dependence of the introduced attenuation on the number of mirrors moved to position 2 is calculated, the accuracy of the attenuation setting is estimated.
Key words: fiber-optic communication system, Variable Optical Attenuator, VOA, micro-electromechanical system, MEMS.

Bylin A., Bylina M., Pak V., Frolova A. Modeling and Investigation of the Polarization Splitter. – PP. 215–219.

A polarizing splitter or polarizing divider is an optical device that divides an incident light beam into two beams with mutually perpendicular states of linear polarization. The paper considers the polarization divider of S. McNeil's design. The main element of the divider is a multilayer thin-film structure consisting of alternating layers with high and low refractive indices. The structure is applied to the hypotenuse surface of a rectangular prism, which is then glued to another of the same prism, forming a cube. To analyze the operation of the divider, its modeling was carried out in the COMSOL Multiphysics program. The dependences of the reflection and transmission coefficients of the divider for each of the polarizations on the wavelength and the number of layers in the multilayer structure are obtained.

Key words: polarizing splitter, polarizing beam-splitting cube, MacNeille construction, Brewster angle, linear polarization, reflection coefficient

Bylina M., Fraz A. Virtual Laboratory Installation for Studying Single Photon Interference. – PP. 220–225.

The article presents a virtual laboratory setup that simulates the operation of a Mach-Zehnder interferometer and makes it possible to observe the propagation of single photons in it. On the basis of this setup, a laboratory work is proposed in which students consolidate knowledge about quantum objects, quantum state and quantum superposition, experimentally detect and investigate the phenomenon of interference of single photons. Guidelines for laboratory work have been prepared, containing a theoretical description of the phenomena being studied, tasks for performing experimental studies and control questions to check the degree of assimilation of educational material.

Key word: interference, quantum state, single photon, Mach-Zehnder interferometer, wave-particle duality, virtual laboratory work.

Bystrov I., Kotenko I. User Behaviour Model for Insider Threat Detection in Information Systems of Organizations. – PP. 225–229.

The application of machine learning for insider threat detection is an actively researched area. A key part of applying machine learning methods is user behaviour modeling. The paper considers the challenges of choosing and constructing features of the model. User behaviour model that uses a relatively small number of informative features is proposed.

Key words: user behavioral models, user behavior analytics, insider threat detection.

Vasilets P., Yesalov K., Panchenko A. Development of an Entity Recognition System in Business Documentation using Computer Vision. – PP. 230–234.

This paper proposes several ways to solve the problem of entity recognition in business documentation based on computer vision algorithms and several approaches in obtaining training data for neural network models. One of them is the generation of synthetic data, the other is an automatic system for converting Microsoft Word documents into images and then marking the entities present on them.

Key words: computer vision, Microsoft Word templates, synthetic data.

Vasilets P., Esalov K., Panchenko A. Comparative Analysis of Computer Vision Systems for Document Normalization. – PP. 234–239.
This paper compares two different approaches to solving the problem of distorted document images. The first one is based on the deep machine learning algorithm of the Transformer architecture, the second one is based on the calculation of the perspective transformation matrix by linear algebra methods.
Key words: neural networks, computer vision, geometric transformations.

Vasyutkin A., Vlasov D., Shvidkiy A. Analysis of Methods to Ensure the Interaction of Network Devices with Applications in the User Space of the Operating System. – PP. 239–243.
This article analyzes the different ways that network applications and network adapters working within OS based on Linux kernel. The article considers both the classical way of passing traffic between a network device and the server part of the application, using the OS network stack, and a different one, based on the organization of packets processing in user space.
Key words: kernel-bypass, Linux, SDN, DPDK.

Vasyutkin A., Vlasov D., Shvidkiy A. Analysis of Approaches to Increasing the Availability of Cloud Infrastructure Services. – PP. 244–248.
The article is devoted to the assessment of approaches to increasing the availability of cloud infrastructure. As an example of a cloud infrastructure, a cluster built on the basis of the open-source product OpenStack is given. Various methods are considered, such as increasing availability through OpenVPN, WireGuard, etc. The advantages and disadvantages of each are shown, as well as how they fit into the overall architecture of an OpenStack-based cluster. A comparison of these methods was made, it was revealed in which scenarios which approaches are most applicable.
Key words: VPN, cloud, OpenStack, OpenVPN, IPSec, WireGuard.

Verevkin S., Fedorchenko E. Analysis of Security data Sources for Modeling and Evaluating Cyber Attacks. – PP. 249–251.
The paper describes the result of the analysis of the most popular data sources containing information about threats and vulnerabilities, as well as additional data on the basis of which it is possible to develop indicators that allow identifying attacking actions in the cyber environment. The conclusions obtained from the analysis of various databases are presented, indicating the advantages and disadvantages of each type of information sources. The direction of further application of the results has been formed and, in accordance with this, the most relevant source of information from the point of view of the data provided has been determined.
Key words: vulnerabilities, attack detection, databases, security testing, risks.

Vershinina X., Saltykov A. Azure Quantum and Quantum Development Kit (QDK) capabilities analysis. – PP. 251–254.
Quantum computing is an extensive interdisciplinary research founded at the intersection of programming, physics, mathematics, mechanical engineering and computer science.
Azure Quantum is a cloud service with a various quantum solutions and technologies kit. Azure is an open ecosystem that provides access to various Microsoft and its partners software, hardware and solutions for quantum computing.

The article purpose is a using Azure Quantum and the Quantum Development Kit (QDK) preliminary possibilities analysis to create quantum algorithms and optimization targets.
Key words: Quantum Development Kit, QDK, Azure Quantum, QKD, Q#.

Vesnin D., Chechulin A. Detection of Similar Trademarks by Analysis of the used Color Palette. – PP. 255–259.
This article discusses the solution of the actual problem of searching for similar trademarks. A technique for detecting similar trademarks by analyzing the used color palette is proposed, which can quickly work on large amounts of data. Its analysis was carried out, the advantages and disadvantages of this method were identified, and the possibility of combining this method with other solutions was analyzed.
Key words: search for similar logos, *rgb* histograms, k-*nn* search.

Vitkova L. An Approach to Detecting Anomalies and Attacks in Container Systems Based on Logs. – PP. 259–263.
Everything that happens in the operating system as a whole can be represented as a sequence of events. The Extended Berkeley Packet Filter (eBPF) is a subsystem of the Linux kernel that allows you to write small programs that will be run by the kernel in response to an event. The article discusses an anomaly and attack detection approach that allows you to create white and black lists of system calls, create container behavior profiles based on data obtained using the eBPF probe. The proposed approach expands the horizon of information security event control in Linux OS.
Key words: Extended Berkeley Packet Filter, eBPF, anomaly detection, intrusion detection, container systems.

Vitkova L. Algorithm for Analysis of Registration Dates of Commentators in the Social Network VK. – PP. 263–266.
Today, the situation in social networks and with social networks is far from unambiguous. The level of information noise is constantly growing. It is almost impossible to distinguish the true source from the bot without special algorithms. The complexity of detecting bots and the fakes they spread is manifested when it is necessary to collect a huge amount of information and conduct content analysis. The article proposes an algorithm for analyzing the registration dates of commentators on the Vkontakte social network, which allows you to quickly get an idea of the commentator's page.
Key words: social network analysis, bot detection, fakes, unwanted information, information security.

Vitkova L., Edemskaya E. Researching Vulnerabilities of Smart Home System and Methods of their Detection. – PP. 267–270.
A smart home is an automated comfort management system. There are a number of vulnerabilities in such systems that need to be detected in a timely manner. At the same time, new vulnerabilities may appear. The article discusses the categories of smart home devices and their corresponding vulnerabilities. It also describes the existing methods for detecting vulnerabilities in IoT.
Key words: smart home, Internet of Things, smart home vulnerabilities, smart home security.

Vitkova L., Zrelova A. Analysis of IPTV to Detect Pirated TV-Channel Content. – PP. 270–274.
Today, the high level of influence of digital technologies on the life of every person is an indisputable fact. This also applies to television. The development of broadband Internet access and high data rates make it easier to access IPTV. The popularity of digital TV leads to the growth of illegal sources and broadcasts. At the same time, there are practically no methods for detecting pirated content of TV channels. The paper analyzes IPTV and proposes a method for detecting pirated content of TV channels.
Key words: IPTV, IPTV architecture, method for detecting pirated content, intellectual property, illegal broadcasting.

Vitkova L., Krestiashin N. Classification of SQL-Injection Threat Sources. – PP. 274–278.
Today, SQL injections are still an actual threat to application security and are among the top three threats to the information security of web applications. SQL injections allow attackers to gain unauthorized access to an application's database. The main reason for the threat of SQL injection is the lack of proper filtering of data received from the user input form. The article proposes a classification of SQL injection.
Key words: SQL Injection, vulnerability, web application, database, information security.

Vitkova L., Parashchuk I., Saenko I. Problems and Features of Analytical Processing Procedures for Large Arrays of Heterogeneous Data on Cybersecurity Events in Infocommunication Networks and Systems. – PP. 279–283.
The problems and key features of the process of intelligent analytical processing of large arrays of heterogeneous data on cybersecurity events of complex systems are considered. It is shown that this process is aimed at identifying links between cybersecurity events, for example, in infocommunication networks and systems, as well as at establishing various quantitative characteristics of the impact of such events or factors on a particular cybersecurity indicator in the interests of assessing the state, decision support and investigation of computer incidents in networks and systems of this class. Based on the results of the analysis of problems and features, it is possible to formulate fundamental principles and recommendations that determine the scientific and, most importantly, specific practical aspects of the implementation of analytical data processing, which, ultimately, will increase the reliability of security control of modern information communication networks and systems.
Key words: analytical data processing, heterogeneous data, cybersecurity events, problem, feature, infocommunication networks and systems, computer incident.

Vladimirov S., Gutovskiy A., Fomin A. Testing of NCDP Network Coding Protocol Timing Characteristic – PP. 283–288.
The paper presents the results of testing the timing characteristics of a multicast datagram protocol NCDP with network coding. A block diagram of a virtual laboratory testbed for testing the protocol in unloaded and loaded networks has been developed. The comparison of the NCDP protocol with multicast transmission without network coding is carried out and conclusions are made about the applicability of the NCDP protocol in modern data networks.
Key words: network coding, multicast transmission, TCP/IP networks, RTT.

Volkov A., Kovalenko V., Muthanna A. S. A. Application of Fog Computing Technologies for Traffic Processing in Networks with UAV Clusters and MEC Multi-Layer Cloud Architecture. – PP. 288–293.

In this paper, we propose to organize a network architecture using UAV clusters at the lower level and a three-tier MEC cloud system at the upper ones. Also in this paper, it is proposed to use fog computing technology at the level of UAV clusters to process traffic from user devices. Within the framework of this work, criteria are also determined for choosing the level of processing and calculating the total resources of each UAV for the subsequent formation of a Fog cluster, which will be formed to process traffic. The article describes the algorithm for the formation of Fog clusters, and also defines the devices that will be responsible for both the formation of the Fog cluster and the choice of processing level.

Key words: UAV, cluster, head node, MEC, Micro-cloud, Mini-cloud, Main cloud, Fog.

Volkogonov V., Gaponenko V., Katasonov A. Comparative Analysis of Software-defined Storage Systems for Special Purpose. – PP. 294–298.

In every IT company that cares about the safety of its data, there is a need to use data storage systems. In this study, a comparative analysis of software data storage systems and an analysis of the supply market was carried out. The proposals of the most common company in the field of application of software data storage systems are considered. The main criterion for comparing this analysis is the number of possible functions needed to solve business problems.

Key words: data storage system, SDS, Administration, IT.

Volostnykh V., Kononov P., Ostroumov O. Ensuring the Security of the Critical Information Infrastructure of an Educational Organization. – PP. 299–304.

The article deals with the problems of ensuring the security of critical information infrastructure of educational organizations, measures to ensure the security of information and telecommunication systems classified as significant objects and ways of their implementation. The authors propose approaches to categorizing information infrastructure objects and identify problems related to ensuring the security of information systems of educational organizations. The article may be useful to specialists of information security departments and students of communication universities..

Key words: security of critical information infrastructure, state system for detecting, preventing and eliminating the consequences of computer attacks, protection of information systems, a significant object of critical information infrastructure, categorization of automated and information systems, computer attacks, electronic document management, information security tools, critical information infrastructure.

Vorontsov A., Shemyakin S. Basics for Using NIST Tests. – PP. 305–310.

The basics of using the NIST tests used to evaluate the measure of randomness of numerical binary sequences are considered. By design, these NIST tests provide a fairly complete estimate of proximity to purely random binary sequences. The main aspects of the use of these tests, as well as a list of other similar tests, are presented.

Key words: random sequences, testing, pseudo-random number generators, statistical hypothesis testing, autocorrelation function.

Voroshnin G., Kovtsur M., Yurkin D. Analysis and Classification of Software Tools for Penetration Testing of IEEE 802.11 Wireless Networks. – PP. 310–314.
Wireless networks of the IEEE 802.11 family have become an integral part of the daily life of almost every person. They are used both in the smallest home networks, consisting of a single access point, and in large corporate networks, where there are hundreds of access points. Wi-fi technology surrounds modern man everywhere: at home, at work, at school, in cafes and shops. At the same time, a very small part of wireless network users thinks about how safe their connection to the Internet is, and, as a result, all the data that they transmit over the network. The number of information security incidents is increasing every year. One of the most common objects of attack is network equipment, which, in particular, provides connection of clients over networks of the IEEE 802.11 family. Along with the process of continuous improvement in the quality and security standards of wireless networks, the methods of attacking wireless networks are also improving. Currently, even new equipment equipped with the most modern information security tools is subject to many elementary attacks that significantly degrade the quality of service. In this regard, the study of wireless network testing tools is relevant both to check the stability of the network and to create methods for detecting or countering intruders.
Key words: information security, wireless network security, penetration testing.

Vyugov S., Kozlov S. Analyzing the Characteristics and Capabilities of a Virtual Network Based on Network Namespaces in the GNU/Linux Operating System. – PP. 315–319.
One of the key elements of the GNU/Linux operating system is process isolation. The internal namespace mechanism implemented in this operating system allows processes to be isolated at the kernel level. The Network process tree, has its own set of routing tables. It is possible to tunnel traffic of individual applications and to create virtual network models with defined quality characteristics of the communication channel.
Key words: namespace, physical stack, virtual stack, communication channel characteristics.

Gaifulina D., Kotenko I. Security Event Processing Models in Intelligent Systems for Monitoring and Assessing the Security of Critical Infrastructures. – PP. 319–324.
In general, critical infrastructures include a set of automated process control systems for critical facilities operating in the areas of healthcare, science, transport, communications, energy, finance, defense and industry. As a rule, such infrastructures require continuous monitoring and analysis of security events in order to predict the probability of a possible failure, decrease in the level of reliability, as well as attacks. We research and develop models for processing security events in intelligent systems for monitoring and assessing the security of critical infrastructures. We propose to use the following types of knowledge representation models about security events as event models: rules, logical representation, semantic networks and frames. Security event processing models are defined in accordance with the presented event models, as well as in accordance with the task being solved: classification, prediction, or restoring event dependencies.
Key words: security events, security event processing, security management.

Gaifulina D., Kotenko I., Fedorchenko E. Sentiment Analysis of Social Network Posts for Destructive Impacts Detection. – PP. 324–328.
The information provided by users in the social networks communities can have a destructive impact on other users, especially representatives of the "youth" socio-demographic group. One of the features used to detect destructive impacts in a social network can be the sentiment of

posts. The authors analyzed the existing sentiment-tagged sets of Russian-language posts, selected a training dataset, and tested a number of classifiers. As a result, the FastText classifier was chosen, which was used to classify the posts of the selected communities into positive, negative, neutral, speech and skip. The results have been verified by the experts. Based on the sentiment of posts, an additional integral sentiment-based metric is proposed to detect the potentially destructive communities in social networks.
Key words: destructive impact, social network, sentiment, classification, FastText, sentiment-based metric.

Gamanova M., Klyuev D., Frolov A. Ways to Protect Information and Prevent Unauthorized Removal of Information by Using Special Equipment. – PP. 329–333.
It is necessary to ensure the prevention of leakage and interception of confidential information, as well as the protection of restricted access information. Spectrum analyzers have the best characteristics for searching and detecting embedded devices, including they are used to protect information in a multi-channel transmission system. The spectrum analyzers under consideration use the method of harmonic analysis of the function y(t), based on the use of discrete analyzers of the frequency spectrum of the signal.
Key words: spectrum analyzer, information protection.

Gerling E., Zebzeev E., Kistruga A. Development of a Method for Analyzing Wireless Network Traffic Based on WPA2 Enterprise. – PP. 334–339.
Wireless data transmission technologies, in particular Wi-Fi, are widespread today. One of the main problems is ensuring secure transmission, especially in corporate networks, because confidential company information is under threat. The required level of protection is provided by the WPA2 Enterprise standard. Another important aspect of information security is traffic analysis, which allows you to identify abnormal activity and the presence of intruders. This article discusses a method of analyzing wireless network traffic based on WPA2 Enterprise. The use of this security standard involves the transmission of traffic in encrypted form, and that is why a detailed decryption process is presented.
Key words: WPA2 Enterprise, IEEE 802.1X, RADIUS, information security, traffic decryption, traffic analysis, network administration.

Gerling E., Kovalev I., Fyodorova A. Research of Performance of Web Server for Low-Power Devices Based on Raspberry OS. – PP. 339–343.
The pandemic has made its own adjustments to the current economic situation in the country and the world, as a result of which the popularity of microcontrollers has increased, the demand for which is growing every day. There is a growing demand for smart home solutions, security systems and various hardware devices. New systems are especially popular in the context of the import substitution trend. Quite often there is a need to implement a user interface, and, accordingly, to install specialized software to solve the tasks. This article reviews known methods for deploying and maintaining web servers based on low power devices, provides examples of existing best practices in the field, and analyzes the potential for choosing the optimal web server for deploying infrastructure based on low power devices such as Raspberry.
Key words: web interface, wireless networks, network security.

Glagolev S., Dotsenko S. Maintaining a Quasi-Soliton Regime in Fiber-Optic Communication Systems using Raman Amplifiers. – PP. 343–348.
The paper considers a method for maintaining a quasi-soliton regime in multispan fiber-optic communication systems using single-mode optical fibers with losses and Raman amplifiers with counter- and bidirectional pumping. Theoretical calculations and modeling in the OptiSystem program of the processes of propagation of quasi-soliton pulses in separate amplifying sections (spans) and in the communication system as a whole are carried out. The results of theoretical calculations are compared with the results of modeling, and the advantages of bidirectional pumping are shown.
Keywords: soliton, quasi-soliton regime, optical Raman amplifier, single-mode optical fiber, chromatic dispersion, self-phase modulation.

Glagolev S., Dotsenko S., Sokolov G., Yudina E. Investigation of the Effect of Chromatic Dispersion in Single-Mode Optical Fibers on Pulses of Different Shapes. – PP. 349–353.
This work is devoted to testing and refining known engineering formulas for calculating the duration and peak power of non-chirped optical pulses with a Gaussian shape and hyperbolic secant, which have traveled a considerable distance along a single-mode optical fiber with known chromatic dispersion and attenuation coefficients. The work is limited to consideration of processes only in fiber-optic communication systems with binary amplitude modulation and return-to-zero coding. Nonlinear phenomena and polarization-mode dispersion in an optical fiber are not taken into account in this work.
Key words: single-mode optical fiber, chromatic dispersion coefficient, Gaussian pulse, hyperbolic secant pulse.

Goikhman V., Olenichev V. Identification of Key Technologies Enabling the Evolution of Mobile Communication from 5G Networks to 6G Networks. – PP. 354–358.
This paper identified six major trends in technology development. An analysis of each direction was carried out. The views of various large companies and associations on the development of key technologies in 6G networks are presented. The main use cases of 6G are presented, including various aspects of their impact on everyday life and work in the future. Development scenarios in these areas are given from the point of view of various large companies and associations, on the basis of which conclusions are drawn regarding the key vectors of technology development in new generation networks.
Key words: 5G, 6G, ML, AI, VR, XR, cellular network, infocommunications, smart city.

Golubkin A., Pirmagomedov R. Implementation of the Augmented Reality System in the "INDUSTRY 4.0" Context. – PP. 358–363.
Augmented reality is used not only as an entertainment option, but also as an auxiliary tool in the field of marketing, medicine, and construction. The report proposed a variant of the project implementation in the context of the industrial Internet of things (IIOT). The architecture, the tasks, as well as the way of their implementation with the indication of specific technologies are considered.
Key words: augmented reality, mixed reality, industry 4.0.

Golyshko A. Infocommunications as a Basis of Digital Civilization. – PP. 364–369.
The role of the modern communications industry in the development of modern society is decisive: the transformation of networks and communication systems (hyper-converged software-defined world); new network technologies and their theoretical foundations (6G, etc.); new challenges and implementation of the import substitution strategy on the example of Research Production Association RusBITech JSC; digital civilization and its humanitarian development scenarios.
Key words: infocommunications, hybrid cloud infrastructure, metauniverse.

Grebenshchikova A., Elagin V. The Auto Regressive Integrated Moving Average Model with Autoregressive Conditional Heteroscedasticity for Prediction the Network Traffic. – PP. 370–372.
The most popular model for predicting network traffic is the autoregression and Integrated Moving average models (ARIMA). The ARIMA model is an important class of parametric models that allows describing nonstationary series. Modern research shows that using the conventional ARIMA model gives a higher error rate compared to the combined ARIMA model with other techniques.
Key words: forecasting the network traffic, iterative application, ARIMA models, GARCH models, self-similarity, multifractal.

Gubarev V. Authentication Methods in Information Systems. – PP. 373–378.
The article considers methods of user authentication in information sistems.
The purpose of the article is to discover modern methods of authentication in information sources and the definition of their positive and negative sides. The relevance of research is explained by the widespread use in the world information systems that need protection from unauthorized access.
Key words: authentication, password, biometric characteristic.

Humbatov R., Ibrahimov B., Ibrahimov R., Namazov M., Mirzoev O. Research of Network Resources and Performance Indicators of Multiservice Telecommunication Networks. – PP. 378–383.
The advantages using the architectural concept future networks FN (Future Networks) are analyzed to build highly efficient multiservice telecommunication networks (MTN) that support a wide range multimedia services. A mathematical model MTN performance based on the architectural concept future FN networks using virtual, channel, information and network resources is proposed. The network performance model differs from the known ones in that to ensure acceptable QoS (Quality of Service) and quality of perception QoE (Quality of Experience) in the general existing NGN (Next Generation Network) architecture multiservice public networks, a new innovative technology was used and four targets of Future FNs.
Key words: limited resources, Future networks, SDN, reliability, performance, IMS, quality of service, security risk, NFV, efficiency.

Dvoretskov K., Martynuk A., Mironov K., Ogoreltsev P., Pomogalova A. Research and Testing of Smart Contracts in the IOTA Blockchain Network. – PP. 384–388.
This paper is devoted to testing the implementation of smart contracts in a decentralized IOTA blockchain network. The relevance of this problem is justified by the growing popularity of the

Internet of Things and the need for increasing functionality of the network because of it. In this paper the process of developing and testing of an application based on the IOTA blockchain platform, the main goal of which is to demonstrate the operation of smart contracts for smart devices, as well as testing the performance and stability of these smart contracts.
Key words: IOTA, EVM, smart contract, decentralized app, DApp.

Dvoretskov K., Martynuk A., Pomogalova A. Development of an Aggregator Platform for Loyalty Systems Using Blockchain Technology. – PP. 388–392.
Blockchain technology is considered to be the most innovative and promising technology of our time. Nowadays, this technology is gaining momentum in a variety of areas. The relevance of the technology application is justified by the immutability of the information entered, ensuring the level of security of users' assets in the system. This work is devoted to the development of a platform for the aggregation of loyalty systems for the retail segment and the creation of a tool for storing and using digital loyalty cards, and the development of new functionality for working with this tool. This work also highlights the problems of current loyalty systems, how these problems can be solved with the help of blockchain technologies.
Key words: Blockchain, decentralized applications, loyalty system.

Javadova M., Ibrahimov B., Mammadov T., Orujova M. Analytical Model of the Protection Mechanism Critical Telecommunication Infrastructures. – PP. 393–398.
The models and mechanisms protection critical telecommunication infrastructures are analyzed, taking into account the information and technical impact on communication systems and the information protection characteristics of the telecommunications system and the management an important object in critical infrastructures. Based on the analysis and refinement of the requirement for the effectiveness technical means of the information security system, a new approach to the construction an analytical model and a mechanism for protecting critical telecommunication infrastructures is proposed. This paper explores a new approach to assess the characteristics telecommunication systems operating in critical infrastructures and managing an important facility under the influence unintentional various sources of security threats.
Key words: critical infrastructure, information security, communication and control system, information security and protection system, telecommunication system.

Dmitrieva D., Krasov V., Pilipova V. Investigation of the GandCrab Ransomware. – PP. 398–403.
Ransomware Trojans are ransomware - malware that makes unauthorized changes to user data or blocks the normal operation of a computer. To decrypt data and unlock a computer, cybercriminals usually require a money transfer (ransom). The main purpose of this research article is a step-by-step acquaintance with the development of one of such ransomware programs - GandCrab, which occupied 40% of the market during peak activity, the nuances of work, as well as an illustrative analysis of this ransomware depending on the level of training.
Key words: data encryption, virus history, software product versions, user information.

Dmitrieva D., Krasov A., Pilipova V. Holography as a Modern Way to Security Information. – PP. 403–407.
In the article the signs of the authenticity of various assets and their authentication were discussed. Counterfeiting of documents and securities has existed since ancient times and is constantly being improved. That is why it is very important to establish the authenticity of all kinds of assets. In the course of the work, it was determined that the most resistant to counterfeiting is holographic protection.
Key words: authenticity of the document, sign of authenticity, holographic protection, hologram.

Dmitrieva J., Elagin V. Research Aspects in the SDN Network. – PP. 407–413.
The article analyzes approaches to managing network resources in the Software-defined network (SDN). In the interests of this, a review of scientific works by Russian and foreign authors has been carried out to identify the solutions used in them, as well as their advantages and disadvantages. The methods considered in scientific articles are systematized according to the following criteria: the level of applicability of the method (physical, logical, network), mathematical modeling, response time, the range of tasks to be solved, bringing the solution to practical implementation. As a result of the review analysis, it was concluded that the solutions were unsatisfactory, as well as the need to create a new method with the following characteristics: a wide scope of application that works at all levels of SDN.
Key words: SDN, Software-Defined Network, OpenFlow, balancing, comparative analysis.

Dokshin A., Dokshina A., Kovtsur. M., Kostandyan. E. Development of a User Profiling System for VPN Connections. – PP. 413–418.
Today, most companies are implementing technologies thanks to which employees do not need to be at their workplace to perform their duties. One of these technologies is a VPN in a corporate network. Attackers also do not need to be inside the company to hack its network. It is enough for them to get the data of any employee for successful authorization in the corporate network. The solution to this problem is based on the company's use of a profiling system for each user when connecting to the corporate network. Profiling involves determining the user's device, for example, based on the MAC address, operating system version, browser and user location at the time of connection to the VPN server. The report describes in detail the mechanism for applying the profiling process based on the pfSense security gateway.
Key words: VPN, remote access, wireless network security, profiling, security gateway, pfSense.

Dolgov E., Osetrin A. Method for Configuring Equipment in a Software-Defined Network Segment. – PP. 418–423.
The task of training administrators of software-defined networks is a topical area of research. The paper considers the features of the architecture and hardware configuration of software-defined networks. In the course of configuring the experimental stand, a technique for setting it up was developed. The results obtained describe the components necessary to create a network of any complexity.
Key words: software defined networks, mininet, ryu, Open vSwitch.

Donskov E., Kotenko I. Security Analysis of SD-IoV-Blockchain Objects. – PP. 423–428.
The concept of SD-IoV (SDN Internet of Vehicles) is one of the advanced areas that is actively developing and allows you to take a fresh look at the possibility of using the Internet of Things in general. However, the most pressing problem is the low security of IoT systems. To solve this problem, researchers propose the integration of SD-IoV technologies and a distributed registry. The purpose of this work is to analyze the security of SD-IoV-Blockchain objects in terms of the level of security of the system as a whole, as well as the security of the part of the network that uses the blockchain. The paper considers vulnerabilities both from a network point of view and from a software point of view, since the smart contracts used to increase the functionality of the network are a key element.
Key words: internet of vehicles, SD-IoV, blockchain.

Drepa V., Kuzmina O., Minyaev A. Developing a Model for a Wireless Client Location System for the IEEE 802.11 Family of Networks. – PP. 428–433.
The location service plays an important role in modern wireless access networks. The relevance of the developed model is justified by network security issues, as it makes it possible to determine the location of an attacker in case of an attack on a wireless network. In addition, the service can simplify the search for the target audience for which targeted advertising needs to be configured, which confirms the importance of the developed model in the media sphere. The article describes the model of the location system for wireless clients of the IEEE 802.11 family of networks. The article describes the components of this model and the principle of their interaction. The article also demonstrates a possible scheme for the implementation of the developed model.
Key words: wireless networks, location detection, RSS, fingerprinting.

Dunaytsev R., Svetova A. An Overview of the Wi-Fi 6 Devices Market. – PP. 434–437.
This paper provides an overview of the market for Wi-Fi 6-enabled client devices. It analyzes the adoption rate of the new generation of Wi-Fi 6 (IEEE 802.11ax) compared to the previous generation of Wi-Fi 5 (IEEE 802.11ac). The growth rate and development of the Wi-Fi device market in Russia are also determined. In addition, the leaders of the domestic market are determined in terms of the range and cost of client devices with Wi-Fi 6 support.
Key words: IEEE 802.11ax, Wi-Fi 6, Wi-Fi router.

Elagin V., Obukhov S. Comparative Analysis of Wired Local Area Networks by Type of Transmission Medium. – PP. 437–442.
The study is devoted to comparing the types of wired transmission media used in local area networks (LAN). The classification of LAN according to the type of data transmission channel is formulated. The research methodology was chosen according to a number of criteria. A comparative analysis of data transmission media in the LAN has been performed. A summary table has been created in order to summarize the analysis data. The conclusion is made about the advantage of a fiber-optic LAN over a LAN based on a copper twisted pair.
Key words: local area networks, twisted pair, optical fiber, hybrid networks, transmission medium.

Elagin V., Yuryev G. Technical Features and Applications of Mixed Reality, Differences from Virtual Reality and Augment Reality. – PP. 442–447.
Mixed Reality (MR) can be used to augment reality in various ways, such as overlaying annotations and data for training or analysis, or providing virtual 3D content shared by multiple users in the same physical space. Mixed reality has been used globally for several years, but its use is still quite limited. This article provides an overview of mixed reality technology, its applications and development potential. It gives an overview of this technology and what it can give people, describes why this technology is of interest to society, and presents some current issues and problems of Mixed Reality as a technology.
Key words: mixed reality, hologram, virtual content, information interaction, technological capabilities.

Elfimov A., Kushnir D. Comparative Analysis of Technologies for the Formation of Distributed Ledgers. – PP. 447–451.
The article is devoted to the mechanisms underlying the formation of distributed registries and, in particular, blockchain and hashgraph. The focus is on a comparative analysis of the various principles for reaching consensus in a distributed ledger and how they can affect the ability to store and secure data. The article also discusses the influence of the technology of building a distributed registry on the scope of its application.
Key words: blockchain, directed asynchronous graph, hashing, hashgraph.

Ermolenko D., Kilicheva K., Muthanna A. S. A. Industry 4.0 for E-Health. – PP. 451–455.
The eHealth 4.0 approach is derived from the well-known Industry 4.0 or the so-called Fourth Industrial Revolution. Its main goal is to make a leap in the manufacturing sector through digitization. Future healthcare management will become more timely and personalized, as new technologies will allow individuals to monitor their health using cyber physical systems. The design principles of Industry 4.0 connect the physical and virtual world in real time. To do this, the next-generation 5G mobile network will provide an intelligent environment for the organization of medical services, so that public and private companies can reconsider their prospects and methods. Technological developments in the field of big data and industry 4.0 separately attract huge attention of scientists and industries. However, a detailed study of big data related to healthcare is still lacking in the available literature. The article presents a new approach to achieving effective indicators related to the identified research problems.
Key words: eHeath, Industry 4.0, 5G, IoT, Blockchain, Cloud Computing.

Zhernova K. Methods for Assessing the Security of Human-Computer Interfaces for Information Security Applications. – PP. 456–459.
For information security, applications are developed using modern types of interfaces, such as touch screens and virtual reality. However, new types of interfaces are also not without vulnerabilities that can be used to attack sensitive data of application users. In addition, these vulnerabilities are poorly understood, so an assessment of their criticality is required. Interface vulnerabilities differ from computer network vulnerabilities, for this reason it is necessary to introduce new parameters for vulnerabilities and modify existing ones. This report proposes methods for assessing the security of interfaces for information security applications based on touch screens and virtual reality.
Key words: human-machine interaction, information security, security assessment, user interfaces, data visualization, touch screens, virtual reality.

Zhernova K., Izrailov K., Kolomeec M., Levshun D., Chechulin A. Conceptual Model of the "System-Operator" Interaction Interface Based on Visualization Technologies That Take into Account the Human Cognitive Apparatus. – PP. 460–463.
In order to determine the possible ways of interaction between the unmanned vehicle system and the operator, it is required to develop a conceptual model of this interaction. The report presents a conceptual model of the "system-operator" interaction interface based on visualization technologies. This conceptual model takes into account the vulnerabilities of the human cognitive apparatus, which can prevent the operator from correctly perceiving the information provided by the system. The conceptual model shows the ways of transmitting visual information from the system to the operator, as well as the dependence of the quality of information perception by the operator on the method of data visualization.
Key words: human-machine interaction, information security, user interfaces, data visualization, machine vision.

Zhernova K., Kolomeec M. Vulnerabilities of Visual Interfaces "System – Operator" in an Unmanned Transport Environment. – PP. 463–466.
Despite the fact that the transport environment of a smart city is unmanned, and therefore partly autonomous, the final decisions regarding information and computer security are made by a person. The operator must respond in time to emerging security events and threats. However, the operator's perception itself has a number of vulnerabilities from which the operator needs to be protected. This report provides a brief description of the system-operator interface of an unmanned transport environment, describes the schemes for interaction between the system and the operator from the system side, and also describes the main vulnerabilities of the interface and attacks in which these vulnerabilities can be involved.
Key words: human-machine interaction, information security, user interfaces, data visualization, machine vision.

Zhernova K., Chechulin A. Methods for Assessing the Quality of Human-Computer Interfaces for Information Security Applications Based on Touch Screens. – PP. 466–469.
In order for the operator to respond to network security events in a timely manner and make adequate decisions, an effective computer network model combined with touch screen technologies is needed. To evaluate the effectiveness of such a model, you need to measure its quality. The main parameters of the model, by which one can judge how successful the development of the model is, are quality, efficiency and effectiveness. This work is devoted to assessing the effectiveness of the operator's work with a computer network model using touch screen interfaces. The report briefly discusses the methods for assessing the quality and effectiveness of the model, suitable for evaluating the developed model of a computer network.
Key words: human-machine interaction, information security, user interfaces, touch screens, quality assessment.

Zarubin A., Redrugina N., Shvidkiy A. Egoistical Distributive Algorithms as Load Management Algorithms in SDS. – PP. 469–473.
This article presents an approach to modeling and calculating the load in a software defined storage. The method used shows how it is possible to improve the operation of a real system by using a egotistical distributive algorithm for controlling the flow of requirements. This helps to solve the problem of calculating models that are complex in execution and time-consuming in analytical calculation.

Key words: software defined storage, egoistical distribution algorithms, analytical modeling, queuing system.

Zarubin A., Saveleva A., Shvidkiy A. Analysis Open Data Storage Systems Characteristics. – PP. 473–478.
The paper presents the most popular open-source data storage systems and develops criteria for their comparative evaluation. These systems currently represent the functionality and performance at the level of commercial systems, as well as a thoughtful approach to building such systems on the basis of publicly available hardware. This approach has already proven its reliability and efficiency, and has led to the emergence of an entire class of storage systems – software-defined storage systems.
Key words: data storage system, software-defined storage system, distributed storage system.

Zebzeev E., Kovzur M., Petrova T. Development of the Ansible Module for Detecting Rogue Wireless Access Points in the Corporate Network. – PP. 478–483.
The shortage of qualified security specialists and the availability of automation tools in security tools have led to an increase in the use of automated processes that "independently" solve tasks based on predefined rules and templates, therefore automation is currently one of the most important trends for the security system. By automating network tasks and functions, and with the help of repetitive processes with automatic control and management, the availability of network services is increased. The report describes the Ansible module for detecting illegitimate wireless access points in a corporate network. The structure of the rogue device detection module is considered.
Key words: automation, Ansible, security, rogue access point.

Zelichenok I., Kotenko I. Development of the Bench Architecture for Testing the Effectiveness of the Multi-Step Attack Detection Module. – PP. 483–492.
The paper describes the process of designing the architecture of the stand to test the effectiveness of the proposed anomaly detection module, and analyzes the solutions used today. The main feature of this stand is the simulation of heterogeneous traffic on different nodes of the system, which will presumably be collected by different components of the anomaly detection module using machine learning methods and big data processing technologies to identify multi-step attacks and create a hyper-warning containing a detailed description of the attack.
Key words: information security, cyber-attacks, multi-step attacks, attack detection.

Zimin A., Revenko Y. Paradigm Shift or use of Network Devices in the Transition to Heterogeneous 5G Networks. – PP. 488–492.
The importance of testing network equipment with the transition to 5th generation networks is only growing. If TDM and even NGN networks had fairly well-established rules for networking and equipment, then the transition to heterogeneous networks, the trend towards self-organization and virtualization, as well as the avalanche growth of services and technologies, increases the requirements for checking equipment for readiness to become a full-fledged and reliable participant in the fifth generation network. With such introductory ones, it is necessary to base and consider new models and algorithms or combinations of existing models, it is necessary to take into account the total image of the network as much as possible, in a sense,

to move from testing each one specific "black box", towards testing in a complex information field.
Key words: 5G, NGN, post-NGN, Network Under Test, heterogeneous networks.

Zimin A., Revenko Y. Decomposition in NGN Network Element NGN/post-NGN. – PP. 493–498.
The approach proposed in the article to conducting tests, including certification tests, of network equipment is based on the principle of divide et impera (divide and conquer, Latin). In the context of this article, we are talking about the paradigm of recursive decomposition of the network architecture into levels, and then into systems of the same level, and then into subsystems of a smaller size, and the decomposition is performed until all subsystems are separate software and hardware or only software network elements that fall under the scope of certain standards, recommendations or regulatory legal acts of the Russian certification system in the field of "Communications".
For unified interfaces and standard protocols of interaction of these network elements, the second component of the proposed approach is just necessary, it is a formalized abstract description of the functions, interfaces and protocols of elementary network elements. This principle is supplemented by combining the decomposition results into some combined finite state automata of behavior (GFSM) for each network element, which allows testing each such network element separately.
Key words: MSC, *GFSM*, NGN/IMS, decomposition.

Ibrahimov B., Tahirova K. Analysis Methods of Network Steganography Using SCTP Protocol. – PP. 499–503.
In this paper, important for practical use issues of hiding mixed-type information in text documents, issues of network steganography, methods and algorithms for hiding data are considered. In part, the article explores the method of steganographic information protection, which makes it possible to increase the resistance to information attacks in telecommunication systems. The methods of network steganography for hiding data using the mechanisms of the SCTP protocol (Transport Protocol with Packet Control) transmitted over communication channels are analyzed.
Key words: Network steganography, covert channel, SCTP, throughput, payload and service package, cost of steganography, data hiding.

Ignatova I., Kirichek R. Analysis of the Application of Time Sensitive Network Technologies in Fifth Generation Communication Networks. – PP. 503–508.
Time Sensitive Network (TSN) technology is becoming the standard for Industry 4.0 converged networks due to its ability to support deterministic latency requirements. However, it cannot provide the necessary flexibility to support the mobile industrial applications required by the factories of the future. This can be achieved by integrating TSN with the 5G/IMT-2020 network, as it was designed to support ultra-reliable, low-latency communications. This has generated significant interest in integrating 5G/IMT-2020 and TSN networks, and the first framework for such integration has been identified. However, work is at an early stage, and solutions to effectively integrate the two networks so that 5G/IMT-2020 can support TSN QoS levels have yet to be developed. This article provides an overview of TSN and 5G/IMT-2020 technologies, as well as the concept of their joint work.
Key words: TSN, IEEE, 5G/IMT-2020, IIoT.

Iliyn A., Mikhaylin A., Poruchikov A., Shishkin A. Cloud Technologies, Using the Example of Flight Simulator, Games and Photorealism. – PP. 509–513.
This article is devoted to an overview of the applications of cloud technologies on the example of the Microsoft Flight Simulator, the necessary budget for the implementation of small projects using cloud technologies, the implementation of cloud computing on the example of creating a 3D scene based on photographs. The influence of use in games, examples of implementation, as well as an analysis of the further development of cloud technologies in various fields are considered.
Key words: cloud technologies, geodata, graphics.

Kazakevich E., Proshin F. Modeling of the Process of Mapping Signals in OTN Units with Allowance to Transmitting PTP-packets. – PP. 514–519.
The capacity of telecommunication network functioning under a condition of increasing the packet traffic is a foreground requirement for modern manufacturers. The transport network assumes using multipurpose data processing algorithms that can work with a stable synchronization between network elements. The PTP is the simplest method of attainment the synchronous work in a complex network with a multiplicity of elements, so it can be applied to OTN. The implementation of that mechanism taking into account OTN architecture with a frame and multiframe principles is possible as a variant at Ethernet level. This work is directed to analysis of PTP-messages processing and forming the algorithm of it. The simulation model of clock correction cycle is suggested to show which of processes affect on accuracy and how important an asymmetry. The model can be tuned according to condition of network functioning and equipment characteristics.
Key words: OTN, synchronization, PTP, agent model, AnyLogic.

Kazakov N., Konovalova V., Kovtsur M., Salita A. Development of a Method for Detecting Arp Inject Attacks in a Wireless Network of the IEEE 802.11 Family. – PP. 519–523.
The article discusses how to detect an ARP Inject attack on a wireless access point. ARP Inject or otherwise ARP-spoofing is a type of MitM attack based on the manipulation of the mechanisms of the ARP protocol. In the modern world, the use of a wireless network is becoming more popular and convenient way to transfer data every day. Unfortunately, this method has a number of vulnerabilities, one of which is used in the attack under consideration, which leads to a violation of the availability of data, as well as their confidentiality. Detecting an attack will minimize the risks associated with the presence of vulnerabilities in the wireless communication channel and protect critical data. In order to identify an attack, it is necessary to build a model that describes its distinctive features, which will be discussed in this article.
Key words: ARP, IEEE 802.11, wireless, intrusion detection, ARP Inject.

Katasonov A., Pesin A., Tcvetkov A. Identifying the Key Parameters of Rootkits at the Kernel Level to Modify the Detection Model. – PP. 524–530.
The most important part of the operation system is the kernel and it plays big role in managing data structures for correct operations. Kernel-level rootkits are the most "difficult to detect" type of malware, which can modify running operation system kernel in order to hide its presence and perform many malicious actions, such as hiding processes, modules, network connections etc. In this paper we give an insight into the characteristic features of kernel-level rootkits and how they can be used to train models in order to detect both known and unknown attacks.

Key words: cyber security, Rootkit, kernel modules, digital forensics, machine learning.

Kirichek R., Krivets A. Programming Cyber-Physical Systems using Visual Programming in the FLProg Application. – PP. 531–534.
Currently, applications of cyber-physical systems have been actively developed. In most cases, the development of certain applications is associated with the programming of controllers. Ignorance of programming languages is a limiting factor when creating projects related to sensors, microcontrollers, sending data to cloud platforms. Programming the Arduino open hardware development board requires knowledge of the C language, but the process of learning it is quite lengthy. To solve this limitation, an open source software product FLProg was created. Software which is a graphical programming environment for Arduino, ESP32, ESP8266 and Intel Galileo boards. In FLProg, you can create all kinds of projects with connecting a huge number of sensors, and most importantly, for this you just need to assemble several graphic blocks in the right order. As a result of the correct assembly of the blocks, a program code is generated that is loaded into the microcontroller using the Arduino IDE. The article highlights the FLProg application, its functional features and examples of projects implemented in this application.
Key words: visual programming, cyber-physical systems, FLProg, Arduino, smart home.

Kirichek R., Rozhkov M. Comparative Analysis of 5G Networks Architecture Based on GSMA and O-RAN Recommendations. – PP. 534–538.
5G is technology standard for broadband cellular networks developed by 3GPP. Unlike previous generations, which required the deployment of core networks and radio access networks on systems of the same generation, together forming a 4G system, the ideology of new generation 5G networks is to complement existing architectures of radio access networks, which allows integrating elements of different generations into different network configurations. While 3GPP defines both a new 5G core network and a new radio access technology called 5G "New Radio", operators are free to choose the methodology for integrating a 5G system into their legacy network architecture. In this regard, the GSMA organization and the O-RAN alliance have developed scenarios for the evolution of 4G network architecture. The article discusses the key features of each of the architectures built based on the GSMA and O-RAN recommendations, their similarities, and differences, as well as the main pros and cons of these methods of building a network infrastructure.
Key words: 5G networks, radio access, wireless networks, virtualization, standard.

Kirichek R., Filin E. Investigation of the Functioning of a Fragment of the lPWAN Network under Conditions of Intentional Electromagnetic Influences. – PP. 539–543.
The Internet of Things has become an indispensable element of information technology, the importance of which will only increase every year. One of the technologies used for data exchange is energy-efficient long-range networks (LPWAN), the main features of which is data transmission in dense urban areas for low-power devices. The task of studying models and methods of intentional electromagnetic influences on the communication channel is urgent. In this paper, the results of an experiment on the implementation of interference on the LoRaWAN network are considered.
Key words: LPWAN; LoRaWAN; LoRa; IEMI.

Kirichek R., Cherkasova A. Model of Testbed Federations for 5G / IMT-2020 Networks. – PP. 543–548.
At present, 5G/IMT-2020 networks are at the stage of testing the technologies used in them. Various testbeds are being actively created and combined. This paper discusses a generalized model for interoperable testbed federations required for comprehensive testing of 5G/IMT-2020 networks
Key words*:* testing, 5G/IMT-2020, API.

Kiryanov A., Toroptsev A. Functional Model of the Prototype Software Tool for Label Swapping of L2 VPN MPLS-Tunnels. – PP. 548–551.
In the process of using L2 VPN MPLS virtual private tunnels, it is possible to use MPLS labels that indicate the network of the used tunnel to simplify the verification of the type of traffic passing through it. To eliminate this possibility, a prototype software tool for L2 VPN MPLS tunnel label spoofing was developed.
Key words: confidential traffic, MPLS L2 VPN, identifying features.

Kislyakov S., Mayorov V. Development of a Business Process for Connecting a Service Based on TM Forum Open Digital Architecture. – PP. 551–556.
As telecommunications technologies penetrate into other areas of activity, OSS/BSS focused only on the telecommunications sphere remain difficult to apply. TM Forum employees have been developing the telecom operator automation ideology - NGOSS/Frameworx - since 1995. But at present, information and telecommunication technologies are an integral part of almost all areas of everyday life - banks, medicine, education, etc. The concept of NGOSS/Frameworx, focused on the telecommunications industry, does not make it easy to automate IT solutions for other areas of activity. Therefore, in an evolutionary step towards automating other areas of activity, TM Forum began developing a new concept called Open Digital Architecture (ODA). At the same time, ODA will continue to support the automation of telecom operators. Software solution providers will naturally be forced to apply new principles and recommendations for their developments. Based on the ODA, a business process for connecting a service to a client was developed.
Key words: Open Digital Architecture, eTOM, Operations Support System, Business Support System.

Kislyakov S., Makar M. Investigation of Properties of Chaoticity of Telecommunication Traffic. – PP. 556–561.
For a number of communication network management tasks, it is required to predict the incoming load or traffic intensity, separate and identify it. In particular, an important task is to predict the incoming load of a contact center or plan and place containers with running applications on network fog nodes according to changing demand and load. For both tasks, different approaches were used – trend-seasonal models were built, models based on artificial neural networks, but the results so far can hardly be called satisfactory. The complexity of forecasting time series that reflect the workload of a contact center or require a specific resource poses the challenge of finding new approaches.
The study is devoted to the study of the parameters of the chaotic process generated by the traffic of the incoming load on the Internet of Things applications hosted on edge/fog network nodes within the platform using container development technologies.
Key words: chaos theory, communication networks, telecommunications.

Kistruga A., Kovtsur M., Petrov M., Shabanov V. Technique for Detecting the Location of an Intruder Implementing a Deauthentication Attack on an IEEE 802.11 Network. – PP. 561–564.

Currently, wireless networks are gaining popularity, they have become more accessible and extensive. Due to the great popularity, attacks on wireless networks of the IEEE 802.11 family have become more frequent, so new methods and technologies are required to protect them. One of the popular attacks that is used by attackers is the deauthentication attack. The report presents a method for detecting the location of an intruder conducting a deauthentication attack on a wireless network of the IEEE 802.11 family.

Key words: IEEE 802.11, Deauthentication, Information Security, Wireshark, Packet Sniffing.

Kichko Ya. Problems and Prospects for the Development of Group Application of Unmanned Aerial Vehicles. – PP. 565–568.

The article examines the trends in the use of unmanned aerial vehicles, the main directions of their development in the United States and Russia. Analyzes the capabilities of modern unmanned aerial vehicles. Identified shortcomings of existing complexes that do not allow providing the required efficiency of data transmission in-group use of unmanned aircraft devices.

Key words: unmanned aerial vehicles, group application of UAVs, algorithms of data exchange, routing of data packets, distribution of flows, optimization of route tables system.

Kovalev I., Pantyukhin O., Pashchenko V. Modern Approaches to Recovery of the Information Process in Local Computer Networks. – PP. 569–573.

Modern approaches and methods of information recovery in local computer networks are considered. New ways of restoring the information process are proposed.

Key words: backup, data recovery, disk cloning, local area network, technical and organizational measures.

Kozhanov J. Methods for Improving the Cryptographic Strength of Messages. – PP. 573–576.

The general principles of symmetric encryption with private keys are considered. Methods for increasing the cryptographic strength of the system are proposed.

Key words: encryption, decryption, cryptographic strength.

Kokoreva E., Kostyukovich A. Analytical Evaluation of Positioning Error in Wi-Fi Network. – PP. 576–581.

Since every modern organization and institution has the local wireless Wi-Fi networks that provide mobile access to the Internet, using them to organize local positioning systems is an apparent idea. The article is devoted to analytical evaluation of the measurement error when calculating the mobile object's coordinates inside the premises without taking into account the multipath signal propagation, fading and other interference.

Key words: Wi-Fi network, geolocation, positioning, accuracy, error, object's coordinates calculation, lateration.

Kokoreva E., Shurygina K. Increasing the Local Positioning Accuracy by Optimizing the Placement of Access Points. – PP. 581–585.
Using Wi-Fi networks for construction of indoor object positioning system is the simplest and most cost-effective way. In such a system, the positioning is based on measuring the signal strength level indicator with the application of the lateration (trilateration) method to calculate the target's coordinates. The article is devoted to the improvement of positioning accuracy by correcting the network structure in accordance with frequency-spatial planning.
Key words: frequency-spatial planning, accuracy, Wi-Fi network, access point, positioning.

Kolomeets M. Informativity Analysis of Malicious Bots Features in Social Networks. – PP. 586–588.
Malicious social media bots are a serious threat as they are used by attackers for reputation gain, blackmail, fraud, misinformation and other malicious activities. At the same time, the task of detecting bots, both by expert methods and by machine learning methods, becomes extremely relevant. To do this, specialists need to understand what data sources may contain the distinctive features of bots in order to form effective decision-making methods based on them. This paper presents a statistical analysis of the informativeness of the features of the VKontakte social network bots by the types of data generated by the account: profile, textual information, media information, distributions, temporal distributions and adjacent accounts. The results of this analysis can be used to create new, more accurate detection methods based on both expert analysis and machine learning analysis.
Key words: information security, social networks, bot detection, statistical analysis, feature informativeness.

Kolomeets M., Chechulin A. Visual Model of the Computer Network Attack Graph. – PP. 589–591.
When analyzing the security of computer networks, automated approaches are often used, in which some decisions are made not automatically, but by the operator. Thus, when analyzing computer network attack graphs, the system operator can make decisions on determining the importance of network hosts, protection strategies, incident modeling, etc. In such a situation, it becomes necessary to provide the operator with convenient tools for manual and semi-automatic analytics, including the use of visual models. This paper presents a visual attack graph model that an operator can use to monitor the state of a computer network and make appropriate decisions. The paper also contains examples of the graphical implementation of this model based on data on a real computer network and its vulnerabilities.
Key words: risk analysis, network security, attack graphs, visual analytics.

Komarov I., Lobach D., Muthanna A. S. A. Intelligent Parking Management System for Unmanned Vehicles Based on Internet of Things Technologies. – PP. 592–596.
This paper discusses the main positioning technologies for unmanned vehicles; positioning accuracy, advantages and disadvantages are compared and analyzed, a smart positioning system for unmanned vehicles is proposed. The results obtained can be used in the framework of practical research and development of positioning in the field of V2X technology.
Key words: Internet of Things, Networks 2030, V2X, Artificial intelligence.

Koptelova V., Kosov N. Identification of the Advantages and Disadvantages of Trading Bots Application Among the Features of Their Functioning. – PP. 596–598.
This work is devoted to determining the need and feasibility of using trading bots in the field of electronic commerce by determining the advantages and disadvantages of such bots.
Key words: trading bots, e-commerce, automated program, advantages of trading bots, disadvantages of trading bots.

Korzhik V., Koucheryavy A., Yakovlev V. The System of Remote Electronic Voting in the Dissert Council the University. – PP. 599–603.
A remote electronic voting system is proposed in the dissertation council of the university, which ensures the fulfillment of the requirements of the Higher Attestation Commission for the voting procedure for awarding academic degrees while maintaining the confidentiality and anonymity of the votes of members of the dissertation council, which is relevant during the pandemic. The composition of the voting system, its parameters and the functioning algorithm are determined. At the heart of the cryptographic core of the voting system, it is proposed to use the cryptographic system of Paillier's homomorphic encryption.
Key words: remote electronic voting system, dissertation council, homomorphic encryption.

Korzhik V., Yakovlev V. Protocol for Key Distribution over Public Noiseless Channels Between Users Based on the Joint Use of Interactive Data Exchange Protocols. – PP. 604–608.
We study a key distribution system that includes three sequentially executed protocols. The first protocol is a protocol exchanging by integers over public noiseless channels (such as the Internet), in which legal users A and B exchange numbers $(p+n_A)$ *and* $(g+n_B)$*, respectively, where p, q are Gaussian random variables with parameters (0,1) , and* n_A, n_B*, are Gaussian random variables with parameters (0,σ). The raw key bits are calculated by the user A as* $K_A = rec[p(g+n_B)]$*, by the user B as* $K_B = rec[q(p+n_A)]$*, and by the intruder E, who controls the exchange of messages between A and B, as* $K_E = rec[(p+n_A)(g+n_B)]$ *, where* $rec[u]$ *is the operation of quantizing u into two levels by sign. The second protocol - the protocol of preferential improvement of the main channel of legal users (PIMC), is performed by transmitting a block consisting of s times repeated random number V=(0,1) by user A. Legal user B accepts the block if all bits in it are the same, otherwise the block is erased. The attacker receives this block and decodes it according to the majority rule. The PIMC can be applied t times. The third protocol, the degradation both channel protocol (DBC), is performed by splitting the sequence of key bits -and-bit addition of v blocks. Analytical relations are obtained to calculate the probability of mismatch of key bits for legal users and the probability of mismatch of key bits for a legal user and an intruder after the execution of each protocol.*
Key words: cryptography, key distribution, noiseless channels.

Kotenko I., Puchkov V. Graph Algorithms and Platforms Graph Database Management to Ensure Cybersecurity. – PP. 609–613.
The paper considers modern graph database management platforms. The possibility of using them as a tool in the analysis of data graphs to ensure cybersecurity, including in assessing the security of cyber-physical systems, is determined. The advantages and disadvantages of graph databases in comparison with traditional relational databases are given. The main attention is paid to the methods of assessing security based on the analysis of attack graphs.

Key words: graph database management systems, cyber-physical systems, security assessment, attack graphs.

Kotenko I., Khmyrov S. The Model of Compromising Critical Information Infrastructure Objects. – PP. 614–619.
Objects of critical information infrastructure (CII) are protected by the state, and security requirements are regulated at the legislative level. The paper considers non-standard methods and vectors of attacks on CII objects. The characterization of the violator implies his high potential and broad opportunities for conducting cyber operations over the victim's infrastructure, as well as high motivation to achieve the goal. The main content of the article is the proposed model of compromising CII objects, built on the basis of existing methods of compromise and vectors of attacks on CII objects.
Key words: targeted attacks, critical infrastructure, attribution of cyber intruder, cybersecurity.

Kropotova K., Mozhginskiy V. Studying the Technology of Multichannel Telecommunication Systems on the Example of Equipment of Cable TV Broadcasting Systems. – PP. 619–622.
The main principle of building multichannel telecommunication systems for many decades has been the frequency division of channels. Now the study of the technology of analog multichannel systems with frequency division of channels has remained only at the theoretical level, although in our opinion it deserves a more thorough practical development, since the principles of this technology are extremely widely and widely used.
Key words: multichannel telecommunication systems, frequency division of channels.

Krylov A., Ushakov I. Security Metric of the Internet of Things. – PP. 622–626.
The Internet of Things (IoT) is a network of devices that are uniquely identified and have embedded software required to transmit information. Network endpoints and protocols are used to communicate with a cloud server, which processes and aggregates big data from various devices, performs analytics, and helps in making business decisions. The IoT is a significant part of today's revolution in industry, agriculture, healthcare and smart cities. Ensuring the security of all actors involved in the IoT network is especially important as it involves the widespread collection and dissemination of data.
Key words: smart cities; Internet of Things (IoT); IoT security; Security risk assessment; IoT protocols; IoT Threats.

Kuznetsov K., Muthanna A. S. A. Implementation Methods of Immersive Technologies in Fifth Generation Communication Networks. – PP. 627–631.
Every year there is an increasing demand for high-speed, reliable data transmission system for the tasks dictated by consumers everywhere with the introduction of mobile fifth generation networks. One of the main problems of such networks is to ensure, as stated in IMT-2020, the latency at the level less than 1 ms. Due to the concept of Tactile Internet there is a demand for very low latency, which requires to exceed the speed of light when transmitting information between the end-devices. To achieve such indicators it is planned to apply various technologies allowing to move services closer to the subscriber (MEC), virtualize and adaptively move network functions (NFV), as well as predictively analyze traffic and discrete human actions.
Key words: 5G, Tactile Internet, MEC, NFV.

Kuznetsov M. Modern Approaches to Formalization and Modeling of Scenarios for the Use of Personal Data. – PP. 632–637.
The collection and use of personal data to meet the digital needs of users are extremely common scenarios today. Users actively provide their personal data to improve the quality of digital services, without always being aware of what data they transmit and how it will be processed. At the same time, user agreements are the only way to inform about what personal data is used and how. There are various approaches to increase the transparency of user agreements, in particular the method based on ontological modeling. This paper discusses the results of the application of ontologies in the field of regulation of the collection and use of personal data, obtained in relevant works on the topic.
Key words: privacy policy, formal representation, ontology, personal data.

Kushnir D., Nikonov E. Consensus Algorithms and Approaches to Their Implementation in Blockchain Systems. – PP. 637–642.
The article discusses the blockchain technology consensus algorithms, their software implementation features in the Python programming language. From the block formation, further analysis of the current state of the distributed ledger up to the usage of hybrid consensuses.
Key words: blockchain, distributed ledger, information security, key, sign.

Kushnir D., Skrobov D. Ensuring Security in Blockchain Technology. – PP. 642–648.
With the expansion of connectivity, the popularization of cloud services and the rise of the Internet of Things (IoT), decentralized approaches to trust are gaining momentum. Because blockchain technologies provide a distributed ledger, they are gaining tremendous attention from the research community in a variety of applications. The purpose of this study is a general analysis of blockchain technology and the study of the issue of ensuring security in such technologies.
Key words: blockchain, security, information protection, internet of things, distributed ledger technology.

Ostroumov O., Lapin S., Lepeshkin O., Chernykh I. Methodological Approach to of a Communication System Functional Stability Comprehensive Assessment. – PP. 649–653.
Considering any system performance of its target installation, it is necessary to take into account the available resources. One of the main resources is time. Modern communication systems, the main purpose of which is to ensure the transmission of all types of messages and the provision of all types of services, are very dynamic. The fulfillment of the goal by the system is ensured by the elements stable functioning. The paper proposes an approach to assessing functional stability in three stages. The need to assess the consequences of destabilizing factors impact on critical objects of the communication system is being updated.
Key words: critical information infrastructure, critical facility, functional stability, control system, communication system.

Pavlov I., Lebedyantsev V. General Methodology of Synthesis of Systems Invariant to Additive Interference. – PP. 654–657.
The article discusses a general methodology for the synthesis of systems invariant to non-additive interference Ξ, which leads to a change in signal parameters. For comparison, the

systems invariant with respect to interference Ξ in the class of systems with constant parameters and non-constant parameters are taken. The methods of modulation and demodulation are determined.
Key words: non-additive interference, invariant communication systems, additive interference, modulation, demodulation, noise immunity.

Levshun D. A Tool for the Expert Evaluation of the Text Publications Tonality. – PP. 657–661.
A tool for the expert evaluation of the text publications tonality is a web application that is developed on the Flask framework using the Python programming language that interacts with a PostgreSQL database. The process of the user's work with the application can be divided into three stages: (1) filing an application for the registration as an expert; (2) authorization in the system; (3) evaluation of the tonality of text publications. At the same time, the text of the publication is divided into the text of the post and the text of the repost. This is done due to the functionality of social networks, which allows one to post publications of other users and communities on personal pages, supplementing them with a comment. The text of the original publication is used as the text of the repost, and the comment left during the posting is used as the text of the post. At the same time, the tonality of the post and repost is evaluated both separately and jointly, while the range of assessments is reduced to the following qualitative characteristics: (1) positive, (2) negative, (3) neutral, (4) skip. Currently this tool is used to create a labeled dataset. This dataset will be used for the supervised learning of one of the components of the system for monitoring and identifying negative personal tendencies of the younger generation when interacting with the Internet space.
Key words: social networks, analysis of the psycho-emotional state, identification of negative personal tendencies, expert evaluation, tonality analysis, dataset labeling.

Lobastova M., Lytkina E., Matyukhin A. Formation of the Simulation Model of the Audio Traffic Generator – PP. 661–664.
Audio traffic can be described by two processes: the process describing the incoming telephone calls and the process of generating data packets used by the codec. The article considers a model of an audio traffic generator that continuously creates packets according to a given distribution law. For VoIP traffic, its probabilistic and temporal characteristics are determined, such as the distribution law at the moment of the conversation, and an analysis of the time between calls and the duration of the conversation is also made. AnyLogic software was used for simulation modeling.
Key words: audio traffic generator, simulation, distribution law, simplest flow.

Makarova A., Polyanicheva A., Samatova K. Analyzing the Vulnerabilities of Voice Traffic Transferring Technologies. – PP. 665–669.
The Voice over IP technology allows for the transfer of voice communications over an IP network and has significant advantages over analog phone connections. Due to the widespread use of this technology, the safety of this transfer is a relevant issue. This article presents a brief overview of VoIP technology vulnerabilities and examines the most common and dangerous vulnerabilities in voice traffic transfer. This study resulted in conducting a criteria analysis of the most common vulnerabilities, and the subsequent identification of relevant defense methods.
Key words: telephony, IP telephony security, vulnerabilities, Voice over IP, VoIP.

Maksimova E., Shterenberg I. Building a General Model of an Adaptive RPA System for Protecting Software in a Local Computer System. – PP. 670–679.

The self-modifying code for information stegoving in an adaptive RPA system is an element of RPA program, namely self-modifying code that can be available for use by an operator. The peculiarity of self-modifying code is in its steganographic transformations, that is, in its ability to remain unnoticed by the system and most successfully stored in file structures. The self-modifying code for the stegraphic information in the adaptive RPA system in addition has a mechanism of self-description or self-modification, which rather resembles polymorphic computer viruses. However, the element of stealth and development illustrates the analogy with bionic systems, where every living cell seeks to survive and protect itself. Such a pattern and such a possibility would allow RPA to protect itself from total destruction and reactivate itself in the system.

Key words: AC – Adaptive System, RPA – Robotic process automation, PO – software program, methods of protection.

Mineev N., Pomogalova A. Development of a Multifunctional Platform for Accounting Works of art Using Decentralized Registry Technology. – PP. 679–683.

The current project aims to create a platform that enables both secure financial transactions with art objects and the keeping of records of art objects. Using blockchain technology, which is a kind of decentralized registry, users can be assured that their organization is assigned certain art objects through a certificate of authenticity for physical art objects as well as a record in the blockchain itself. With the blockchain record, all users can track the description of the art object, the history of the owners since first registering on the platform, the author of the artwork, and the current value of the artwork.

The project uses Ethereum blockchain because of its ability to create smart contracts within the blockchain itself, allowing for secure transactions related to art objects, and a large developer community that provides many different tools for developing and testing smart contracts based on the Ethereum blockchain, as well as implementing them in a client-server application structure.

Key words: blockchain network, blockchain, decentralized registry, data storage, copyright, intellectual property.

Minyaev A., Parshin E. Analysis of Processes of Safe Development of DevSecOps. – PP. 683–689.

The publication touches on the topic of secure DevSecOps development. The advantages of this process, the necessary requirements for successful implementation are considered. In addition to everything, it was found out why security should be automated, what problems can arise with inexperienced or incorrect use. Is it possible to successfully implement DevSecOps without certain experience. We have found that many understand DevSecOps as the integration of testing and security practices into the DevOps development methodology. Should everyone be responsible for security? What needs to be automated in secure development and with the help of what? The author has tried to answer all the questions and on the basis of this draw the appropriate conclusions.

Key words: DevSecOps, Information security, secure development, DevOps.

Morozov I., Parashchuk I., Sayarkin V. Analysis of the Basic Principles and Requirements for the Construction of Information Security Subsystems in Modern Electronic Document Management Systems. – PP. 689–693.

The analysis of conceptual and target requirements for the construction of information security subsystems for modern electronic document management systems is carried out. The general methodological principles of the construction and functioning of subsystems of this class are formulated. These results are intended to help in the development and technical implementation of highly effective tools and complexes aimed at operational and qualitative solutions to the tasks assigned to the information protection subsystem for modern electronic document processing systems.

Key words: information security subsystem, electronic document management system, electronic document, principles, requirements, resources, user, system.

Muthanna A. S. A., Nikitin E. Possibilities of Using Fifth-Generation Networks in the Millimeter-Wave Band, for the Operation of IoT. – PP. 693–698.

Fifth-generation communication networks have been developed with three main objectives in mind - increasing bandwidth, reducing latency and supporting reliable connectivity. To address these challenges, 3GPP developed a set of specifications for NR in 2019, one of the most important developments was the possibility of using the technology in millimeter-wave bands. But it is worth noting the fact that the implementation of Internet of Things Applications This article will investigate the possibility of such devices working in millimeter-wave bands.

Key words: fifth-generation networks, millimeter-wave range, IoT

Muthanna A. S. A., Rusakov A. The Need to Move to Edge Computing in the Industrial Internet of Things. – PP. 699–703.

This article will discuss the existing concepts of the Industrial Internet of Things and Edge Computing, as well as the benefits of implementing edge computing in the Industrial Internet of Things and a possible network architecture built using this approach.

Key words: industrial internet of things, edge computing, fog computing.

Muthanna A. S. A., Tagandurdyyev N. Study of Aspects of UAV Deployment for the Implementation of Smart City Applications. – PP. 704–707.

5G is a technology that makes it possible to bring to life a huge number of concepts and ideas that were previously not feasible due to the limited capabilities of computing and telecommunication systems. The smart city is one such concept. Ultra-high speeds, massive machine-to-machine communications, ultra-low latency are services that can provide a solid foundation for the implementation of smart city applications. Environmental monitoring, vehicle traffic tracking, emergency call systems are just a few of the applications that a smart city and, in turn, 5G can offer.

The efficiency and quality of implementation of the above 5G services depends on the technological solutions of the computing environment. MEC is one such solution. Building unmanned aerial vehicles based on MEC will lead to increased efficiency and quality of services for the smart city.

This article analyzes the organization of unmanned aerial vehicles together with MEC and SDN technologies to implement the concept of a smart city. This article illustrates the functional features of the architecture of the urban network of the future. The features of the interaction of urban communication centers with the network infrastructure are also shown.

Key words: SDN, Edge Computing, 5G, vehicular network, IoT.

Neelova O. The State Machine Model for Manage Dynamic Branch Predictions. – PP. 708–710.
This item have described the dynamic branch prediction process. Specifically, it presents the model of state machine for operate branch prediction's bits.
Key words: branch predictions, prediction's bits, state machine, tag's memory.

Nikitin B., Polyakova E., Sergeev A. Quantum Sensorics. Current State and Development Trends. – PP. 710–716.
Quantum technologies will determine the further development of modern science and technology. In Russia, there is an opportunity to create a significant potential for breakthrough and capture leading positions in certain areas. Quantum sensorics is one of the directions of development of quantum technologies, which has very good prospects. With the right approach to the development of the potential of this area and the training of a sufficient number of highly qualified specialists in this field, a qualitative breakthrough is possible in various sectors of the economy, science and technology.
Key words: quantum sensor, quantum measurement systems, fiber optic, TRL-x.

Novikova E. Analysis of Approaches to Design of the Intrusion Detection Systems Based on Federated Learning Principles. – PP. 716–719.
One of the open problems related to the security of systems based on the Internet of Things technology is the problem of the privacy and security of the sensitive and critical data that are important in intrusion detection task. A possible way to solve this problem is to use federated learning to design intrusion detection systems. Federated learning (FL) is a relatively new model of the privacy preserving distributed machine learning. This paper explores the applicability of FI for building an intrusion detection system for critical infrastructures to ensure the privacy of the data that describe technological processes and equipment settings. The federated learning systems presented in the literature are analyzed and their advantages and disadvantages are discussed.
Key words: Internet of Things, anomaly detection, privacy, federated learning.

Okuneva D. Business Analysis and Application Design Software. – PP. 720–723.
The article presents an overview of the capabilities of the modern development environment for applied solutions 1C:EDT. It is based on the development environment for modular cross-platform applications Eclipse. The main difference from the 1C:Enterprise 8 configurator is that when using 1C:EDT, you can develop a configuration outside the context of the 1C:Enterprise 8 platform. 1C:EDT supports the principles of creating application solutions on the 1C:Enterprise 8 platform, facilitates the work of a programmer due to built-in automation tools, and allows expanding the functionality of development tools using plug-in technology. In addition, to analyze the structure of a business application in the form of an ER diagram, the Data Schema functionality is used, group development and versioning is performed using the external version control system Git.
Key words: 1C:EDT, GIT, business analysis, configurator, applied solutions, java, eclipse.

Orlov D., Salman W., Yakovlev V. A Method to Ensure the Anonymity of Electronic Voting from the Attack of Tracking the Votes of Individual Voters. – PP. 723–726.
A method is proposed to protect the anonymity of voters based on the representation of the voter's vote (number) as the sum of the terms and encryption separately of each term. Further, the cryptograms obtained by encrypting the terms are sent to different servers for multiplication. The anonymity of the voter's vote is ensured if at least one server is "honest".
Key words: electronic voting, homomorphic encryption system, Paillier cryptosystems, anonymity of electronic voting.

Parashchuk I., Chechulin A. Fuzzy Identification of Vulnerabilities in the Interfaces of the Unmanned Transport Environment of the «Smart City». – PP. 727–732.
An approach to the formal description of the signs of vulnerabilities in the interfaces of the unmanned transport environment of the «smart city» in order to identify threats is proposed. This approach is based on the method of solving problems of identification of objects and processes in the conditions of fuzziness of their observed features. This method is aimed at eliminating the fuzziness (as one of the types of uncertainty) of identifying vulnerabilities of interfaces of this class. It is based on the use of fuzzy and linguistic variables when processing fuzzy knowledge about the characteristics of potential vulnerabilities. Solving such tasks will increase the reliability of monitoring the security of interfaces, increase the security of unmanned vehicle control systems.
Key words: smart city, interface, unmanned vehicles, vulnerability, fuzzy sets, linguistic variable**.**

Pahomov M., Saharov D. To the Question of Detection of Anomalies in Signal Traffic on the Basis of Intelligent Data Analysis. – PP. 732–737.
This paper presents data mining methods for detecting anomalies in 5G signaling traffic. An experiment on generating anomalies in signal traffic has been carried out, approaches and algorithms for detecting anomalies have been developed. A comparative analysis was carried out and conclusions were drawn about the effectiveness of the above methods for solving the problem.
Key words: signal traffic, data analysis, machine learning, information security, anomaly detection.

Permyakov A., Smirnov I. Monitoring and Certification System of Fiber-Optic Infrastructure of Public Communication Networks Based on Interferometric Methods. – PP. 737–742.
In this paper, the issue of the organization of monitoring and certification of fiber-optic infrastructure in public communication networks is considered. The solution proposed by the authors for the development of a monitoring and certification system is aimed at increasing the awareness of decision makers about the state of the fiber-optic infrastructure of public communication networks.
Key words: public communication networks, fiber-optic communication lines, infrastructure monitoring, certification, interferometer, database.

Pestov I. Methodology for Countering Threats to Information Security Violations of Instances and Cloud Infrastructure, Based on a Description of Attacks and Methods to Counter them Using Graph Theory. – PP. 742–746.
Methods for countering information security threats are becoming increasingly popular today, since automation of this process will significantly reduce the response time to an attack and, as a result, the downtime of the information system. A simple information system entails not only financial losses, but also reputational ones, which is unacceptable for an organization of any type.
Key words: Information security, attack analysis, graph theory, countering threats.

Pestov I., Fedorova Z. Analysis of Virtual Machine architecture. – PP. 747–751.
The use of a virtual machine, its technical and user parameters are determined by the architecture of the virtual machine. Virtualization has become an important tool for developing computer systems. Architectural elements appear with new or improved characteristics. Advantages and disadvantages of virtual machines.
Key words: virtual machines, virtualization, hypervisor, operating system.

Pestov I., Khristoforov R., Shvidkiy A. Analysis of Approaches to the Development of Cloud Services. – PP. 752–757.
This article presents the results of a research approaches to the development of cloud services. As part of the research, the following tasks were solved: key cloud models were considered, approaches to application architecture design and cloud software development methods were analyzed.
Key words: Cloud services, cloud infrastructure, development tools.

Rafalskaya M. Graphical Representation of Multidimensional Dependencies of Traffic Quality Indicators on the Parameters of its Distribution Along Several Routes. – PP. 757–762.
One of the mechanisms for ensuring the quality of traffic service is its distribution along several routes. The methods of visual graphical representation of multidimensional dependencies of traffic quality indicators on the parameters of its distribution along several routes by reducing these dependencies to the functions of one and two arguments are considered.
Key words: multidimensional graphs, traffic distribution, traffic service quality.

Reznikov B., Stepanenkov G., Tarabanov I. Vulnerability of Optical Data Transmissions. – PP. 763–766.
Nowadays, communication systems using optical data transmission channels are becoming more and more popular. This article gives an overview of the main vulnerabilities of networks using optical communication technologies and possible solutions to identify emerging threats in the communication system.
Key words: optical communication systems, data protection, optical transmission system security, vulnerability.

Saenko I., Udaltsov A. Analysis of Sinchronization of Database in the Absence of Deterministic Queries. – PP. 767–771.
The paper incorporates issues of synchronization of databases in the absence of deterministic queries. Analysis of possible types of synchronous replication. The conditions for selecting a format of fixing in the database are justified.
Key words: database, synchronization, replication.

Sinyuk A., Tarasov A. The Evaluation of the Possibility of Open Generation of Multiple Keys in the Communication Network. – PP. 771–774.
The network cryptographic connectivity of correspondents is most susceptible to destruction when a common key is compromised by an enemy. The search for conditions for the open and simultaneous formation of several keys in the communication network is updated. An information-theoretic assessment of the possibility of forming multiple keys in the process of open network multi-key matching is carried out by evaluating the information basic sets for key formation. The directions of further conditions are given.
Key words: broadcast communication channel, enemy, key, entropy, mutual information, joint information, information speed, open network multi-key agreement.

Spirkina A. Development of the Simulation Model of the Blockchain System. – PP. 775–780.
This paper describes the development of a simulation model of the blockchain system, which includes a generalized traffic model and takes into account the properties of the subsystem processes.
The models proposed by the author are simple but powerful tools for identifying many important indicators, such as the rate of occurrence of transactions per second, block size, block processing time by validators, which affect certain characteristics, for example, waiting time in the memory pool, packet residence time in the system, transaction delay.
Key words: distributed registry, blockchain, QoS, Quality of service.

Fedorova O., Tsvetkov A. Development of a Kernel-Level Rootkit Detection Algorithm Based on the Interception of Operating System Kernel Events. – PP. 780–784.
Rootkits are a type of software that specializes in hiding entities in computer systems, providing continuous control or access to them, it is especially difficult to detect compared to other types of software. There are various tools for detecting rootkits using a wide range of detection methods and mechanisms. However, the effectiveness of such tools is not fully proven, especially in modern academic research and in the context of the Linux operating system.
Key words: Linux kernel, Linux kernel module, RootKit, superuser rights, system calls, hardware interrupts, protection mechanism, virtual laboratory stand.

Sharlaeva M. Research of Methods of Poisoning in Augmented Reality. – PP. 784–788.
In this article the existing methods of determining the location of objects in order to choose the most effective when creating applications of augmented reality are considered. Navigation in augmented reality is more demanding than tracking mobile robots. It is necessary to ensure a high level of accuracy in real time and to extend the range, taking into account the diversity of surrounding objects. Further use of the most efficient algorithm is to create an augmented reality application for the visually impaired.
Key words: marker technology, no-marker technology, location methods, augmented reality.

Shvidkiy A. Analysis of Methods for Determining the Characteristics of Data Storage Systems of Different Types of Load. – PP. 788–793.

The paper analyzes the methods of determining the characteristics of distributed data storage systems by identifying various parameters for load patterns. The questions of influence on the performance of distributed storage system architecture are considered separately because the peculiarities of its design do not allow to apply to the analysis the same methods which have been used for the analysis of the classic storage systems. Based on the analysis we propose load generation templates that reflect the basic requirements for load testing.

Key words: storage system, software-defined storage, distributed storage.

Yakovlev V. Formalization of a Model of a Physically Uncloneable System Based on a Universal Class of Hash Functions. – PP. 793–798.

A physically unclonable function (PUF) is a characteristic of a physical (digital) system that cannot be cloned (reproduced, copied) on other physical systems. One of the important PUF parameters is the unpredictability of the response for a given request. The problem of formalizing the PUF parameters is that with limited physical (linear) dimensions of the PUF, the number of PUFs is polynomially limited, so the output characteristics of different PUFs for the same queries become repetitive. A formalization of the PUF parameter based on a class of strongly universal$_2$ hash functions is proposed, which makes it possible to quantify the PUF unpredictability parameter and formulate requirements for the PUF used in various applications.

Key words: physically uncloneable functions, universal hash functions, unpredictability.

Yakovlev V. Key Distribution System over Public Noiseless Channels Using Exchange by Integers Between Users. – PP. 799–803.

A communication network of M correspondents is considered. For correspondents to work with each in a secure mode, they form paired keys as follows. Each correspondent, for example, A generates: a secret Gaussian random number a with parameters (0,1); and an open random number ($a+n_a$), where n_a is a Gaussian random number with parameters ($0,\sigma^2$). Open random numbers are placed by all correspondents in the storage, access to which each correspondent has access, including attacker E (without the right to modify numbers). If correspondents A and B want to form a common key, then they go to the storage of public numbers and get the numbers ($b + n_b$) - A and ($a + n_a$)- B) in it, respectively. and form bits of the "raw" key: $K_A = p(g + n_B)$ corr. A and $K_B = q(p + n_A)$ corr. B. An attacker E can form an estimate of the correspondent pair's key. The following assertions have been proved:

1. The keys of any pair of correspondents A and B are not correlated with the key of the third correspondent C.

2. Estimates of the attacking key with respect to the keys of two pairs of correspondents K_{EAB} and K_{EAC}, are uncorrelated.

Key words: cryptography, key distribution, noiseless channels.

СВЕДЕНИЯ ОБ АВТОРАХ

АББАСОВ Мехраб Фахраддин оглы — студент группы ИКПИ-91 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, mehrababb@gmail.com

АБРАМЕНКО Георгий Тимофеевич — студент группы ИКТБ-17м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, georgabramenko@gmail.com

АБРАМОВ Сергей Степанович — доктор технических наук, доцент, заведующий кафедрой радиотехнических устройств и техносферной безопасности, профессор кафедры радиотехнических устройств Сибирского государственного университета телекоммуникации и информатики, академик МАС, abramov@sibsutis.ru

АБРАМОВА Евгения Сергеевна — кандидат технических наук, доцент, доцент кафедры радиотехнических устройств и техносферной безопасности Сибирского государственного университета телекоммуникации и информатики, evgenka_252@mail.ru

АЛЕКСАНДРОВ Игорь Васильевич — соискатель кафедры программной инженерии и вычислительной техники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, chrono555@yandex.ru

АЛЕКСЕЕВА Надежда Николаевна — ассистент кафедры инфокоммуникационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, alekseeva.nn@spbgut.ru

АЛЕХИН Роман Вячеславович — студент группы ИКБ-95 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, roman2001-10@outlook.com

АЛЬ-СВЕЙТИ Малик А. М. — аспирант кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ma_sweity@mail.ru

АНДРЕЕВА Елена Ивановна — кандидат физико-математических наук, доцент кафедры фотоники и линий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, andreevaelenafils@gmail.com

АНДРЮНИН Александр Игоревич — студент группы ИКТФ-16м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, Sasha4365@gmail.com

АНТОНЕНКО Анастасия Дмитриевна — студентка группы ИКТИ-05м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, glutton02@gmail.com

АХМЕТШИНА Милена Энверовна — студентка группы ИКТБ-07М Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А.Бонч-Бруевича, ahmet-mil@yandex.ru

АХРАМЕЕВА Ксения Андреевна — кандидат технических наук, доцент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, cbor.mail@gmail.com

БАБАЕВ Амиль Балаоглан оглы — старший преподаватель кафедры информационных технологии и программирование Бакинского инженерного университета, amil.babaev@beu.edu.az

БАБКОВ Иван Николаевич — кандидат технических наук, доцент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ib9809@mail.ru

БАКАТОВ Виталий Николаевич — студент группы ИСТ-851 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, bakatovvitalij@gmail.com

БАТЕНКОВ Кирилл Александрович — доктор технических наук, доцент, сотрудник Академии Федеральной службы охраны Российской Федерации, pustur@yandex.ru

БЕККЕЛЬ Людмила Сергеевна — кандидат технических наук, доцент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича

БЕЛАЯ Татьяна Иоанновна — кандидат технических наук, доцент кафедры программной инженерии и вычислительной техники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, studentszip@yandex.ru

БЕРЕЗИН Александр Юрьевич — аспирант кафедры программной инженерии и вычислительной техники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, berezinalexhdr@gmail.com

БИРЮКОВ Михаил Александрович — кандидат технических наук, доцент кафедры программной инженерии и вычислительной техники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, urgent.ma@gmail.com

БОБРОВА Ксения Борисовна — аспирант кафедры «Электрическая связь» Петербургского государственного университета путей сообщения Императора Александра I, ведущий инженер ЗАО «Институт телекоммуникаций», atorina141@yandex.ru

БОГОМАЗ Мария Эдуардовна — бакалавр, студентка кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, maria.bogomaz15@gmail.com

БОГОМОЛОВА Мария Анатольевна — кандидат технических наук, декан факультета информационных систем и технологий Поволжского государственного университета и информатики, bmasamara@mail.ru

БОРОВСКАЯ Яна Александровна — магистрант кафедры сетей и систем связи Поволжского государственного университета телекоммуникаций и информатики, yana.borovskaya.98@mail.ru

БРАНИЦКИЙ Александр Александрович — кандидат технических наук, старший научный сотрудник лаборатории проблем компьютерной безопасности Санкт-Петербургского Федерального исследовательского центра Российской академии наук; доцент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, alexander.branitskiy@gmail.com

БУГРОВА Екатерина Сергеевна — студентка ИКБ-95, техник НОЦ «Программно-определяемые системы» Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, bugrova.es@sut.ru

БУРДИН Владимир Александрович — доктор технических наук, профессор, заведующий кафедрой линий связи и измерений в технике связи Поволжского государственного университета телекоммуникаций и информатики

БУРДИН Антон Владимирович — доктор технических наук, доцент, заместитель генерального директора по научной работе и развитию АО «НПО Государственный оптический институт им. С.И. Вавилова»; профессор кафедры фотоники и линий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича; профессор кафедры линий связи и измерений в технике связи Поволжский государственный университет телекоммуникаций и информатики, bourdine@yandex.ru

БУХАРИН Владимир Владимирович — доктор технических наук, доцент, профессор кафедры автоматизации предприятий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, bobahbuch@mail.ru

БЫЛИН Алексей Романович — ведущий инженер-программист кафедры фотоники и линий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, aborn2772@gmail.com

БЫЛИНА Мария Сергеевна — кандидат технических наук, доцент, заведующий кафедрой фотоники и линий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, BylinaMaria@mail.ru

БЫСТРОВ Илья Сергеевич — аспирант лаборатории проблем компьютерной безопасности Санкт-Петербургского Федерального исследовательского центра Российской академии наук, ilya.bystrov@outlook.com

ВАСИЛЕЦ Павел Васильевич — студент группы ИКПИ-81 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, pahanjes.spb@gmail.com

ВАСЮТКИН Артем Васильевич — магистрант кафедры инфокоммуникационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, artemcoman98@mail.ru

ВЕРЕВКИН Сергей Александрович — аспирант Санкт-Петербургского Федерального исследовательского центра Российской академии наук»; младший научный сотрудник Военного института (научно-исследовательского) Академии А. Ф. Можайского, vrjovkin@rambler.ru

ВЕРШИНИНА Ксения Витальевна — студентка группы ИКТФ-06м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, xeniavershinina.v@gmail.com

ВЕСНИН Дмитрий Владимирович — студент кафедры безопасности информационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, qwertyforce2@gmail.com

ВИТКОВА Лидия Андреевна — кандидат технический наук, старший научный сотрудник лаборатории проблем компьютерной безопасности, ведущий специалист международного центра цифровой криминалистики Санкт-Петербургского Федерального исследовательского центра Российской академии наук; старший преподаватель Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, lidia@glorystory.ru

ВЛАДИМИРОВ Сергей Сергеевич — кандидат технических наук, доцент, доцент кафедры сетей связи и передача данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, vladimirov.opds@gmail.com

ВЛАСОВ Дмитрий Владимирович — магистрант кафедры инфокоммуникационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, dmitry.vlasov@fastmail.com

ВОЛКОВ Артем Николаевич — ассистент кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, artem.n@5glab.ru

ВОЛКОГОНОВ Владимир Никитич — кандидат технических наук, доцент, доцент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, vladimir.volkogonov@gmail.com

ВОЛОСТНЫХ Виктор Анатольевич — кандидат военных наук, доцент, научный сотрудник научно-исследовательского центра Военной орденов Жукова и Ленина Краснознаменная академии связи имени Маршала Советского Союза С. М. Буденного, ra1alo@mail.ru

ВОРОНЦОВ Андрей Анатольевич — студент группы ИКТЗ-84 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, vorontsov.andrey000@yandex.ru

ВОРОШНИН Григорий Евгеньевич — студент группы ИКТБ-18м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, voroshnin.g@yandex.ru

ВЬЮГОВ Станислав Георгиевич — сотрудник Академия Федеральной службы охраны Российской Федерации, senserk@icloud.com

ГАЙФУЛИНА Диана Альбертовна — аспирант, младший научный сотрудник лаборатории проблем компьютерной безопасности Санкт-Петербургского Федерального исследовательского центра Российской академии наук, gaifulina@comsec.sbp.ru

ГАМАНОВА Маргарита Алексеевна — аспирант кафедры радиоэлектронных систем Поволжского государственного университета телекоммуникаций и информатики, margo.ut@yandex.ru

ГАПОНЕНКО Владислав Александрович — студент группы ИБС-81 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, gapon70@gmail.com

ГЕРАСИМОВА Яна Александровна — студентка группы ИКТГ-14м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, gerasimova.jana2014@yandex.ru

ГЕРЛИНГ Екатерина Юрьевна — кандидат технических наук, доцент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, gerlingeu@gmail.com

ГЛАГОЛЕВ Сергей Федорович — кандидат технических наук, доцент, доцент кафедры фотоники и линий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, glagolevsf@yandex.ru

ГОЙХМАН Вадим Юрьевич — кандидат технических наук, доцент кафедры инфокоммуникационных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, vg@sotsbi.ru

ГОЛУБКИН Александр Анатольевич — магистрант Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, golubkin1998@mail.ru

ГОЛЫШКО Александр Викторович — кандидат технических наук, ведущий аналитик Департамента телекоммуникационных технологий АО «НПО РусБИТех», a.golyshko@rusbitech.ru

ГОРДЕЕВ Михаил Алексеевич — студент группы ИСТ-942 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, eugene@xfox111.net

ГРЕБЕНЩИКОВА Александра Андреевна — аспирант и ассистент кафедры инфокоммуникационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, sgreben1@mail.ru

ГРЕБЕШКОВ Александр Юрьевич — доктор технических наук, доцент, профессор кафедры сетей и систем связи Поволжского государственного университета телекоммуникаций и информатики, grebeshkov-ay@psuti.ru

ГУБАРЕВ Владимир Дмитриевич — студент группы ИБС-92 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича. dft4944@gmail.com

ГУМБАТОВ Рамиз Топуш оглы — доктор технических наук, профессор кафедры автоматика и электроэнергетике Бакинского инженерного университета, ramiz.humbatov@beu.edu.az

ГУРЕЕВ Владимир Олегович — аспирант кафедры линий связи и измерений в технике связи Поволжского государственного университета телекоммуникаций и информатики, v.gureev@psuti.ru

ГУТОВСКИЙ Алексей Сергеевич — магистр группы ИКТГ-04м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, lesha.gutovsky@yandex.ru

ДАГАЕВ Александр Владимирович — кандидат технических наук, доцент кафедры программной инженерии и вычислительной техники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, adagaev@list.ru

ДВОРЕЦКОВ Кирилл Алексеевич — студент группы ИКПИ-05 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, dvoreckovkirill@gmail.com

ДЖАВАДОВА Мирфатма Миртаги кызы — кандидат технических наук, доцент кафедры информатики и информационные безопасности Азербайджанского архитектурно-строительного университета, f.axadova@mail.ru

ДЖАФАРОВА Эльнаре Миртаги кызы — диссертант кафедры телекоммуникации и информационные безопасности Азербайджанского технического университета, elnara.axadova@mail.ru

ДМИТРИЕВ Евгений Владимирович — кандидат технических наук, заместитель директора филиала по общим вопросам, филиал ФГУП НИИР-СОНИИР (г. Самара), evgendm@yandex.ru

ДМИТРИЕВА Диана Сергеевна — студентка группы ИКТФ-16м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, dmitrievadiana1405@gmail.com

ДМИТРИЕВА Юлия Сергеевна — аспирант кафедры инфокоммуникационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, dmitrieva_spbgut@bk.ru

ДОКШИН Александр Денисович — студент группы ИКТЗ-01м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, a.dokshin007@gmail.com

ДОКШИНА Арина Викторовна — студентка группы ИКТЗ-01м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, arina_danshina1999@mail.ru

ДОЛГИРЕВА Елена Сергеевна — инженер удостоверяющего центра ЗАО «Защита электронных технологий», lenin91@mail.ru

ДОЛГОВ Евгений Петрович — кандидат технических наук, сотрудник кафедры безопасности сетевых технологий Академии Федеральной службы охраны Российской Федерации, dolevp@list.ru

ДОНСКОВ Евгений Андреевич — аспирант Санкт-Петербургского Федерального исследовательского центра Российской академии наук, radion2002@gmail.com

ДОЦЕНКО Сергей Эдуардович — инженер кафедры фотоники и линий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, 0472895@gmail.com

ДРЕПА Владислав Евгеньевич — студент группы ИКТЗ-83 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, vladikdrepa@mail.ru

ДУНАЙЦЕВ Роман Альбертович — кандидат технических наук, доцент, доцент кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, roman.dunaytsev@spbgut.ru

ЕДЕМСКАЯ Екатерина Дмитриевна — студентка группы ИКБ-82 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ekaterina.edemskaya51@gmail.com

ЕЛАГИН Василий Сергеевич — кандидат технических наук, доцент, доцент кафедры инфокоммуникационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, elagin.vas@gmail.com

ЕЛФИМОВ Александр Владимирович — магистрант группы ИКТЗ-11М Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, elwimoval@gmail.com

ЕРМОЛАЕВ Артур Анатольевич — студент группы ИКТФ-16м Санкт-Петербургского государственного университета телекоммуникаций им. Бонч-Бруевича, artur99ermolaev@gmail.com

ЕРМОЛЕНКО Даниил Владимирович — магистрант Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, daniil-ermolenko@mail.ru

ЕСАЛОВ Кирилл Эдуардович — начальник НОЦ «Инфокоммуникационных технологий и нейрокогнитивных архитектур» Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, kesalov@spbgut.ru

ЖЕРНОВА Ксения Николаевна — аспирант, младший научный сотрудник лаборатории проблем компьютерной безопасности Санкт-Петербургского Федерального исследовательского центра Российской академии наук, zhernova@comsec.spb.ru

ЗАЙЦЕВА Елена Сергеевна — Инженер кафедры линий связи и измерений в технике связи Поволжского государственного университета телекоммуникаций и информатики, zaytzewa@inbox.ru

ЗАРУБИН Антон Александрович — кандидат технических наук, доцент, заведующий кафедрой инфокоммуникационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, azarubin@sut.ru

ЗАХАРОВ Иван Вячеславович — аспирант кафедры «Электрическая связь» Петербургского государственного университета путей сообщения Императора Александра I, ведущий программист ЗАО «Институт телекоммуникаций», zakharov-ivan-v@yandex.ru

ЗЕБЗЕЕВ Егор Алексеевич — студент группы ИКТЗ-83 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, zebzeev.avis@gmail.com

ЗЕЛИЧЕНОК Игорь Юрьевич — аспирант, младший научный сотрудник Санкт-Петербургского Федерального исследовательского центра Российской академии наук, zelichenok@spb.comsec.ru

ЗЕМЦОВ Антон Александрович — студент группы ИКПИ-15 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, anton_ata@mail.ru

ЗИМИН Андрей Владимирович — старший преподаватель кафедры инфокоммуникационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, zimin@niits.ru

ЗРЕЛОВА Анастасия Леонидовна — студентка группы ИКТЗ-84 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, nastyzr@gmail.com

ИБРАГИМОВ Байрам Ганимат оглы — доктор технических наук, профессор кафедры телекоммуникации и информационных безопасности Азербайджанского технического университета, i.bayram@mail.ru

ИБРАГИМОВ Руфат Фикрет — диссертант Институт систем управления Национальной академии наук Азербайджана, i.rufat@mail.ru

ИГНАТОВА Ирина Олеговна — студентка группы ИКТИ-15м Санкт-Петербургского государственного университета им. проф. М. А. Бонч-Бруевича, ira-ignatova98@mail.ru

ИЗРАИЛОВ Константин Евгеньевич — кандидат технических наук, научный сотрудник лаборатория проблем компьютерной безопасности Санкт-Петербургского Федерального исследовательского центра Российской академии наук, izrailov@comsec.spb.ru

ИЛЬИН Артём Андреевич — рядовой, оператор научной роты Военной орденов Жукова и Ленина Краснознаменная академии связи имени Маршала Советского Союза С. М. Буденного, keisari357@gmail.com

ИСМАЙЛОВА Севиндж Рамиз кызы — кандидат технических наук, старший преподаватель кафедры информационных технологии и программирование Азербайджанского технического университета, sevinc_ism@hotmail.com

КАЗАКЕВИЧ Елена Владимировна — кандидат технических наук, доцент, заведующий кафедрой «Электрическая связь» Петербургского государственного университета путей сообщения Императора Александра I, kev-pgups@yandex.ru

КАЗАКОВ Никита Игоревич — студент группы ИКТБ-18м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, Kazakov.ni2.18@gmail.com

КАЗЕНКИН Александр Иванович — магистрант группы ПИм-11 Поволжского государственного университета и информатики, директор по развитию ООО «Сети. Системы. Сервис», o777kt@mail.ru

КАРЕЛЬСКИЙ Павел Владимирович — аспирант кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, pasha.karelscky@yandex.ru

КАТАСОНОВ Александр Игоревич — студент группы ИКТБ-07м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ksasha716@yandex.ru

КИЛИЧЕВА Клавдия Хайруллоевна — магистрант группы ИКТГ-04м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, bambosik@yandex.ru

КИРИЧЕК Руслан Валентинович — доктор технических наук, доцент, заведующий кафедрой программной инженерии и вычислительной техники Санкт-Петербургского государственного университета им. проф. М. А. Бонч-Бруевича, kirichek@sut.ru

КИРЬЯНОВ Александр Владимирович — кандидат технических наук, сотрудник кафедры безопасности сетевых технологий Академии Федеральной службы охраны Российской Федерации, alex1175@rambler.ru

КИСЛЯКОВ Сергей Викторович — кандидат технических наук, доцент кафедры инфокоммуникационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича; бизнес-аналитик НТЦ АРГУС s.v.kislyakov@gmail.com

КИСТРУГА Антон Юрьевич — аспирант кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, anton.kistruga@gmail.com

КИЧКО Яна Викторовна — адъюнкт кафедры автоматизированных систем специального назначения Военной орденов Жукова и Ленина Краснознаменная академии связи имени Маршала Советского Союза С. М. Буденного, kichkoyanka@mail.ru

КЛЮЕВ Дмитрий Сергеевич — доктор физико-математических наук, доцент, заведующий кафедрой радиоэлектронных систем Поволжского государственного университета телекоммуникаций и информатики, klyuevd@yandex.ru

КОВАЛЕВ Илья Алексеевич — студент группы ИКТБ-18м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, cov.cov.cov70@gmail.com

КОВАЛЕВ Игорь Станиславович — кандидат военных наук, доцент, доцент кафедры Военной орденов Жукова и Ленина Краснознаменная академии связи имени Маршала Советского Союза С. М. Буденного

КОВАЛЕНКО Вадим Николаевич — аспирант кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, kovalenkovadim1996@gmail.com

КОВЦУР Максим Михайлович — кандидат технических наук, доцент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, maxkovzur@mail.ru

КОЖАНОВ Юрий Федорович — кандидат технических наук, доцент кафедры инфокоммуникационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, juriy.kozhanov@mail.ru

КОЗЛОВ Сергей Викторович — кандидат технических наук, сотрудник Академии Федеральной службы охраны Российской Федерации, kozlov_sv@mail.ru

КОКОРЕВА Елена Викторовна — кандидат технических наук, доцент, доцент кафедры цифрового телерадиовещания и систем радиосвязи Сибирского государственного университета телекоммуникаций и информатики, elen.vik@gmail.com

КОЛОМЕЕЦ Максим Вадимович — младший научный сотрудник лаборатории проблем компьютерной безопасности Санкт-Петербургского Федерального исследовательского центра Российской академии наук, kolomeec@comsec.spb.ru

КОМАРОВ Иван Ильич — студент кафедры систем связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, komaroff.ivan@yandex.ru

КОНОВАЛОВА Виктория Вадимовна — студентка группы ИКТБ-17м, Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, konovalova.viktoriya.99@mail.ru

КОНОНОВ Павел Александрович — аспирант кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, kononov.pa@spbgut.ru

КОПТЕЛОВА Валентина Александровна — магистрант группы ИКТБ-07м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, koptelova.va@spbgut.ru

КОРЖИК Валерий Иванович — доктор технических наук, профессор, профессор кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, val-korzhik@yandex.ru

КОСОВ Никита Алексеевич — старший преподаватель кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, kosov.n.a@mail.ru

КОСТАНДЯН Эрик Геворгович — студент группы ИКБ-82 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, erikos2772@icloud.com

КОСТЮКОВИЧ Анатолий Егорович — кандидат технических наук, доцент кафедры инфокоммуникационных систем и сетей Сибирского государственного университета телекоммуникаций и информатики, aek1954@gmail.com

КОТЕНКО Игорь Витальевич — доктор технических наук, профессор, главный научный сотрудник лаборатории проблем компьютерной безопасности Санкт-Петербургского Федерального исследовательского центра Российской академии наук; профессор кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича ivkote@comsec.spb.ru

КРАСОВ Андрей Владимирович — кандидат технических наук, доцент, заведующий кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, krasov@inbox.ru

КРЕСТЬЯШИН Никита Антонович — студент группы ИКБ-82 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, kaktuz28@mail.ru

КРИВЕЦ Андрей Сергеевич — студент группы ИКТЗ-05 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, krivets_2002@mail.ru

КРОПОТОВА Ксения Алексеевна — магистрант кафедры радиоэлектронных и телекоммуникационных систем Казанского национального исследовательского технического университета имени А. Н. Туполева - КАИ, magistr@rambler.ru

КРЫЛОВ Алексей Вадимович — студент группы ИКТЗ-01м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, Krylov180497@yandex.ru

КУЗНЕЦОВ Станислав Александрович — студент группы ИКТЗ-01м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, staskonkurs12@mail.com

КУЗНЕЦОВ Константин Алексеевич — студент кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, kuznetsov.sut@gmail.com

КУЗНЕЦОВ Михаил Дмитриевич — аспирант кафедры информационные системы Санкт-Петербургского государственного электротехнического университета «ЛЭТИ» им. В.И. Ульянова (Ленина), mkuznetsov7991@gmail.com

КУЗЬМИНА Ольга Ивановна — студентка группы ИКТЗ-83 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, Olgakuzmina2000@mail.com

КУЛИКОВ Илья Александрович — студент группы ИКТЗ-01м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, wyzzus@gmail.com

КУЧЕРЯВЫЙ Андрей Евгеньевич — доктор технических наук, профессор, заведующий кафедрой Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, akouch@mail.ru

КУШНИР Дмитрий Викторович — кандидат технических наук, доцент, доцент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, dmitry.kushnir@gmail.com

ЛАНСЕРЕ Николай Николаевич — ассистент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, nlansere@yandex.ru

ЛАПИН Степан Павлович — адъюнкт кафедры безопасности инфокоммуникационных систем специального назначения Военной орденов Жукова и Ленина Краснознаменная академии связи имени Маршала Советского Союза С. М. Буденного, oleg-26stav@mail.ru

ЛЕБЕДЯНЦЕВ Валерий Васильевич — доктор технических наук, профессор, профессор кафедры инфокоммуникационных систем и сетей Сибирского государственного университета телекоммуникации и информатики, lebvv1951@mail.ru

ЛЕВШУН Дмитрий Сергеевич — кандидат технических наук, старший научный сотрудник лаборатории проблем компьютерной безопасности Санкт-Петербургский Федеральный исследовательский центр Российской академии наук, levshun@comsec.spb.ru

ЛЕПЕШКИН Олег Михайлович — доктор технических наук, доцент, профессор кафедры Института военно-технического образования и безопасности Санкт-Петербургского политехнического университета Петра Великого, lepechkin1@yandex.ru

ЛОБАСТОВА Мария Викторовна — кандидат технических наук, старший преподаватель кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, mlobastovabk1@rambler.ru

ЛОБАЧ Денис Антонович — студент кафедры систем связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, lo-de@mail.ru

ЛЫТКИНА Екатерина Александровна — студентка группы ИКТГ-14м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, kartoguru1998@mail.ru

МАЙОРОВ Виталий Вячеславович — студент группы ИКТС-03м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, vitmaj@mail.ru

МАКАР Мария Алексеевна — магистрант кафедры инфокоммуникационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, maria.elka@yandex.ru

МАКАРОВА Александра Дмитриевна — студентка группы ИКБ-04 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, madweb@lenta.ru

МАКАРОВА Александра Константиновна — бакалавр, студентка кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, alex-ecureuil@mai.ru

МАКСИМЕНКО Мария Эдуардовна — студентка группы ИКТЗ-05 Санкт-Петербургского государственного университета, mariyamaximenko@mail.ru

МАКСИМОВА Елена Игоревна — студентка группы РПБИ-81 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, littllest@yandex.ru

МАКУХА Артем Александрович — адъюнкт кафедры автоматизированных систем специального назначения Военной орденов Жукова и Ленина Краснознаменная академии связи имени Маршала Советского Союза С. М. Буденного, artem.makukha84@mail.ru

МАМЕДОВ Турал Гусейн оглы — адьюнкт Военной академии Вооруженных сил Республики Азербайджана, mamedov.t@gmail.com

МАНКАЕВ Расул Мурат-Алиевич — студент группы ИКТБ-07М Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, 24rasul1999@mail.ru

МАНУКЯН Агарон Андраникович — студент группы ИКТБ-08 Санкт-Петербургского государственного университета телекоммуникаций им. проф. Бонч-Бруевича, 03manukyan03@gmail.com

МАРТЫНЮК Анастасия Андреевна — студентка группы ИКПИ-05 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ans.martyn@gmail.com

МАТЮХИН Александр Юрьевич — кандидат технических наук, доцент кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета им. проф. М. А. Бонч-Бруевича, matukhin@list.ru

МЕЛЬНИК Максим Владимирович — магистрант группы ИКТБ-17м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, mkmxvh@gmail.com

МИНЕЕВ Назар Сергеевич — студент группы ИКПИ-83 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, сотрудник НОЦ ИКНС, mineevnazar@gmail.com

МИНЯЕВ Андрей Анатольевич — кандидат технических наук, старший преподаватель кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, minyaev.a@gmail.com

МИРОНОВ Кирилл Борисович — студент группы ИКПИ-05 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, mirokiro@mail.ru

МИХАЙЛИН Артём Денисович — курсант факультета многоканальных телекоммуникационных систем Военной орденов Жукова и Ленина Краснознаменная академии связи имени Маршала Советского Союза С. М. Буденного, cadetmix@icloud.com

МИХАЙЛИЧЕНКО Антон Валерьевич — адъюнкт кафедры автоматизированных систем специального назначения Военной орденов Жукова и Ленина Краснознаменная академии связи имени Маршала Советского Союза С. М. Буденного, antoxa9111603538@gmail.com

МИХАЙЛОВА Любовь Алексеевна — бакалавр, студентка кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, lubovami@mai.ru

МОЖГИНСКИЙ Виталий Львович — кандидат технических наук, доцент кафедры радиоэлектронных и телекоммуникационных систем Казанского национального исследовательского технического университета имени А.Н. Туполева - КАИ, 9047664058@ya.ru

МОРОЗОВ Иван Васильевич — преподаватель кафедры автоматизированных систем специального назначения Военной орденов Жукова и Ленина Краснознаменная академии связи имени Маршала Советского Союза С. М. Буденного, moroz_i.v@mail.ru

МУРАШКИН Никита Анатольевич — студент группы ИКПИ-95 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, niwhalea23@gmail.com

МУТХАННА Аммар Салех Али — кандидат технических наук, доцент кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ammarexpress@gmail.com

НАМАЗОВ Манафедин Бешир оглы — кандидат технических наук, доцент кафедры автоматика и электроэнергетике Бакинский инженерный университет, manaf1963@mail.ru

НЕЕЛОВА Ольга Леонидовна — старший преподаватель кафедры программной инженерии и вычислительной техники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, drutten@mail.ru

НИКИТИН Борис Константинович — кандидат технических наук, доцент кафедры фотоники и линий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича

НИКИТИН Александр Сергеевич — ведущий инженер-программист АО «НИИ «Рубин», a.s.nikitin@rubin-spb.ru

НИКИТИН Егор Денисович — студент группы ИКТИ-15м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, Yagor187@gmail.com

НИКОЛАЕВ Владимир Викторович — адъюнкт кафедры автоматизированных систем специального назначения Военной орденов Жукова и Ленина Краснознаменная академии связи имени Маршала Советского Союза С. М. Буденного, fortune-rus@yandex.ru

НИКОЛАЕНКО Анастасия Олеговна — студентка группы ИКТФ-06м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, nastena.nikolaenko.98@mail.ru

НИКОНОВ Евгений Русланович — студент группы ИКБ-83 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, NIKKSTUDIO3023@gmail.com

НОВИКОВА Евгения Сергеевна — кандидат технических наук, доцент, старший научный сотрудник лаборатории проблем компьютерной безопасности Санкт-Петербургского Федерального исследовательского центра Российской академии наук; доцент кафедры информационных систем Санкт-Петербургского государственного электротехнического университета «ЛЭТИ» им. В.И. Ульянова (Ленина), novikova@comsec.spb.ru

ОБУХОВ Станислав Андреевич — студент группы ИКТС-71 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, stasstas1155@yandex.ru

ОГОРЕЛЬЦЕВ Павел Анатольевич — студент группы ИКБ-95 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, paul.ogorelcev@gmail.com

ОКУНЕВА Дарина Владимировна — кандидат технических наук, декан факультета инфокоммуникационных сетей и систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, darina_okuneva@mail.ru

ОЛЕНИЧЕВ Владислав Витальевич — студент кафедры систем связи и передачи данных Санкт-Петербургского государственного университета Телекоммуникаций им. проф. М. А. Бонч-Бруевича, vladislavolenicev@gmail.com

ОРЛОВ Григорий Александрович — студент группы ИКТБ-07м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, grigory.a.orlovg@gmail.com

ОРЛОВ Дмитрий Андреевич — студент группы ИКТБ-08м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, orlovsut62@gmail.com

ОРУДЖОВА Милана Ягуб кызы — кандидат технических наук, старший преподаватель кафедры информационных технологии и программирование Азербайджанского технического университета, o.milana@gmail.com

ОСЕТРИН Алексей Сергеевич — студент Академии Федеральной службы охраны Российской Федерации, osetrin.al@yandex.ru

ОСТРОУМОВ Олег Александрович — кандидат технических наук, докторант Военной орденов Жукова и Ленина Краснознаменная академии связи имени Маршала Советского Союза С. М. Буденного, oleg-26stav@mail.ru

ПАВЛОВ Иван Иванович — кандидат технических наук, доцент, заведующий кафедрой систем автоматизированного проектирования, доцент кафедры радиотехнических устройств и техносферной безопасности Сибирского государственного университета телекоммуникации и информатики, академик МАС iipavlov02@mail.ru

ПАВЛОВА Мария Сергеевна — старший преподаватель кафедры радиотехнических устройств и техносферной безопасности Сибирского государственного университета телекоммуникации и информатики, mspavlova@ngs.ru

ПАК Виолетта Олеговна — студентка группы ИКТФ-06м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, violetta_tdk@mail.ru

ПАНТЮХИН Олег Игоревич — кандидат технических наук, доцент, доцент кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, p_oleg99@mail.ru

ПАНЧЕНКО Анастасия Александровна — студентка группы ИКПИ-81 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, panchenkofff@gmail.com

ПАРАЩУК Игорь Борисович — доктор технических наук, профессор, Заслуженный изобретатель РФ, профессор кафедры автоматизированных систем специального назначения Военной орденов Жукова и Ленина Краснознаменная академии связи имени Маршала Советского Союза С. М. Буденного, shchuk@rambler.ru

ПАРШИН Евгений Александрович — студент группы ИКТБ-18м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, jpnvk@yandex.ru

ПАХОМОВ Михаил Сергеевич — студент группы ИКТЗ-83 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, mpakhomov99@gmail.com

ПАШИН Станислав Сергеевич — заместитель директора (руководитель бизнес-инкубатора) Центра стратегических инициатив, Поволжский государственный университет телекоммуникаций и информатики (г. Самара), pashinstanislav@outlook.com

ПАЩЕНКО Василий Владимирович — кандидат технических наук, доцент кафедры Военной орденов Жукова и Ленина Краснознаменная академии связи имени Маршала Советского Союза С. М. Буденного, vvpah@mail.ru

ПЕРМЯКОВ Александр Сергеевич — адъюнкт Военной орденов Жукова и Ленина Краснознаменная академии связи имени Маршала Советского Союза С. М. Буденного, sensemile.nic@mail.ru

ПЕСИН Артем Евгеньевич — студент группы ИБС-03 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, lichilich79@gmail.com

ПЕСТОВ Игорь Евгеньевич — старший преподаватель кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, pestovie@outlook.com

ПЕТРОВ Максим Павлович — студент группы ИБС-81 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, for_institute2018@mail.ru

ПЕТРОВА Татьяна Васильевна — студентка группы ИКТЗ-83 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, tanya26012001@mail.com

ПИЛИПОВА Валерия Михайловна — студентка группы ИКТФ-16м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, valeriiapilipova@gmail.com

ПИРМАГОМЕДОВ Рустам Ярахмедович — Ph.D., кандидат технических наук, научный сотрудник Университета Тампере, rustam.pirmagomedov@gmail.com

ПОЛЯКОВА Елена Валерьевна — старший преподаватель кафедры фотоники и линий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, e.v@inbox.ru

ПОЛЯНИЧЕВА Анна Валерьевна — аспирант, ассистент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, polavaly@gmail.com

ПОМОГАЛОВА Альбина Владимировна — ассистент, заместитель заведующего кафедрой по научной работе кафедры программной инженерии и вычислительной техники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, a.l.b.i.n.a@bk.ru

ПОРУЧИКОВ Александр Алексеевич — курсант факультета многоканальных телекоммуникационных систем Военной орденов Жукова и Ленина Краснознаменная академии связи имени Маршала Советского Союза С. М. Буденного, 357.lumi@gmail.com

ПРОШИН Федор Алексеевич — аспирант кафедры «Электрическая связь» Петербургского государственного университета путей сообщения Императора Александра I, fedorproshin@gmail.com

ПУЧКОВ Владимир Викторович — младший научный сотрудник, аспирант лаборатории проблем компьютерной безопасности Санкт-Петербургского Федерального исследовательского центра Российской академии наук, puchkov-81@bk.ru

РАФАЛЬСКАЯ Маргарита Игоревна — адъюнкт кафедры 22 «Сетей связи и систем коммутации» Военной орденов Жукова и Ленина Краснознаменная академии связи имени Маршала Советского Союза С. М. Буденного, margo-23@bk.ru

РЕВЕНКО Юлия Павловна — магистрант кафедры инфокоммуникационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, revenko2018j@gmail.com

РЕДРУГИНА Наталия Михайловна — ассистент кафедры инфокоммуникационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, redrugina.nm@spbgut.ru

РЕЗНИКОВ Богдан Константинович — преподаватель кафедры фотоники и линий связи, преподаватель кафедры программной инженерии и вычислительной техники, преподаватель базовой кафедры «Специальные средства связи» Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, rznkff@gmail.com

РЕМДЕНОК Павел Александрович — студент группы ИКПИ-15 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, itztoru@vk.com

РОЖКОВ Максим Александрович — аспирант кафедры программной инженерии и вычислительной техники Санкт-Петербургского государственного политехнического университета, monolittiran@gmail.com

РУСАКОВ Артём Андреевич — Студент группы ИКТК-85 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, fig753@gmail.com

САВЕЛЬЕВА Анастасия Андреевна — старший преподаватель кафедры инфокоммуникационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, saa@spbgut.ru

САЕНКО Игорь Борисович — доктор технических наук, профессор, профессор кафедры автоматизированных систем специального назначения Военной орденов Жукова и Ленина Краснознаменная академии связи имени Маршала Советского Союза С. М. Буденного; ведущий научный сотрудник лаборатории проблем компьютерной безопасности Санкт-Петербургского Федерального исследовательского центра Российской академии наук, ibsaen@mail.ru

САЛИТА Андрей Сергеевич — студент группы ИКТБ-18м, Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, salita@internet.ru

САЛМАН Васан Давуд — аспирантка кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, wasan.salman@mail.ru

САЛТЫКОВ Антон Радиевич — старший преподаватель кафедры фотоники и линий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, anton.saltykov@gmail.com

САМАТОВА Карина Алексеевна — бакалавр, студентка кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, karinasamatova1@gmail.com

САХАРОВ Дмитрий Владимирович — кандидат технических наук, доцент, доцент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. Проф. М.А. Бонч-Бруевича, sguard7@mail.ru

САХАРОВА Мария Александровна — кандидат технических наук, доцент кафедры «Электрическая связь» Петербургского государственного университета путей сообщения Императора Александра I (ПГУПС), начальник отдела разработки систем связи ЗАО «Институт телекоммуникаций», zuvakamariya@mail.ru

САЯРКИН Виталий Андреевич — курсант Военной орденов Жукова и Ленина Краснознаменная академии связи имени Маршала Советского Союза С. М. Буденного, vitaliysayarkin@gmail.com

СВЕТОВА Анастасия Васильевна — студент группы ИКТУ-98 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, nastya_sv00@mail.ru

СЕРГЕЕВ Алексей Николаевич — старший преподаватель кафедры фотоники и линий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, a32@bk.ru

СИНЮК Александр Демьянович — доктор технических наук, доцент, профессор кафедры общепрофессиональных дисциплин Военной орденов Жукова и Ленина Краснознаменная академии связи имени Маршала Советского Союза С. М. Буденного, eentrop@rambler.ru

СКРОБОВ Даниил Витальевич — студент группы ИКТИ-15м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, dany-1999@yandex.ru

СМИРНОВ Иван Юрьевич — адъюнкт Военной орденов Жукова и Ленина Краснознаменная академии связи имени Маршала Советского Союза С. М. Буденного, sensemile.nic@mail.ru

СОКОЛОВ Георгий Юрьевич — студент группы ИКФ-81 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, greenfire1549@gmail.com

СОСУНОВ Даниил Вячеславович — студент кафедры линий связи и измерений в технике связи Поволжского государственного университета телекоммуникаций и информатики, sosunovdaniil05@gmail.com

СПИРКИНА Анастасия Валентиновна — аспирантка кафедры инфокоммуникационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, spirkina.av@spbgut.ru

СТЕПАНЕНКОВ Григорий Викторович — студент группы ИКТФ-16м; техник кафедры программной инженерии и вычислительной техники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, 261199g@gmail.com

ТАГАНДУРДЫЕВ Нурмурад — студент группы ИКТМ-02м кафедры инфокоммуникационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, nuriktagan@gmail.com

ТАРАБАНОВ Илья Федорович — студент группы ИКТМ-12м, инженер НОЦ "Программно-определяемые системы" Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, tarabanov.ilya@yandex.ru

ТАРАСОВ Александр Алексеевич — адъюнкт кафедры общепрофессиональных дисциплин Военной орденов Жукова и Ленина Краснознаменная академии связи имени Маршала Советского Союза С. М. Буденного, taras4912@mail.ru

ТАХИРОВА Конул Мобил кызы — адъюнкт Военной Академии Вооруженных Сил Азербайджанской Республики, konul_tahirova@yahoo.com

ТОРОПЦЕВ Антон Юрьевич — студент Академии Федеральной службы охраны Российской Федерации, toroptsev.an@gmail.com

УДАЛЬЦОВ Александр Владимирович — старший помощник начальника учебно-методического отдела Военной орденов Жукова и Ленина Краснознаменная академии связи имени Маршала Советского Союза С. М. Буденного, axil2003@yandex.ru

УРАГО Андрей Владимирович — бакалавр, студент группы ИСТ-031м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, Andrey.urago@gmail.com

УШАКОВ Кирилл Алексеевич — студент группы ПИ-91 Поволжского государственного университета и информатики, kirill_ushakov@internet.ru

УШАКОВ Игорь Александрович — кандидат технических наук, доцент кафедры защищенные системы и сети связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ushakovia@gmail.com

ФАДЕЕВ Илья Игоревич — ассистент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, collapsefrustration@gmail.com

ФЕДОРОВА Злата Анатольевна — студентка группы ИКТЗ-84 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, zf_sweetday@mail.ru

ФЁДОРОВА Анастасия Эдуардовна — студентка группы ИКТЗ-11м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, fyodorova.aaee@gmail.com

ФЁДОРОВА Ольга Вячеславовна — студентка группы ИКТБ-18м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, olgafedorova666@gmail.com

ФЕДОРЧЕНКО Елена Владимировна — кандидат технических наук, старший научный сотрудник лаборатории проблем компьютерной безопасности Санкт-Петербургского Федерального исследовательского центра Российской академии наук; доцент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, doynikova@comsec.spb.ru

ФИЛИН Егор Дмитриевич — аспирант кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, filin.ed@mail.ru

ФОМИН Владимир Владимирович — доктор технических наук, профессор кафедры программной инженерии и вычислительной техники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича; профессор кафедры информационно-сетевых технологий Санкт-Петербургского государственного университета аэрокосмического приборостроения, v_v_fomin@mail.ru

ФОМИН Артем Игоревич — магистр группы ИКТГ-04м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, artem.fomin633@gmail.com

ФОМИНЫХ Артур Андреевич — студент группы ИКТЗ-01м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, fominykhartur@yandex.ru

ФРАЗ Алексей Вячеславович — студент группы ИКТФ-06м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, frazalex@yandex.ru

ФРОЛОВ Алексей Олегович — аспирант кафедры радиоэлектронных систем Поволжского государственного университета телекоммуникаций и информатики, frolov_alex_1@mail.ru

ФРОЛОВА Александра Сергеевна — студентка группы ИКТФ-06м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, alexandravasileva1@mail.ru

ХИТРОВ Павел Алексеевич — студент группы ИКТО-81 Санкт-Петербургского государственного университета телекоммуникаций им. Бонч-Бруевича, pasha2000976@gmail.com

ХМЫРОВ Семен Сергеевич — аспирант лаборатории проблем компьютерной безопасности Санкт-Петербургского Федерального исследовательского центра Российской академии наук, khmyrov.s.s@gmail.com

ХРИСТОФОРОВ Роман Олегович — техник НОЦ «Программно-определяемых систем» Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, romanleonhristoforov@gmail.com

ЦВЕТКОВ Александр Юрьевич — старший преподаватель кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, alexander.tsvetkov89@gmail.com

ЧЕРКАСОВА Анастасия Николаевна — студентка группы ИКТИ-15м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевич, nari_5@mail.ru

ЧЕРНЫХ Илья Сергеевич — начальник отделения кафедры «Безопасности инфокоммуникационных систем специального назначения» Военной орденов Жукова и Ленина Краснознаменная академии связи имени Маршала Советского Союза С. М. Буденного, oleg-26stav@mail.ru

ЧЕЧУЛИН Андрей Алексеевич — кандидат технический наук, доцент, доцент защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича; ведущий научный сотрудник лаборатории проблем компьютерной безопасности, руководитель международного центра цифровой криминалистики Санкт-Петербургского Федерального исследовательского центра Российской академии наук, chechulin@comsec.spb.ru

ШАБАН Ольга Валерьевна — аспирантка кафедры линий связи и измерений в технике связи Поволжского государственного университета телекоммуникаций и информатики, o.shaban@psuti.ru

ШАБАНОВ Владислав Павлович — студент группы ИБС-81 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, shabanovvladislav2000@gmail.com

ШАРЛАЕВА Мария Владимировна — ассистент кафедры программной инженерии и вычислительной техники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, masha110.97@mail.ru

ШВИДКИЙ Артем Александрович — ассистент кафедры инфокоммуникационных систем, начальник научно-образовательного центра «Программно-определяемых систем» Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, shvidkiy@sut.ru

ШЕМЯКИН Сергей Николаевич — кандидат технических наук, доцент, кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, s4421764@yandex.ru

ШЕСТАКОВ Александр Викторович — доктор технических наук, старший научный сотрудник, проректор по научной работе Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, shestakov.av@spbgut.ru

ШИШКИН Артём Андреевич — курсант факультета радиосвязи Военной орденов Жукова и Ленина Краснознаменная академии связи имени Маршала Советского Союза С. М. Буденного, Glebom@mail.ru

ШТЕРЕНБЕРГ Игорь Григорьевич — кандидат педагогических наук, сотрудник Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, shterenberg@yandex.ru

ШУРЫГИНА Ксения Игоревна — студент магистратуры, лаборант кафедры цифрового телерадиовещания и систем радиосвязи Сибирского государственного университета телекоммуникаций и информатики, miraclele@yandex.ru

ЮДИНА Елизавета Александровна — студентка группы ИКФ-81 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, udinchita@mail.ru

ЮРКИН Дмитрий Валерьевич — кандидат технических наук, доцент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, dvyurkin@ya.ru

ЮРЬЕВ Глеб Игоревич — аспирант кафедры инфокоммуникационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, me@vicis.ru

ЯКОВЛЕВ Николай Викторович — студент группы ИКТФ-16м Санкт-Петербургского государственного университета телекоммуникаций им. Бонч-Бруевича, yakovlev.nv_spbopen@mail.ru

ЯКОВЛЕВ Виктор Алексеевич — доктор технических наук, профессор кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, viyak@bk.ru

ЯКУБОВА Ольга Алексеевна — студент группы ИКПИ-14 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, y.o.a@yandex.ru

АВТОРСКИЙ УКАЗАТЕЛЬ

СПбГУТ)))

Санкт-Петербургский государственный университет
телекоммуникаций им. проф. М. А. Бонч-Бруевича