VII

МЕЖДУНАРОДНАЯ НАУЧНО-ТЕХНИЧЕСКАЯ И НАУЧНО-МЕТОДИЧЕСКАЯ КОНФЕРЕНЦИЯ

▪ АКТУАЛЬНЫЕ ПРОБЛЕМЫ ИНФОТЕЛЕКОММУНИКАЦИЙ В НАУКЕ И ОБРАЗОВАНИИ ▪

СБОРНИК НАУЧНЫХ СТАТЕЙ

2018

УДК 001:061.3(082)
ББК 72 А43

Актуальные проблемы инфотелекоммуникаций в науке и образовании. VII Международная научно-техническая и научно-методическая конференция; сб. науч. ст. в 4 т. / Под. ред. С. В. Бачевского; сост. А. Г. Владыко, Е. А. Аникевич. СПб. : СПбГУТ, 2018. Т. 1. 727 с.

ГЕНЕРАЛЬНЫЙ СПОНСОР

СПОНСОРЫ КОНФЕРЕНЦИИ

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.

ISBN 978-5-89160-167-3

ИНФОРМАЦИОННАЯ ПОДДЕРЖКА

COMNEWS

НАУЧНО-ТЕХНИЧЕСКИЙ ЖУРНАЛ ИНФОРМАЦИЯ КОСМОС

linkmeup
первый подкаст для связистов

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ
научное рецензируемое издание • электронный научный журнал
Telecom IT — ISSN 2307-1303

НАУЧНЫЙ ЖУРНАЛ
ТУЗ
«ТРУДЫ УЧЕБНЫХ ЗАВЕДЕНИЙ СВЯЗИ»

Научное издание
Литературное редактирование,
корректура Е. А. Аникевич
Оформление Д. В. Ушаков
Верстка Е. М. Аникевич
Подписано в печать 30.05.2018.
Вышло в свет 30.06.2018. Формат 60×90 1/8.
Уст. печ. л. 45,44. Заказ № 042-ИТТ-2018.
пр. Большевиков, д. 22, корп. 1.
Россия, Санкт-Петербург, 193232

СОДЕРЖАНИЕ

УДК 654.926

ОПЫТ ПОСТРОЕНИЯ СИСТЕМЫ МОНИТОРИНГА КАБЕЛЬНОЙ ИНФРАСТРУКТУРЫ С ИСПОЛЬЗОВАНИЕМ ОПТОВОЛОКОННОГО АКУСТИЧЕСКОГО СЕНСОРА «ДУНАЙ»

В. Г. Леденев

ООО «Т8»

Технология обнаружения виброакустических воздействий с использованием распределенных оптоволоконных сенсоров находит все большее применение в различных областях промышленности благодаря как ряду преимуществ, присущих самой технологии, так и разработке целого ряда специализированных программных приложений. В частности, на базе данной технологии может быть развернута система мониторинга такого ценного инфраструктурного ресурса, как кабельная канализация.

распределенный оптоволоконный сенсор, обнаружение виброакустических воздействий, оптическая платформа «Дунай», ООО «Т8», когерентный рефлектометр, мониторинг кабельной инфраструктуры, контроль доступа.

Технология обнаружения виброакустических воздействий с использованием распределенных оптоволоконных сенсоров (DAS – *Distributed Acoustic Sensor*) имеет богатую историю применения в различных областях промышленности. В первую очередь там, где существует необходимость обнаружения активности внутри и вблизи объектов линейной топологии, таких как: охранные зоны трубопроводов, протяженные охраняемые периметры и т. п.

В основе технологии лежит анализ рассеяния, образующегося на внутренних неоднородностях оптического волокна. Источником падающего излучения является когерентный лазер, испускающий в оптическое волокно короткие сканирующие импульсы. Оптическое волокно выступает в роли распределенного чувствительного элемента. Подробнее о принципах работы оптоволоконных сенсоров можно прочитать в работах [1, 2, 3].

Общими преимуществами технологии являются:

– возможность использования в качестве чувствительного элемента оптических волокон (ОВ) из состава существующих волоконно-оптических кабелей (ВОК);

– полностью пассивный распределенный чувствительный элемент без необходимости установки оборудования на дальнем конце линии;

– значительная протяженность участка мониторинга (десятки километров).

Сочетание этих преимуществ с развитием специализированного программного обеспечения привело к расширению спектра возможных применений.

В частности, появилась идея создания системы мониторинга кабельной инфраструктуры. Фактически, речь идет об осуществлении контроля доступа в колодцы кабельной канализации с использованием в качестве чувствительного элемента ОВ из состава ВОК, проложенных через данные колодцы.

Актуальность задачи очевидна. Кабельная канализация является ценным инфраструктурным ресурсом. С одной стороны, владелец кабельной канализации несет риски ее несанкционированного использования для прокладки кабелей, а также хищений и вандализма. С другой стороны, существует потребность в осуществлении контроля над проведением плановых работ линейными бригадами (определение времени начала и окончания, соответствия места проведения работ выданному заданию).

Компания «Т8» предложила техническое решение по построению системы мониторинга с использованием оптоволоконного акустического сенсора «Дунай» собственного производства. Помимо аппаратной платформы применено специализированное программное обеспечение распознавания и отображения событий, разработанное специалистами компании.

На этапе постановки задачи стало ясно, что интерес для владельца кабельной канализации представляет не только обнаружение факта проникновения в колодец, но и распознавание отдельных стадий, а именно: воздействие на крышку люка колодца, собственно проникновение, воздействие на кабель, протяжка кабеля между колодцами.

Эта задача представляется решаемой уже потому, что, как показано на рис. 1–2 ниже, даже визуальные представления различных воздействий в окне «Водопад» [1] отличаются между собой. Тем более, возможно распознавание воздействий с помощью искусственной нейронной сети. Окно «Водопад» служит вспомогательным средством для оператора дежурной службы.

Очевидно, что степени критичности отдельных стадий проникновения отличаются. Воздействия на крышку люка могут быть в большей степени вызваны случайным воздействием и не говорят о проникновении. Данным воздействиям, как предупреждающим сигналам, была присвоена категория опасности «Внимание». Все остальные стадии воздействия были объединены в категорию опасности «Тревога», как сигнализирующие о проникновении в колодец и требующие принятия оператором системы определенных

действий. Объединение отдельных стадий воздействия в категории опасности повысило точность распознавания и облегчило работу дежурной службе.

а) б) в)

Рис. 1. Визуальные представления следов различных воздействий:
а) три удара по крышке люка колодца; б) спуск лестницы в колодец;
в) воздействие на кабель (дернули 3 раза)

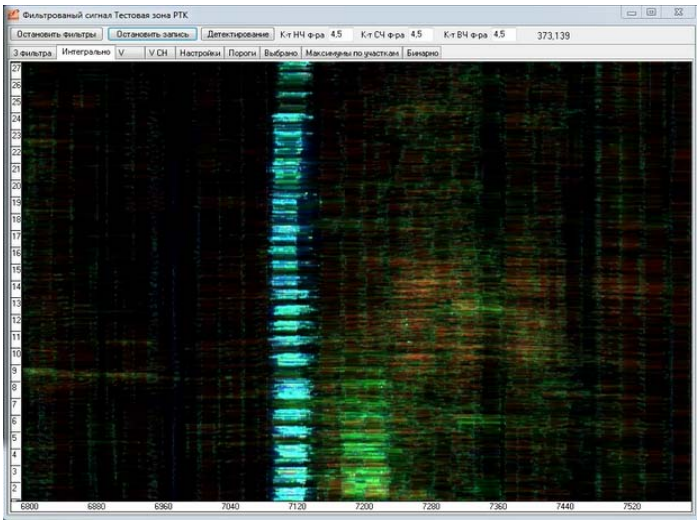


Рис. 2. Визуальное представление следа протяжки кондуктора между колодцами

Необходимыми элементами графического интерфейса оператора системы были признаны следующие:

– окно карты-схемы с обозначенной линией мониторинга;
– окно списка колодцев, охваченных мониторингом;
– окно таблицы активных событий;
– поле «Светофор», отображающее состояние линии в целом.

Пример главного окна графического интерфейса оператора дежурной смены представлен на рис. 3.

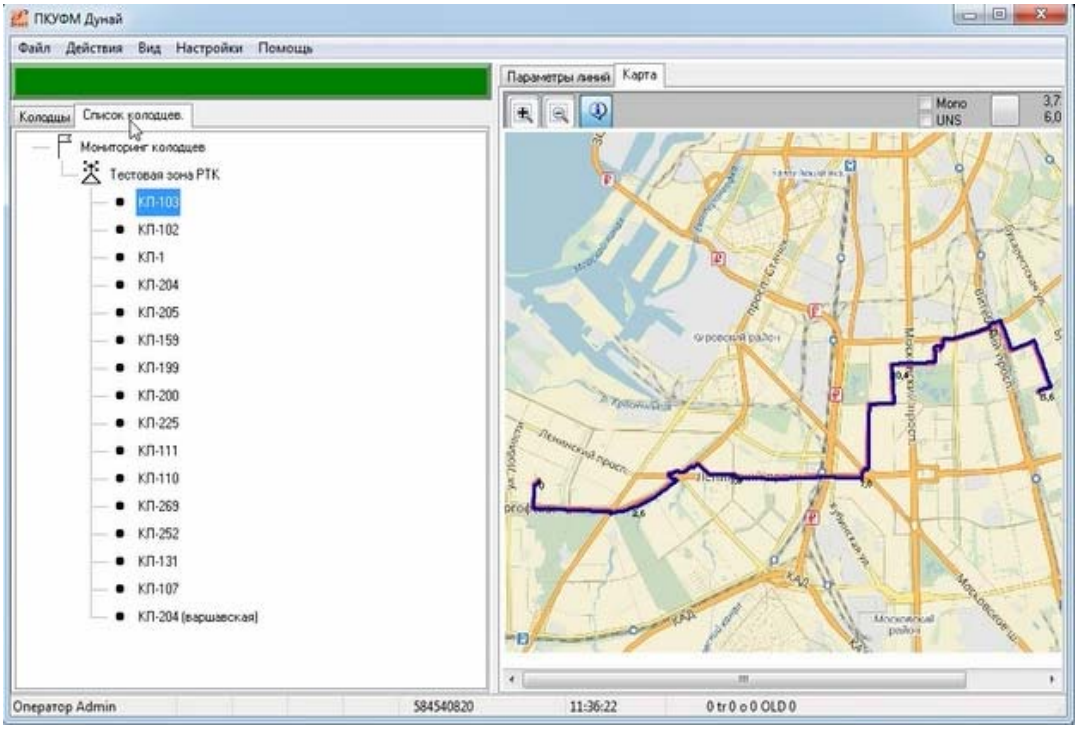


Рис. 3. Вид главного окна графического интерфейса оператора дежурной смены

При обнаружении проникновения в колодец система в автоматическом режиме обнаруживает воздействие, классифицирует его, присваивает ему одну из категорий опасности (Внимание или Тревога) и информирует оператора с помощью средств графического интерфейса:

– на карте-схеме отображается пиктограмма воздействия, окрашенная в цвет в соответствии с категорией опасности;
– такая же пиктограмма отображается в списке колодцев;
– информация о воздействии появляется в таблице активных событий;
– поле «Светофор» окрашивается в цвет, соответствующий категории опасности.

Виды главного окна при обнаружении воздействия категории «Тревога» представлена на рис. 4, 5.

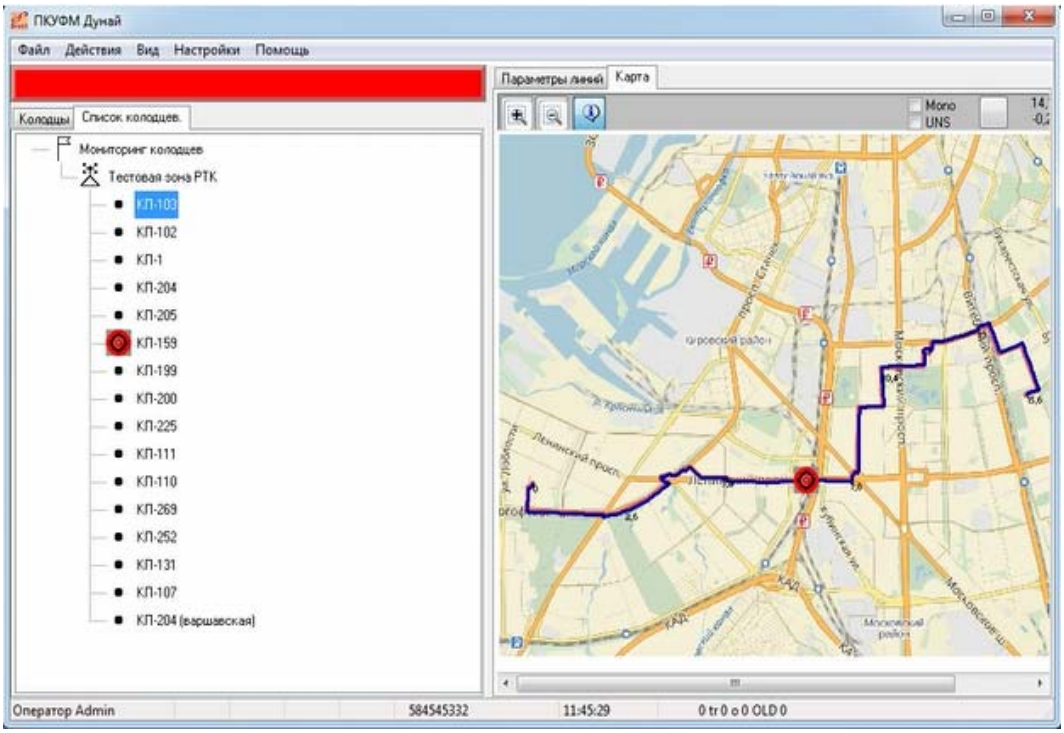


Рис. 4. Вид главного окна при обнаружении воздействия категории «Тревога» (карта-схема, список колодцев, поле «Светофор»)

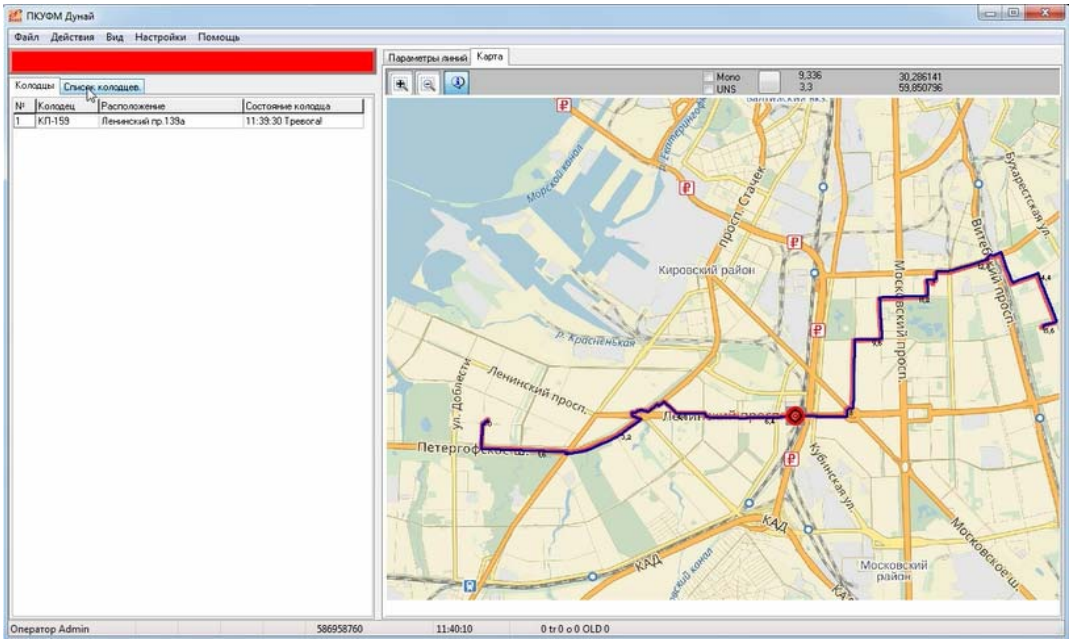


Рис. 5. Вид главного окна при обнаружении воздействия категории «Тревога» (карта-схема, таблица активных событий, поле «Светофор»)

Помимо элементов отображения информации о событии графический интерфейс предоставляет оператору дополнительные функциональные возможности, повышающие эффективность его работы.

В частности, оператору доступны следующие функции:

– реагирование на событие (обработка события);

– временный вывод колодца из режима мониторинга для проведения в нем плановых работ;

– отправка сообщения по электронной почте с информацией о событии и участком карты-схемы, на котором обнаружено воздействие;

– просмотр журналов (архивов) по обнаруженным воздействиям, действиям оператора и системным событиям (состояние аппаратного и программного обеспечения системы).

Система мониторинга кабельной инфраструктуры на основе оптоволоконного акустического сенсора «Дунай» позволяет владельцам кабельной канализации решать актуальную задачу по контролю доступа в колодцы кабельной канализации с целью предотвращения хищений кабеля, вандализма, несанкционированной прокладки кабеля, а также с целью контроля проведения плановых технических работ.

Специализированное программное обеспечение АРМ оператора дежурной смены обеспечивает отображение информации об обнаруженных воздействиях в графическом и табличном (текстовом) виде.

Дополнительные функциональные возможности обеспечивают обработку обнаруженных воздействий, информирование вышестоящих должностных лиц, контроль за действиями операторов и состоянием аппаратно-программных средств системы.

Представляется обоснованным утверждение, что в будущем количество используемых операторами связи ВОК будет расти. Ценность кабельной канализации, как ценного инфраструктурного ресурса, будет увеличиваться. Можно предположить, что системы мониторинга кабельной инфраструктуры, подобные рассмотренной в настоящей статье, будут востребованы на рынке. Развитие систем будет направлено, во-первых, в сторону повышения точности обнаружения и распознавания воздействий, а также в сторону интеграции с существующими у владельцев кабельной канализации системами инвентаризации технической инфраструктуры.

Список используемых источников

1. Горбуленко В. В., Леонов А. В., Марченко К. В., Трещиков В. Н. Волоконно-оптическая система мониторинга «Дунай» // Фотон-Экспресс. 2014. № 5 (117). С. 12–15.

2. Грознов Д. И., Леонов А. В., Наний О. Е., Нестеров Е. Т., Трещиков В. Н. «Дунай» – система мониторинга активности в охранной зоне трубопровода // Экспозиция. Нефть. Газ. 2014. № 4. С. 51–53.

3. Леонов А. В., Марченко К. В., Нестеров Е. Т., Трещиков В. Н. Волоконно-оптическая система мониторинга протяженных объектов (нефтепроводов) на основе когерентного рефлектометра // T-Comm: Телекоммуникации и транспорт. 2014. № 1. С. 25–28.

УДК 004.056

АНАЛИТИКА КИБЕРБЕЗОПАСНОСТИ: АНАЛИЗ СОВРЕМЕННОГО СОСТОЯНИЯ И ПЕРСПЕКТИВНЫЕ НАПРАВЛЕНИЯ ИССЛЕДОВАНИЙ

И. В. Котенко

Санкт-Петербургский институт информатики и автоматизации Российской академии наук

Анализируется проблема построения систем, реализующих расширенную аналитику безопасности. Характеризуется современное состояние исследований и разработок в области аналитики кибербезопасности. Представляются модели, методики, методы и средства для аналитики кибербезопасности. Намечаются перспективные направления исследований и разработок SIEM-систем. Рассматриваются собственные исследования в области разработки систем мониторинга безопасности и управления инцидентами.

кибербезопасность, мониторинг безопасности и управление инцидентами, аналитика кибербезопасности, реагирование на кибератаки, поведенческая аналитика пользователей и сущностей, анализ защищенности, выработка контрмер, большие данные, машинное обучение, распределенная и параллельная обработка данных, распределенный искусственный интеллект, визуальная аналитика.

В настоящее время мы являемся свидетелями активного противостояния между системами нападения и защиты в киберпространстве. Важными особенностями этого противостояния является: повышение уровня автоматизации, мощности, изощренности и масштабности этих систем; использование целевых атак; профессиональная разработка кибероружия и средств защиты, увеличение количества субъектов, осуществляющих его разработку.

Проблема повышения эффективности процессов сбора, обработки и анализа событий и информации кибербезопасности, в том числе идентификации текущей ситуации и формирования контрмер по защите информации в критических инфраструктурах является фундаментальной, междисциплинарной и значимой для Российской Федерации.

Защита информации в распределенных компьютерных сетях и системах, характерных для критически важных инфраструктур, должна базироваться на использовании развитых интеллектуальных сервисов киберзащиты, реализации технологий больших данных, машинного обучения и анализа поведения пользователей и приложений [1, 2, 3, 4].

Реализация методов, моделей и алгоритмов защиты информации, основанных на интеллектуальных сервисов киберзащиты указанных технологиях осуществляется через построение и функционирование систем аналитики безопасности или расширенной аналитики безопасности (*Advanced Security Analytics*), как важнейшего компонента системы защиты информации, реализующего аналитическую обработку информации кибербезопасности.

Термин расширенной аналитики подразумевает использование более развитых процедур анализа информации безопасности, в основном связанных с использованием технологий больших данных, машинного обучения, искусственного интеллекта и анализа поведения пользователей.

Направление исследований, связанных с аналитикой кибербезопасности в настоящее время испытывает бурный всплеск в различных областях деятельности. В таких программных документах и нормативно-правовых актах как «Доктрина информационной безопасности Российской Федерации», утвержденная Указом Президента Российской Федерации от 5 декабря 2016 г. № 646, Приказ Федеральной службы охраны Российской Федерации от 7 сентября 2016 г. № 443 «Об утверждении Положения о российском государственном сегменте информационно-телекоммуникационной сети «Интернет», рекомендациях в области стандартизации Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Предотвращение утечек информации» (РС БР ИББС-2.9-2016) и др., обосновывается необходимость применения технологий, связанных с аналитикой кибербезопасности, для критических инфраструктур.

Систему аналитики кибербезопасности можно воспринимать как интеллектуальную надстройку над системой управления информацией и событиями безопасности (*Security Information and Event Management*, SIEM) или системой мониторинга и управления инцидентами безопасности [5, 6, 7, 8, 9].

Основная цель SIEM-системы – повышение информационной безопасности за счет обеспечения возможности в режиме, близком к реальному времени, манипулировать информацией о безопасности и осуществлять проактивное управление инцидентами и событиями безопасности [6, 7]. «Проактивный» означает «действующий до того, как ситуация станет критической». Предполагается, что проактивное управление инцидентами и событиями безопасности основывается на автоматических механизмах, использующих информацию об «истории» анализируемых сетевых событий и прогнозе будущих событий, а также на автоматической подстройке параметров мониторинга событий к текущему состоянию защищаемой системы.

К информации, характеризующей события безопасности, относятся все данные об изменении состояния элементов защищаемой инфраструктуры,

формируемые программным или аппаратным способом, подлежащие хранению в электронном виде в специальных журналах в форме учетных записей (логов) или поступающие по каналам связи [5].

В системе управления информацией и событиями безопасности, включающей систему аналитики кибербезопасности, следует выделять три группы механизмов обработки событий безопасности [2]: механизмы сбора и преобразования исходной информации; механизмы хранения, поиска и выдачи информации по запросам; механизмы анализа информации и выработки решений.

В общем случае архитектура системы управления информацией и событиями безопасности имеет несколько уровней (рис. 1): уровень данных, уровень событий, прикладной уровень.

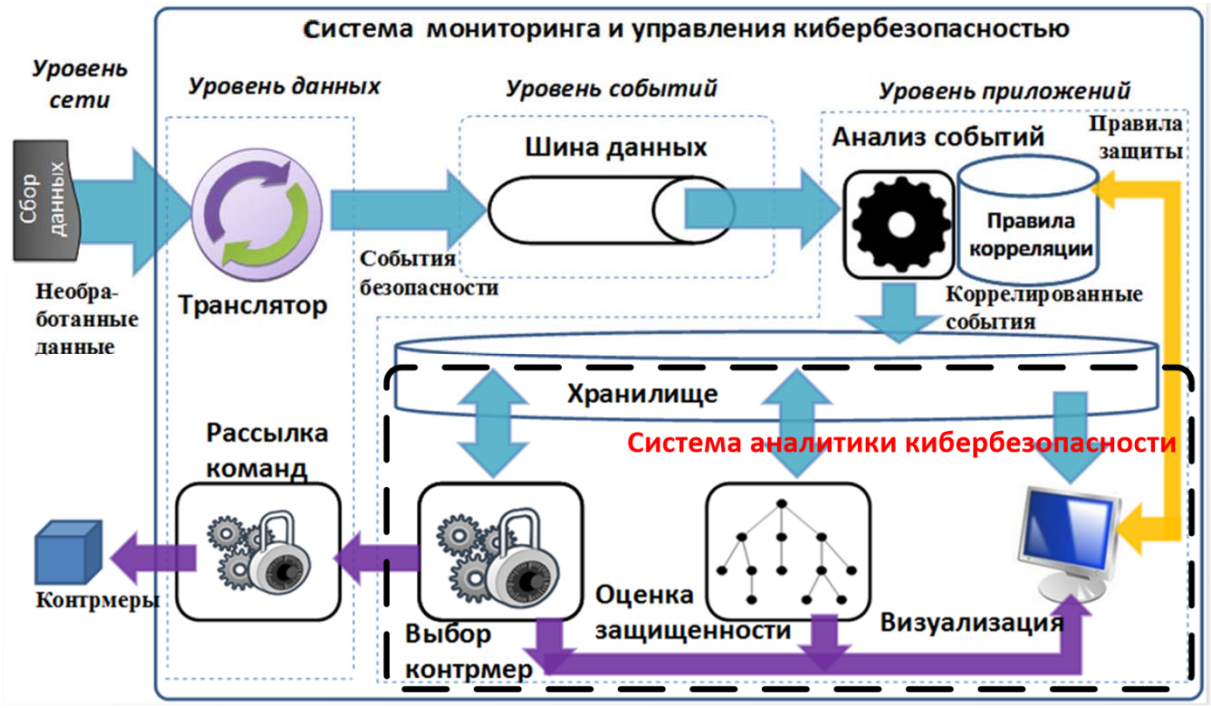


Рис. 1. Архитектура систем управления информацией и событиями безопасности и уровни обработки информации

На уровне данных осуществляется сбор данных о событиях безопасности, их обобщение, нормализация и предварительная корреляция.

Уровень событий отвечает за распространение информационных потоков событий безопасности между потребителями в реальном времени.

Прикладной уровень (уровень приложений) осуществляет обработку событий безопасности, моделирование, поддержку решений и реагирование, визуализацию, хранение событий в репозитории. Этот уровень и реализуется системой аналитики кибербезопасности.

Данные о событиях безопасности формируются на уровне защищаемой инфраструктуры, подлежат предварительной обработке на уровне данных, распространяются с помощью уровня событий к требуемым элементам прикладного уровня и, в конечном итоге, окончательно обрабатываются элементами этого последнего уровня.

Основные ограничения SIEM-систем – это ограничения по целевой инфраструктуре, неспособность многоуровневой интерпретации инцидентов и событий, неспособность обеспечить высокую степень надежности и стойкости среды сбора данных о событиях, низкая масштабируемость и др.

Функциональные требования к SIEM-системам нового поколения заключаются в применении проактивного управления инцидентами и событиями, формировании контрмер в реальном времени, интеллектуальности, высокой масштабируемости, многоуровневости и многодоменности обработки событий безопасности, а также надежном и устойчивом сборе данных о событиях и упреждающем управлении безопасностью.

Расширенный список задач, решаемых SIEM-системой, может быть представлен следующим образом: сбор, обработка и анализ событий безопасности, поступающих в систему из множества гетерогенных источников; анализ действий пользователей и приложений; обнаружение в реальном времени атак и нарушений критериев и политик безопасности; оценка защищенности информационных, телекоммуникационных и других критически важных ресурсов; профилирование и анализ поведения пользователей, отдельных сущностей и приложений; анализ и управление рисками информационной безопасности; проведение расследований инцидентов; обнаружение расхождения критически важных ресурсов и бизнес–процессов с внутренними политиками безопасности и приведение их в соответствие друг с другом; выработка и реализация решений по защите информации; формирование отчетных документов.

Новые возможности следующего поколения систем мониторинга и управления кибербезопасностью, основанные на расширенной аналитике кибербезопасности, предлагается сформулировать в виде следующего списка: межуровневая корреляция событий безопасности, поступающих из различных неоднородных источников; адаптивная масштабируемая обработка событий, обеспечивающая управление большими объемами данных о безопасности в реальном или близком к реальному времени; прогностический анализ безопасности, позволяющий осуществлять проактивное обнаружение и предотвращение атак путем принятия соответствующих контрмер за время, близкое к реальному; высокая доступность и отказоустойчивость сбора данных о событиях безопасности и доведения решений в условиях распределенности защищаемой инфраструктуры и активного вредоносного и/или непреднамеренного воздействия на каналы связи; выработка контрмер в реальном или близко к реальному времени; возможность

построения комплексных систем мониторинга и реагирования, как SOC, или подключения к «ФинЦЕРТ» Банка России или ГосСОПКА (в случае отечественных решений).

В настоящее время аспекты реализации расширенной аналитики для управления информацией и событиями безопасности активно исследуются и применяются множеством научных и коммерческих компаний по всему миру. В качестве наиболее известных мировых компаний, разрабатывающих продукты расширенной аналитики для идентификации ситуации по кибербезопасности и формирования контрмер, можно назвать: EMC (США), IBM (США), Splunk, AlienVault (Испания, США), Hewlett-Packard (США) и др. [10, 11, 12, 13, 14, 15, 16, 17]. Разрабатываются решения по расширенной аналитике и в российских SIEM-системах, в том числе Ankey SIEM (Газинформсервис), MaxPatrol SIEM (*Positive Technologies*), RuSIEM (РУСИЕМ, Сколково), КОМРАД (НПО «Эшелон») и других.

Одна из важнейших задач расширенной аналитики кибербезопасности связывается с реализацией поведенческой аналитики пользователей и сущностей защищаемой системы (*User and Entity Behavior Analytics*, UEBA), заключающейся в профилировании и выявлении аномалий в поведении пользователей, выполняемых процессов и компонентов. Алгоритмы обработки больших данных и машинного обучения (включая методы глубокого машинного обучения (*deep learning*), кластерного анализа, классификации данных, включая глубокие леса (*deep forest*), сиамские нейронные сети и др.) позволяют строить модели (профили, паттерны) поведения пользователей и компонентов системы и определять отклонения (аномалии) в поведении от этих моделей в реальном времени, как за короткий промежуток времени, так и с учетом предистории событий за длительный период (от одного месяца до года и более). Появился ряд продуктов UEBA таких компаний, как Splunk, IBM, HPE/MicroFocus, Balabit, Dtex, E8 Security, Exabeam, Forcepoint, Fortscale, Gurucul, Haystax Technology, HPE Niara, Interset, Microsoft, Palo Alto Networks, Preempt, RedOwl, Securonix и др. [12].

В качестве мировых научных конкурентов следует указать, в первую очередь, научные организации и университеты, ведущие исследования в области сбора, обработки и анализа данных для идентификации ситуации по кибербезопасности и формирования контрмер, например: Fraunhofer-SIT (Германия), Orange Labs – France Telecom (Франция), Télécom Sud-Paris (Франция).

В институте безопасных информационных технологий Fraunhofer SIT работает около 200 работников. Fraunhofer SIT [18] является одним из наиболее известных научно-исследовательских организаций в области компьютерной безопасности в Германии и Европе. Одним из направлений исследований данного института является анализ событий безопасности

на разных уровнях. Для этого в институте были разработаны модели обработки инцидентов безопасности, независимые от соответствующего уровня абстракции, представляющие собой концепцию моделирования событий. Данная концепция выражает подход к моделированию, поддерживающий многоуровневое управление инцидентами безопасности, основанное на потоках событий. Также в данном институте проходят тренинги по безопасности в области Больших данных (https://www.sit.fraunhofer.de/en/security4bigdata/).

Orange Labs – France Telecom (Франция). Orange Labs [19] представляет собой научно-исследовательское подразделение глобальной сети France Telecom-Orange Group. Данная организация тесно сотрудничает с научно-исследовательскими лабораториями по всему миру. Orange Labs включает 3600 исследователей в 17 лабораториях, расположенных на четырех континентах (8 во Франции и 9 в Европе, Америке, Африке и Азии). Лаборатория безопасности и доверенных транзакций (*Security and Trusted Transactions*, STT) центра разработки промежуточного программного обеспечения и сервисов продвинутых платформ (*Middleware and Advanced Platform Services*, MAPS) занимается безопасностью в различных областях облачных технологий, в том числе с применением расширенной аналитики кибербезопасности.

Télécom SudParis (Франция). Télécom SudParis [20] – ведущая инженерная магистерская школа, которая является частью Institut Telecom (IT) Института информационных и коммуникационных технологий (*Institute for Information and Communication Technology*) во Франции. Организация ведет разработку распределенных систем управления инцидентами, направленных на обнаружение вторжений, корреляцию предупреждений, управление информационной безопасностью и выработку контрмер.

Коллектив лаборатории проблем компьютерной безопасности Санкт-Петербургского института информатики и автоматизации Российской академии наук (СПИИРАН), возглавляемой автором настоящей статьи, активно участвует в создании научного задела для исследования и разработки систем мониторинга безопасности и управления инцидентами, основанных на технологиях расширенной аналитики безопасности, в частности программных платформ для параллельной распределенной обработки данных о событиях безопасности и системы сбора, хранения и обработки информации и событий безопасности на основе средств Elastic Stack, Hadoop и Spark [21, 22, 23], моделирования атак, анализа уязвимостей, визуальной аналитики и реагирования на атаки [24, 25, 26].

Особенности предлагаемых решений состоят в следующем:

1) использование интегрированного репозитория безопасности (содержащего данные о конфигурации системы, моделях нарушителя, уязвимостях, атаках, оценках, контрмерах и др.);

2) реализация эффективных методик генерации графов атак и зависимостей сервисов, базирующихся на методиках топологического анализа уязвимостей (TVA), которые формируют потенциальные последовательности использования уязвимостей для построения графов атак;

3) учет как известных, так и новых атак, основанных на уязвимостях 0-го дня;

4) применение anytime-алгоритмов для обеспечения близкого к реальному времени генерации подграфов атак и процедур анализа защищенности (*anytime*-алгоритм – итерационный вычислительный алгоритм, который способен выдать наилучшее на данный момент решение);

5) комбинированное использование графов атак и графов зависимостей сервисов;

6) вычисление комплекса разнообразных показателей защищенности, включая показатели уровня защищенности, уровня воздействия и потенциала атаки, уровня навыков нарушителя, эффективности контрмер, степени побочных потерь при реализации контрмер и др.;

7) стохастическое аналитическое моделирование и интерактивная поддержка принятия решений для выбора предпочтительных решений по безопасности на основе определения предпочтений относительно различных типов целей и требований (рисков, стоимости, выигрыша) и установления компромиссов между высокоуровневыми целями защиты информации

Предложенный подход позволяет для разработки графических элементов использовать различные технологии визуализации (рис. 2).

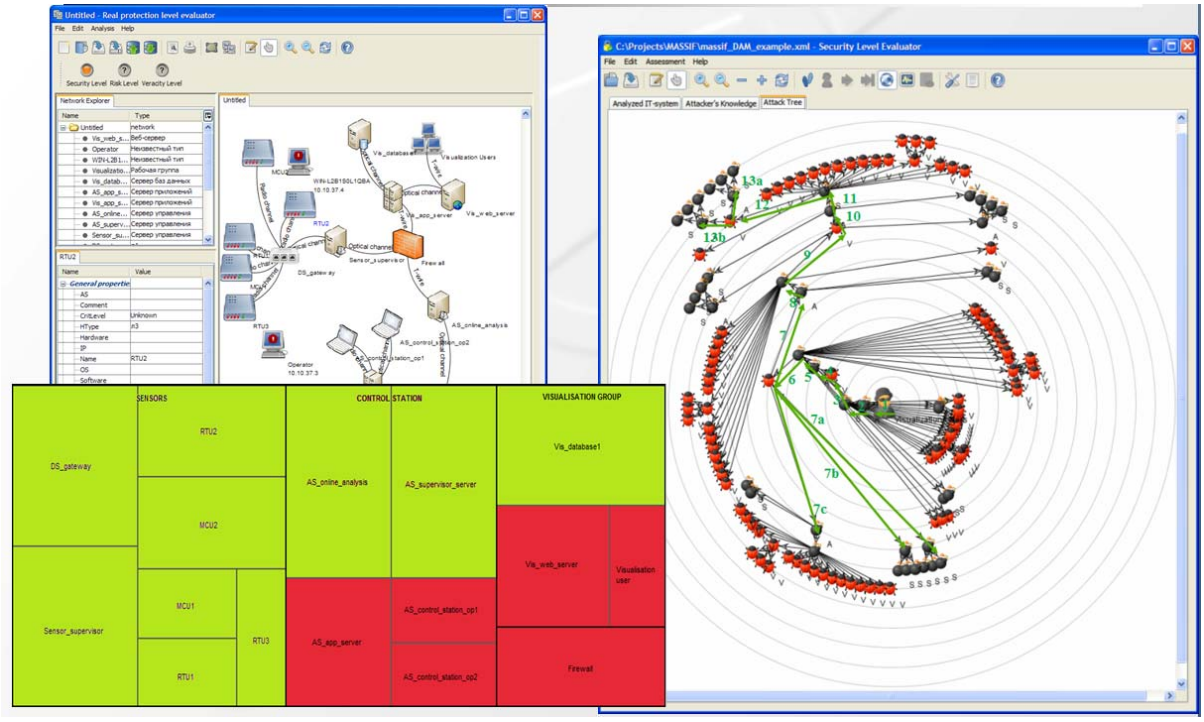


Рис. 2. Примеры реализованных интерфейсов

На рис. 3 представлено основное окно компонента визуализации, включающее следующие элементы: (1) главное меню; (2) панель управления; (3) панель графического представления уровня защищенности; (4) диалог доступа к сети (*Network Explorer*); (5) диалог свойств сети (*Property Explorer*); (6) окно представления конфигурации сети; (7) окно представления графа атак.

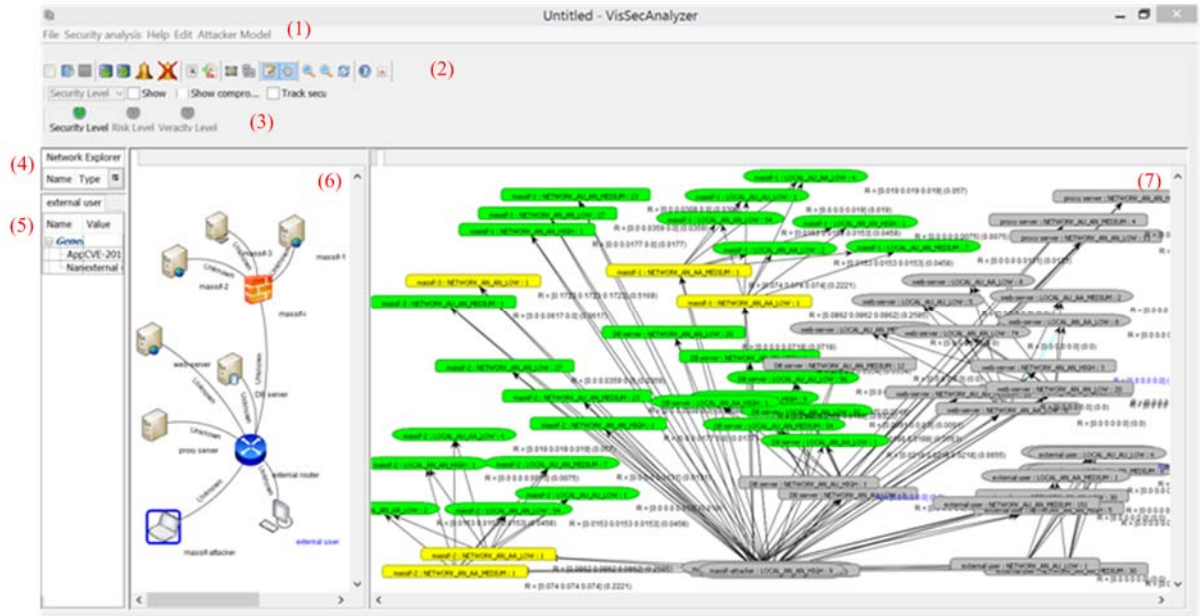


Рис. 3. Элементы основного окна компонента визуализации

Тестовые области, на которых проводилась оценка решений по расширенной аналитике, относились к наиболее характерным классам КВИ, каковыми являлись компьютерная сеть для обеспечения Олимпийских Игр, система мобильных компьютерных платежей, распределенная компьютерная сеть транснационального провайдера услуг и инфраструктура гидротехнического сооружения (дамбы).

Работа выполнена при финансовой поддержке РФФИ (проекты 16-29-09482 и 18-07-01488) и бюджетной темы АААА-А16-116033110102-5.

Список используемых источников

1. Котенко И. В. Интеллектуальные механизмы управления кибербезопасностью // Управление рисками и безопасностью. Труды Института системного анализа Российской академии наук. 2009. Т. 41. С. 74–103.

2. Котенко И. В., Саенко И. Б. Построение системы интеллектуальных сервисов для защиты информации в условиях кибернетического противоборства // Труды СПИИРАН. СПб. : Наука, 2012. Вып. 3 (22). С. 84–100.

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

4. 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.

5. Miller D. R., Harris Sh., Harper A. A., VanDyke S., Black Ch. Security Information and Event Management (SIEM) Implementation. McGraw-Hill Companies. 2011. 430 p.

6. 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. СПб. : Наука, 2012. Вып. 1 (20). С. 27–56.

7. 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.

8. Novikova E., Kotenko I. Analytical Visualization Techniques for Security Information and Event Management // Proceedings of the 21st Euromicro International Conference on Parallel, Distributed and network-based Processing (PDP 2013). Los Alamitos, California. IEEE Computer Society. 2013. P. 519–525.

9. Котенко И. В., Полубелова О. В., Саенко И. Б., Чечулин А. А. Применение онтологий и логического вывода для управления информацией и событиями безопасности // Системы высокой доступности. 2012. № 2. С. 100–108.

10. Kavanagh K. M., Rochford O., Bussa T. Magic Quadrant for Security Information and Event Management. Gartner. August 2016 (дата обращения 15.05.2018).

11. Kavanagh K. M., Bussa T. Magic Quadrant for Security Information and Event Management. Gartner. December 2017.

12. 19 Top UEBA Vendors [Электронный ресурс]. URL: https://www.esecurityplanet.com/products/top-ueba-vendors.html (дата обращения 15.05.2018).

13. Дрозд А. Обзор SIEM-систем на мировом и российском рынке [Электронный ресурс]. URL: https://www.antimalware.ru/analytics/Technology_Analysis/Overview_SECURITY_systems_global_and_Russian_market#part4 (дата обращения 15.05.2018).

14. Платформа RSA Security Analytics компании EMC [Электронный ресурс]. URL: https://russia.emc.com/security/securityanalytics/security-analytics.htm (дата обращения 15.05.2018).

15. IBM Security QRadar SIEM [Электронный ресурс]. URL: http://www-03.ibm.com/software/products/ru/qradar-siem (дата обращения 15.05.2018).

16. AlienVault OSSIM (Open Source Security Information Management) [Электронный ресурс]. URL: https://www.alienvault.com/products/ossim (дата обращения 15.05.2018).

17. HP ArcSight [Электронный ресурс]. URL: http://arcsight-russia.ru/products-hp-arcsight/products-hp-arcsight (дата обращения 15.05.2018).

18. Fraunhofer Institute for Secure Information Technology [Электронный ресурс]. Режим доступа: https://www.sit.fraunhofer.de/en/ (дата обращения 15.05.2018).

19. Orange Labs. [Электронный ресурс] URL: https://laborange.fr/ (дата обращения 15.05.2018).

20. Télécom SudParis [Электронный ресурс]. URL: http://www.telecom-sudparis.eu/ (дата обращения 15.05.2018).

21. Saenko I., Kotenko I., Kushnerevich A. Parallel Processing of Big Heterogenious Data for Security Monitoring of IoT Networks // Proceedings of the 25th Euromicro International Conference on Parallel, Distributed and network-based Processing (PDP 2017). Los Alamitos, California. IEEE Computer Society. 2017. P. 329–336.

22. Котенко И. В., Кулешов А. А., Ушаков И. А. Система сбора, хранения и обработки информации и событий безопасности на основе средств Elastic Stack // Труды СПИИРАН. 2017. № 5(54). С. 5–34.

23. Igor Kotenko, Andrey Fedorchenko, Igor Saenko, and Alexey Kushnerevich. Parallelization of security event correlation based on accounting of event type links // Proceedings of the 25th Euromicro International Conference on Parallel, Distributed and network-based Processing (PDP 2018). Los Alamitos, California. IEEE Computer Society. 2018. P. 462–469.

24. Elena Doynikova, Igor Kotenko. Countermeasure selection based on the attack and service dependency graphs for security incident management // Lecture Notes in Computer Science (LNCS), Vol. 9572, Springer, 2016. P. 107–124.

25. G. Gonzalez-Granadillo, E. Doynikova, I. Kotenko, and J. Garcia-Alfaro. Attack Graph-based Countermeasure Selection using a Stateful Return on Investment Metric // Lecture Notes in Computer Science, Springer-Verlag, Vol.10723. 2018. P. 293–302.

26. Maxim Kolomeec, Andrey Chechulin, Igor Kotenko. Visual analysis of CAN bus traffic injection using radial bar charts // The 1st IEEE International Conference on Industrial Cyber-Physical Systems (ICPS2018). Saint Petersburg, Russia, May 15-18, 2018. P. 841–846.

УДК 004.6

АКТУАЛЬНЫЕ ВОПРОСЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КИБЕРФИЗИЧЕСКИХ СИСТЕМ

И. А. Зикратов

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

Развитие телекоммуникационных систем и их интеграция с физическими объектами окружающего мира приводят к появлению новых моделей информационных систем, основанных на парадигме Индустрии 4.0. Особенности построения и функционирования киберфизических систем, такие как децентрализация управления, пространственная удаленность киберфизических устройств и нахождение их вне пределов контролируемой территории, необходимость использования телекоммуникационных технологий для обмена информацией между информационными объектами, ограниченность их представления о системе, а также непредсказуемая динамика внешней среды, обуславливают необходимость новых подходов для обнаружения и нейтрализации информационных угроз.

киберфизические системы, телекоммуникационные технологии, информационные угрозы.

Четвертая промышленная революция**,** более известная как «Индустрия 4.0», получила свое название от инициативы бизнесменов, политиков и ученых Германии в 2011 г. Целью инициативы было заявлено повышение конкурентоспособности обрабатывающей промышленности этой страны через усиленную интеграцию киберфизических систем (КФС) в производственные процессы. Другими словами, Индустрия 4.0 – производственная сторона, эквивалентная ориентированному на потребителей «Интернету вещей», в котором предметы быта, от автомобилей до тостеров, будут подключены к Интернету.

Киберфизическая система (КФС) (англ. *Cyber Physical System*) информационно-технологическая концепция, подразумевающая интеграцию вычислительных ресурсов в физические процессы. В такой системе датчики, оборудование и информационные системы соединены на протяжении всей цепочки создания стоимости, выходящей за рамки одного предприятия или бизнеса. Эти системы взаимодействуют друг с другом с помощью стандартных интернет-протоколов для прогнозирования, самоорганизации и адаптации к изменениям.

К технологическим тенденциям, на которых базируется концепция КФС, относятся:

– Большие данные и аналитика.

– Автономные (в том числе мобильные) роботы и самоорганизующиеся группы роботов.

– Системы компьютерного зрения.

– 3D-моделирование и симуляторы (в том числе в режиме реального времени).

– Облачные вычисления и облачные технологии.

– Интернет вещей и встраиваемые системы (IoT).

– Информационная безопасность (ИБ).

– 3D-печать.

– Дополненная реальность.

Возможности, предоставляемые посредством использования таких технологий, привлекают, прежде всего, крупный бизнес. Так, например, будущая IT архитектура Газпромнефти выглядит следующим образом (рис.).

В тоже время, следствием интеграции физических объектов в Интернет является появление новых, несвойственных ранее автоматизированным системам управления технологическими процессами, угроз. Предпосылками их появления могут быть:

1. Наличие специфических условий функционирования КФС:

– непредсказуемая динамика внешней среды вплоть до сознательного противодействия;

– неполнота и противоречивость знаний элементов КФС о состоянии внешней среды и других участников;

– разнообразие вариантов путей достижения цели, структур коллектива, распределения ролей;

– сложность обеспечения надежной коммуникации, распределенность группировки в пространстве;

– наличие элементов КФС вне пределов зоны контролируемой территории;

– масштабируемость системы в пространстве и времени;

– сложность внешнего контроля за элементами КФС.

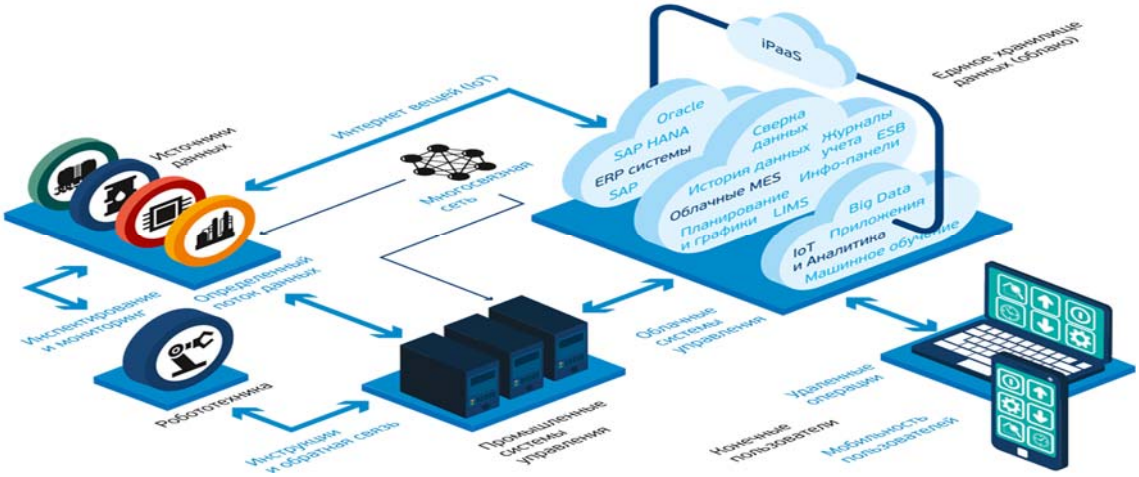


Рисунок. Будущая IT архитектура Газпромнефти

2. Появление новых (для АСУ ТП) видов угроз:

– подмена объектов (информационных и физических);

– модификация алгоритмов;

– модификация данных;

– отказ от авторства;

– разглашение информации;

– дезинформация;

– повышение привилегий;

– отказ в обслуживании;

– физические атаки;

– скрытые атаки;

– силовые атаки.

*3. Новые качества угроз, такие ка*к комплексность (сложность, множественность, гетерогенность), многовекторность (атака на различные уровни КФС, нарушителями ставятся различные цели и используются разные способы их достижения), возрастание роли методов социальной инженерии.

4. Возрастание стоимости причинённого ущерба

5. Появление новых уязвимостей, обусловленных слабой защищенность физических объектов вследствие требований к простоте и стоимости реализации, энергосберегающим характеристикам

6. Снижение эффективности существующих методов и способов защиты информации

7. Новые требования к компетенциям специалистов АСУ и ИБ

Появление новых угроз и уязвимостей приводит к необходимости разработки новых методов их обнаружения и нейтрализации. К числу таких подходов можно отнести:

Построение архитектуры КФС с учетом требований безопасности. Например, уменьшение количества критически важных информационных объектов в КФС, переход от централизованного к децентрализованным и комбинированным моделям управления, использование самоорганизующихся систем с коллективным (групповым, роевым) управлением [1].

Совершенствование методов обнаружения, нейтрализации и противодействия угроз. Например, переход от механизмов защиты на основе регулирования доступа на основе статуса информационного объекта (ИО) в системе, к моделям вычисления доверия и репутации ИО в системе. Использование искусственного интеллекта и методов социофизического моделирования [2].

Таким образом:

1. Обеспечение ИБ КФС на сегодняшний день является актуальной задачей, имеющей, тем не менее, различные подходы для ее решения [3].

2. Решение задачи ИБ КФС требует междисциплинарности подготовки специалистов на основе индивидуализации образовательных траекторий.

3. Решение задачи ИБ КФС требует активного внедрения технологий искусственного интеллекта в механизмы систем защиты информации и от информационных воздействий.

Список используемых источников

1. Зикратов И. А., Викснин И. И., Зикратова Т. В. Мультиагентное планирование проезда перекрестка дорог беспилотными транспортными средствами // Научно-технический вестник информационных технологий, механики и оптики. 2016. Т. 16. № 5. С. 839–849.

2. Zikratov I., Pantiukhin I., Sizykh A. The method of classification of user and system data based on the attributes // Proc. 18th Conference of Open Innovations Association. St. Petersburg, Russia, 2016. P. 404–409. doi: 10.1109/FRUCTISPIT.2016.7561557.

3. Brambilla M., Ferrante E., Birattari M., Dorigo M. Swarm robotics: a review from the swarm engineering perspective // Swarm Intelligence. March 2013. V. 7. № 1. P. 1–41. URL: http://link.springer.com/article/10/1007/s11721-012-0075-2), свободн.

ИНФОКОММУНИКАЦИОННЫЕ СЕТИ И СИСТЕМЫ

УДК 004.056

Приглашённый доклад

МЕТОДИКИ И СРЕДСТВА РЕАГИРОВАНИЯ НА КИБЕРАТАКИ В СИСТЕМАХ ИНДУСТРИАЛЬНОГО ИНТЕРНЕТА ВЕЩЕЙ

Е. В. Дойникова[1,2], И. В. Котенко[1,2]

[1]Санкт-Петербургский институт информатики и автоматизации Российской академии наук
[2]Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

Развитие индустриального Интернета вещей создает новые возможности для реализации кибератак. Как следствие, в последние годы существенно возрос интерес к технологиям противодействия кибератакам в таких системах. В данной работе анализируются основные исследования и практические реализации в области защиты систем индустриального Интернета вещей, выделяются их достоинства и недостатки. Приводятся преимущества использования нейро-нечетких сетей и генетических алгоритмов при принятии решений по реагированию. В настоящее время разрабатывается система автоматизированного реагирования на кибератаки в системах индустриального Интернета вещей на основе данных технологий.

индустриальный Интернет вещей, кибератаки, реагирование на кибератаки, принятие решений, нейро-нечеткие сети, генетические алгоритмы.

На текущий момент информационные технологии плотно проникли во все сферы жизни человека. Одним из интересных и относительно новых понятий является «индустриальный Интернет вещей». Оно появилось с внедрением в производство киберфизических систем. Говоря об индустриальном Интернете вещей, в первую очередь, необходимо разобраться с определением и состоянием дел в области стандартизации.

Отметим, что в настоящее время как стандарты в области Интернета вещей, так и в области индустриального Интернета вещей, находятся на стадии разработки. Для развития индустриального Интернета вещей было создано сообщество «консорциум индустриального Интернета» (*industrial internet consortium*, IIC), объединяющее множество ведущих мировых промышленных, исследовательских и правительственных организаций (в том

числе, Bosch, EMC^2, Huawei, IBM, Intel, SAP, «Ростелеком» и многие других) [1, 2]. Его партнером в России является Национальная ассоциация участников рынка промышленного Интернета (НАПИ) [3]. Их целью заявлено продвижение индустриального Интернета, объединяющего подключенные «умные» машины и процессы. В их задачи входит не формирование стандартов как таковых, а разработка требований к индустриальному Интернету вещей (путем разработки его архитектуры и оценки применимости к ней существующих стандартов) и передача их организациям, занимающимся стандартизацией [1]. В отличие от автоматизированных систем управления технологическим процессом (АСУ ТП), в сферу интересов индустриального Интернета входит значительно больше областей. Это управление железнодорожным транспортом, управление роботами, управление производством, медицинские сети, включая сети имплантируемых устройств, подключенные автомобили, подключенные ветровые турбины, системы управления отходами и многие другие [4].

На данный момент консорциум предлагает архитектурное описание индустриального Интернета в соответствии с ISO/IEC/IEEE 42010:2011, включающее уровень бизнеса (отвечает на вопрос «зачем?»), уровень применения (отвечает на вопрос «что?» с точки зрения действий), функциональный уровень (отвечает на вопрос «что?» с точки зрения функций) и уровень реализации (отвечает на вопрос «как?»).

Очевидно, что повсеместное внедрение «подключенных «умных» машин и процессов», с одной стороны, создает новые возможности для киберпреступников, а с другой стороны, представляет для них повышенный интерес с точки зрения возможной выгоды. Так, в [5] отмечается, что повсеместная взаимосвязь вещей с одной стороны обладает огромным потенциалом, делая информацию, сервисы и продукты более доступными, а с другой стороны, они становятся более уязвимыми, чем когда-либо. Поэтому особое внимание консорциум уделяет обеспечению безопасности, которой занимается отдельно выделенная группа. К настоящему времени ими разработан документ [6]. Документ определяет ключевые характеристики систем, заслуживающих доверия (безопасность, защищенность, надежность, устойчивость, приватность), описывает отличительные особенности защиты систем индустриального Интернета вещей, предлагает средства защиты узлов и средств связи, дает рекомендации по мониторингу и анализу защищенности, а также управлению защищенностью.

На данный момент работа консорциума представляется наиболее продвинутой инициативой в области комплексной безопасности индустриального Интернета. Однако необходимо также отметить другие инициативы в этой области, например, предложенную Национальным институтом стандартов и технологий США (NIST) систему безопасности критических инфраструктур [7], позволяющую организациям применить лучшие практики

в области управления рисками кибербезопасности. Она позиционирует риски кибербезопасности как часть процессов управления рисками организации и включает три уровня: ядра (набор действий, критериев и ссылок, формирующих руководство по разработке системы безопасности организации), профиля (соотнесение действий по безопасности с требованиями бизнеса и ресурсами организации) и реализации (определение текущего взгляда организации на риски кибербезопасности и процессов по управлению рисками).

Кроме того, существует ряд исследовательских работ в данной области. В [8, 9, 10] рассматриваются основные сложности, связанные с безопасностью индустриального Интернета вещей, в том числе, сложность реализации контрмер (ввиду множества взаимосвязей между элементами и распределенной архитектуры), большие объемы данных, затрудняющие анализ рисков для множества взаимосвязанных систем, большая поверхность атаки (которая включает в себя аппаратное обеспечение, программное обеспечение, протоколы связи и многое другое), а также большое количество нежелательных состояний, которые могут нанести материальный ущерб или ущерб здоровью человека. В [5] частично затронуты проблемы безопасности индустриального Интернета вещей. Отмечено, что особую важность приобретает автоматизация мониторинга безопасности, из-за множества журналов безопасности и большого количества данных безопасности. Перспективными направлениями названы системы на основе поведенческого анализа [11], нанотехнологии, квантовые компьютеры (например, для машинного обучения, или квантовой криптографии), биокомпьютеры. К возможным решениям авторы отнесли устойчивую самостоятельную адаптацию устройств индустриального Интернета вещей, системы смешанного доверия, анализ больших данных, проактивное реагирование на угрозы. Кроме того, авторы отмечают важность стандартизации для обеспечения безопасности данных при хранении и передаче, и важность взаимодействия производителей аппаратного и программного обеспечения для формирования будущего безопасного Интернета вещей.

В [9] отмечается необходимость не только комплексного обеспечения безопасности индустриального Интернета вещей, но и обеспечения безопасности его отдельных элементов. Кроме того, даются частные рекомендации по обеспечению безопасности, такие как децентрализация данных, шифрование данных при хранении и передаче, использование локальных хранилищ данных. В [12] говорится о том, что идеальным решением был бы учет требований безопасности при разработке элементов индустриального Интернета вещей. В частности, в отчете Motorola Solutions [13] говорится о применении широкого спектра решений по безопасности от аутентификации на конечных устройствах и шифрования данных до передовых межсе-

тевых экранов и средств мониторинга. В [14] также рассматривается ряд методов (мозговой штурм, экспертные оценки, математическая логика, аналитические методы) и средств (соответствие стандартам, российский индустриальный шлюз безопасности, криптографические средства) обеспечения безопасности. Однако на обновление всех систем индустриального Интернета вещей уйдет огромное количество времени, и на данный момент наилучшим решением является учет требований безопасности при формировании архитектуры и тщательный анализ и мониторинг защищенности.

Одним из основных элементов безопасного индустриального Интернета вещей в вышеперечисленных источниках называют создание комплексной системы мониторинга безопасности. В [6] к функциям мониторинга и анализа разработчики относят: мониторинг узлов и связей между ними, безопасное удаленное формирование журналов событий, мониторинг процессов, являющихся частью отдельных задач индустриального Интернета вещей; поведенческий и основанный на правилах анализ событий; проактивные действия по предотвращению инцидентов, реактивное обнаружение атак и восстановление, и выявление причин инцидентов или форензику. Данная функциональность накрывается системам мониторинга безопасности и управления инцидентами (SIEM-системами) [15]. Однако для мониторинга безопасности индустриального Интернета вещей данные системы нуждаются в интеллектуализации [16] и ряде усовершенствований, в том числе на важнейших этапах обнаружения атак, моделирования ситуации и оценки защищенности и выбора контрмер [17, 18, 19, 20]. При этом должны быть учтены такие особенности систем индустриального Интернета вещей как разнородность элементов и связей между ними, открытость, большие объемы разнородных данных. Для этого авторами ведется работа по внедрению в общий процесс мониторинга безопасности таких методов интеллектуального анализа данных, как нейро-нечеткие сети для решения частных задач классификации в рамках оценки защищенности при прогнозировании целей кибератак и генетических алгоритмов для принятия решений по реагированию на инциденты безопасности.

Работа выполнена при финансовой поддержке РФФИ (проекты 16-29-09482 и 18-07-01488), бюджетной темы АААА-А16-116033110102-5 и стипендии президента РФ (СП-751.2018.5).

Список используемых источников

1. Diab W. W. Overview of IIC and Industrial Analytics: Fueling the IIoT Revolution [Электронный ресурс] // 3rd International Symposium, 2017. Режим доступа: http://www.meti.go.jp/press/2017/12/20171201005/20171201005e.pdf (дата обращения 30.03.2018).

2. Industrial Internet Consortium. Официальный сайт [Электронный ресурс]. Режим доступа: www.iiconsortium.org (дата обращения 30.03.2018).

3. Национальная ассоциация участников рынка промышленного Интернета (НАПИ). Официальный сайт [Электронный ресурс]. Режим доступа: http://www.iotunion.ru/ru/ (дата обращения 30.03.2018).

4. Сидоров Г. «Интернет вещей» (IoT) в России. Технология будущего, доступная уже сейчас [Электронный ресурс] // Бизнес-завтрак PwC и НАПИ, ООО «ПрайсвотерхаусКуперс Консультирование»: 2017. Режим доступа: https: // www.pwc.ru / ru / events / assets / iot-seminar-all-presentations.pdf (дата обращения 30.03.2018).

5. Blowers M., Iribarne J., Colbert E., Kott A. The future Internet of things and security of its control systems [Электронный ресурс]. Режим доступа: https://arxiv.org/ftp/arxiv/papers/1610/1610.01953.pdf (дата обращения 30.03.2018).

6. Industrial Internet of Things. Volume G4: Security Framework [Электронный ресурс] // Report, 2016. Режим доступа: https://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB.pdf (дата обращения 30.03.2018).

7. Framework for improving critical infrastructure cybersecurity. Volume 1.0 [Электронный ресурс] // National Institute of Standards and Technology, 2014. Режим доступа: https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf (дата обращения 30.03.2018).

8. Sadeghi A.-R., Wachsmann C., and Waidner M. Security and Privacy Challenges in Industrial Internet of Things // Proceedings of the 52nd Annual Design Automation Conference (DAC'15). Sec. 4. New York, New York, USA: ACM Press, 2015.

9. Urquhart L., McAuley D. Avoiding the Internet of Insecure Industrial Things [Электронный ресурс]. Computer Law and Security Review (Forthcoming), 2017. Режим доступа: https://ssrn.com/abstract=3083605 (дата обращения 30.03.2018).

10. Paine T. Industrial Internet of things and communications at the edge [Электронный ресурс]. Режим доступа: http: // foxon.cz / downloads / Kepware / Kepware-Industrial-IOT-eBook_EN.pdf (дата обращения 30.03.2018).

11. Blowers M. Know Thy operator; Establishing ground truth in Industrial Control Systems (ICS) // Las Vegas: BSIDES, 2014.

12. Meltzer D. Securing the industrial Internet of things [Электронный ресурс] // ISSA Journal, 2015. Режим доступа: https://c.ymcdn.com/ sites /www.issa.org /resource/resmgr/journalpdfs/feature0615.pdf (дата обращения 30.03.2018).

13. The industrial Internet of things. Next generation technology enchancing productivity and safety [Электронный ресурс] // Motorola Solutions, 2017. Режим доступа: https://www.motorolasolutions.com/content/dam/msi/docs/products/industrial-internet-of-things/iiot/industrial_internet_of_things_brochure.pdf (дата обращения 30.03.2018).

14. Карантаев В. Вопросы защиты информации при внедрении новых инфокоммуникационных технологий: практика применения СКЗИ [Электронный ресурс] // Infotecs : 2017. Режим доступа: https: // www.pwc.ru/ru/events/ assets/iot-seminar-all-presentations.pdf (дата обращения 30.03.2018).

15. Котенко И. В., Саенко И. Б. SIEM-системы для мониторинга и управления инцидентами // Транспортная безопасность и технологии. 2017. № 04 (51). С. 96–97.

16. Котенко И. В. Интеллектуальные механизмы управления кибербезопасностью // Управление рисками и безопасностью. Труды Института системного анализа Российской академии наук. 2009. Т. 41. С. 74–103.

17. Kotenko I., Stepashkin M. Network Security Evaluation based on Simulation of Malefactor's Behavior // SECRYPT 2006 – International Conference on Security and Cryptography, Proceedings International Conference on Security and Cryptography, SECRYPT 2006. Setubal, 2006. P. 339–344.

18. 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. P. 617–623.

19. Novikova E., Kotenko I. Analytical Visualization Techniques for Security Information and Event Management // Proceedings of the 2013 21st Euromicro International Conference on Parallel, Distributed, and Network-Based Processing, PDP 2013. P. 519–525.

20. Котенко И. В., Полубелова О. В., Саенко И. Б., Чечулин А. А. Применение онтологий и логического вывода для управления информацией и событиями безопасности // Системы высокой доступности. 2012. Т. 8. № 2. С. 100–108.

УДК 004.725

О РЕАЛИЗАЦИИ ТУМАННЫХ ВЫЧИСЛЕНИЙ В СЕТЯХ ПОСТ-NGN

А. О. Авчарова, Б. С. Гольдштейн

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

С внедрением инновационных технологий, к 2020 г. ожидается увеличение трафика до 194 экзабайта в год. Существующие облачные архитектуры не могут идти в ногу с объемом и скоростью этих данных. Туманные вычисления – расширение традиционной облачной модели. Архитектура тумана выборочно перемещает вычисления, хранение, связь, управление и принятие решений ближе к краю сети, с целью решить ограничения в текущей инфраструктуре.

туманные вычисления, облачные вычисления, OpenFog, IoT.

Туманные вычисления нацелены на решение сквозных проблем, таких как контроль производительности, задержки и эффективность использования ресурсов. Облачные и туманные вычисления находятся во взаимовыгодном и взаимозависимом положении. Естественно, что некоторые функции более выгодны для выполнения в туманных узлах, тогда как другие лучше подходят для облаков. Традиционное «облако» по-прежнему будет оставаться важной частью вычислительных систем [1].

Основной областью применения туманных вычислений является Интернет вещей (*Internet of Things*). Интернет вещей управляет преобразованием сети путем подключения повседневных объектов и устройств друг

к другу и к облачным сервисам. В современных моделях развертывания подчеркивается обязательная облачная связь, однако это не представляется возможным во многих реальных ситуациях.

Облачные архитектурные подходы не могут поддерживать прогнозируемые скорости передачи данных и объемные требования к IoT. Поэтому необходимо перенести часть вычислительных и сетевых ресурсов ближе к краю сети, что является основой для туманных вычислений. Элементы вычислений, сетей, хранения и ускорения этой новой модели известны как туманные узлы [2].

Для наглядности можно привести несколько примеров.

Сценарий нефтепровода

Каждый нефтепровод оснащен датчиками давления, расхода, различными регулирующими клапанами и др.

Можно переносить все показания датчиков в облако (возможно, используя дорогостоящие спутниковые каналы), анализировать показания на серверах облаков для обнаружения ненормальных условий и отправлять команды назад, чтобы отрегулировать положение клапанов. Но есть несколько проблем: пропускная способность для передачи данных в облако и из него может стоить тысячи долларов в месяц; эти соединения могут быть небезопасны; задержка может составлять несколько сотен миллисекунд, что в данном случае критично; и, если облако недоступно или перегружено, управление будет потеряно.

Второй вариант сценария – размещение иерархии локальных туманных узлов вблизи трубопровода, которые могут подключаться к датчикам и приводам. Узлы тумана могут быть очень безопасными, уменьшая угрозу взлома. Узлы тумана могут реагировать на аномальные условия в миллисекундах [1].

Перемещение большинства функций принятия решений этой системой управления в туман и одновременное обращение к облаку, чтобы сообщать о статусе или приемах команд, создает превосходную систему управления.

Сценарий визуальной безопасности и наблюдения

Камеры наблюдения и безопасности развертываются во всем мире. Они имеют возможность генерировать огромное количество данных, которые могут превышать терабайты в день для одной камеры. Обширная пропускная способность визуальных данных и других датчиков, собираемых по крупномасштабной сети, делает невозможным перенос всех данных в облако для получения информации в реальном времени.

«Туман» позволяет создавать системы распределенного видеонаблюдения в режиме реального времени, которые поддерживают конфиденциальность. Узлы тумана используются для интеллектуального разделения обработки видеоизображения. Алгоритмы видеоаналитики могут быть расположены на самих туманных узлах и выполняться на обычных процессорах или ускорителях [1].

Для реализации приведенных выше примеров необходимо разобраться в архитектуре OpenFog. Рассмотрим основные принципы, на которых строится эта архитектура (рис. 1) [1].

– *Безопасность.* Многие приложения IoT, поддерживаемые OpenFog RA, имеют важные аспекты жизни. Поэтому любое нарушение безопасности в Тумане может иметь серьёзные последствия. Соответствие требованиям OpenFog RA гарантирует, что развертывание тумана будет построено на безопасной комплексной вычислительной среде.

– *Масштабирование.* Возможность масштабирования позволяет сетям тумана изменять размер. Вы можете увеличить мощность отдельных туманных узлов, добавив такие аппаратные средства, как процессоры, устройства хранения данных или сетевые интерфейсы.

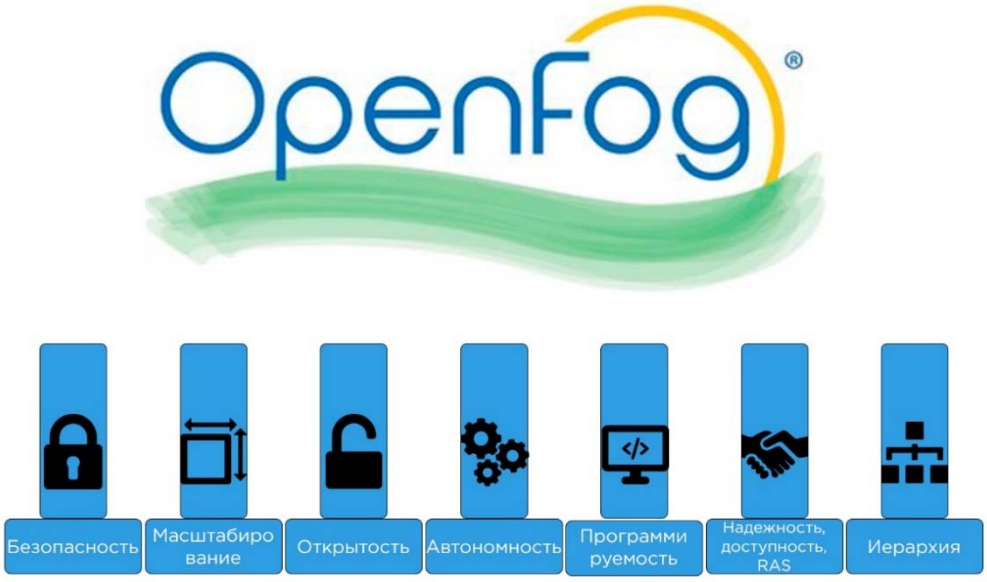


Рис. 1. Основные столпы OpenFog

– *Открытость.* Открытость необходима для успеха вездесущей системы туманных вычислений для платформ и приложений IoT. Открытость как основополагающий принцип позволяет туманным узлам существовать в любых сетях.

– *Автономность.* Автономность позволяет туманным узлам продолжать предоставлять разработанные функции даже при сбоях. Он не полагается на централизованный объект для работы (например, облако).

– *Программируемость.* Компонент программируемости обеспечивает высоко адаптивное развертывание, включая поддержку программирования на программном и аппаратном уровнях.

– *Надежность, доступность и удобство обслуживания* (*RAS*). Надежное развертывание будет продолжать предоставлять разработанные функции при нормальных и неблагоприятных условиях эксплуатации. Доступность обеспечивает непрерывное управление. Обслуживание развертывания «тумана» обеспечивает правильную его работу.

– *Иерархия.* Вычислительная и системная иерархия не требуется для всех архитектур OpenFog, но она по-прежнему выражается в большинстве развертываний. Представлены различные комбинации «тумана» и «облака».

1. Иерархия развертывания тумана, которая не зависит от облака. Примерами могут служить боевые системы вооруженных сил, некоторые системы здравоохранения, больницы и банковские системы банкоматов.

2. Облако, используемое для обработки информации, относящейся к принятию решений с допустимой задержкой. К примерам относятся коммерческое управление зданием, коммерческий мониторинг солнечных панелей и розничная торговля.

3. Локальная инфраструктура тумана, используемая для чувствительных к задержке вычислениям, в то время как облако используется для баланса оперативной и деловой обработки информации.

4. Использование облака для всего стека из-за ограниченных сред, в которых развертывание тумана может оказаться неэкономичным. Например, сельское хозяйство и удаленные метеостанции.

Вышеперечисленные иерархии представлены для примера. В реальности же иерархии могут быть гораздо сложнее [2].

Разобравшись в столпах, рассмотрим пример реализации архитектуры OpenFog – визуальная безопасность для аэропортов, которая обеспечивает наглядный сквозной сценарий для туманных вычислений [1].

Для обнаружения возможных угроз требуется обширная сеть камер наблюдения (несколько тысяч камер в каждом аэропорту), а также датчики безопасности, звуковые и RFID датчики.

Камера IP обеспечивают приблизительно 1 ТБ/день на камеру, которая должна быть передана персоналу службы безопасности, либо потоки видео будут перенаправлены на локальные машины для сканирования и анализа.

Можно использовать облака для хранения и обработки данных. Это позволит хранить все данные в одном месте. Но при этом будут возникать проблемы с задержкой, высокая стоимость передачи данных, проблемы с доступом в облако, а также ограничения в обмене данными между системами внутри аэропорта. Поэтому все это приводит к необходимости использования туманных вычислений.

В данной сети будут использоваться различные туманные узлы, схожие по своей структуре [2]:

– *Сеть.* Каждый датчик подключен к узлу тумана с использованием Ethernet.

– *Ускорители.* Сценарий визуальной безопасности предлагает множество мест для включения ускорителей. Они могут использоваться для преобразования аналогового входа в цифровой формат. Ускорители также играют роль при визуальном распознавании.

– *Хранение.* Для заданной камеры, схема расчета тумана должна захватывать 24 часа видеоданных. Для этого требуется ~ 1 ТБ локализованного хранилища. В некоторых реализациях хранилище будет находиться на камере. Однако для сценария визуальной безопасности аэропорта будет оптимально настроить хранилище в иерархии туманных узлов. Это будет означать снижение стоимости камеры и объединение функций видеонаблюдения с возможностями видеоаналитики в одном и том же узле тумана.

– *Вычислительные ресурсы.* Если установлен туманный узел, программное обеспечение более высокого уровня должно понимать возможности обработки данных, генерируемых всеми подключенными датчиками и камерами. В нашем сценарии рекомендуется, чтобы большая часть вычисления выполнялась в узле тумана, а не на камере. Значительная память (от десятков до сотен ГБ) требуется на каждом туманном узле, чтобы избежать узких мест производительности в видеоадаптивных приложениях.

В данном сценарии развернуты несколько туманных узлов в каждом аэропорту и на разных уровнях иерархии (рис. 2) [1].

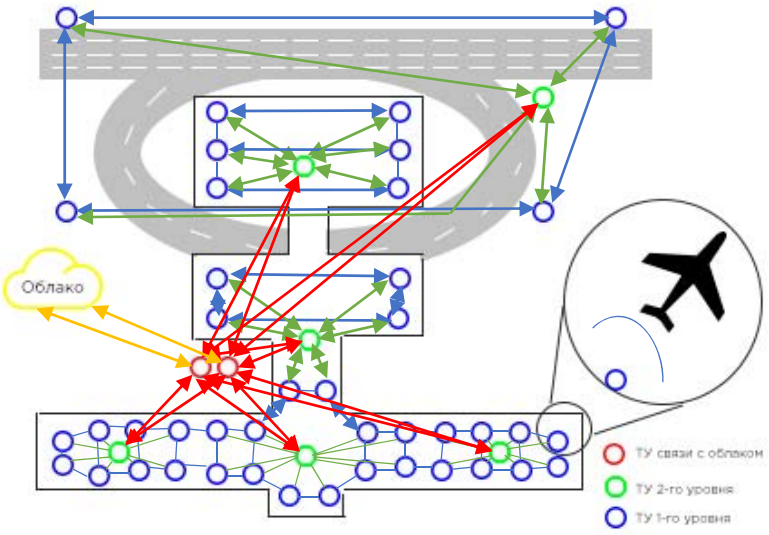


Рис. 2. Схема расположения туманных узлов в аэропорту

Среди них:

– узлы тумана для распознавания номерных знаков;

– узлы тумана вокруг парковки и станции прибытия;

– туманные узлы в зоне прибытия и вылета (непосредственно перед скринингом безопасности);

– узлы тумана, поддерживающие процесс скрининга. Эти туманные узлы соединены как с пассивными RFID-считывателями, так и с другими датчиками, а также с камерами;

– туманные узлы, находящиеся в терминале;

– иерархические туманные узлы, которые поддерживают и контролируют группировку туманных узлов.

Рассмотренный пример служит иллюстрацией тому, насколько выгоднее и проще использовать туманные вычисления в современном мире. Именно поэтому работа над созданием эталонной архитектуры OpenFog с каждым днем приближает нас к внедрению данной технологии в нашу жизнь.

Список используемых источников

1. OpenFog Consortium Architecture Working Group: OpenFog Reference Architecture for Fog Computing. Feb., 2017.

2. Enzo Baccarelli, Paola G. Vinueza Naranjo, Michele Scarpiniti, Mohammad Shojafar, Jemal H. Abawajy: Fog of Everything: energy-efficient networked computing architectures, research challenges, and a case study. 2017.

УДК 004.056

РАЗРАБОТКА ПРОГРАММНОГО МОДУЛЯ ЗАЩИТЫ ОТ ЛОЖНЫХ ВЫЗОВОВ ДЛЯ IP-АТС ELASTIX

А. И. Акимова, М. М. Ковцур

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

IP-телефония нашла широкое применение в корпоративных сетях связи. Одной из популярных программных IP-АТС является Elastix. АТС построена по модульной архитектуре и допускает разработку и установку дополнительных программных компонентов. Целью доклада является разработка алгоритма защиты IP-АТС от ложных вызовов на номера бесплатной горячей линии.

IP-АТС, Elastix, алгоритмы защиты, информационная безопасность.

На текущий момент IP-телефония нашла широкое применение в корпоративных сетях связи. Ее преимущество состоит в простоте развертывания, низкой стоимости звонков, легкой настройке и высоком качестве связи.

Одной из самых популярных программных АТС, согласно статистике поисковых запросов, является Elastix. Данная АТС поддерживает широкий набор функций и хорошо себя зарекомендовала, имеет графический интерфейс управления и модульную архитектуру.

За счет этих преимуществ, среди множества компаний заметно возросло количество переходов от традиционной к IP-телефонии. Один из сервисов, популярно внедряемых в корпоративных сетях – номер бесплатной горячей линии 8-800. Сервис оказывает поддержку действующим или потенциальным клиентам. Для повышения лояльности компании сами платят за вызовы, которые совершают клиенты. Поэтому возникает следующая проблематика: возрастает вероятность атак на данные номера с целью совершения пустых звонков, позволяющих увеличить расходы компании или привести оборудование к сбою из-за повышенной нагрузки. Для защиты от подобных атак и предлагается разработка специального модуля.

Чтобы более подробно представить текущую ситуацию, ниже приведена небольшая статистика звонков [1]:

– от 10 % звонков происходят со стационарных номеров г. Москвы;

– от 15 % звонков происходят со стационарных номеров других регионов России;

– 70–75 % звонков происходят с мобильных номеров России.

Стоимость звонков составляет примерно 0,80/1,00 руб./мин. (за входящие звонки со стационарных номеров г. Москвы) и от 3,20/10,00 руб./мин. (за входящие звонки с номеров мобильных операторов связи России). Расчеты показывают: если атакующий использует всего 50 номеров, каждые 10 минут такой атаки могут стоить порядка 5 000 руб., причем длительность атаки может варьироваться. Это может приносить достаточно ощутимые убытки даже для крупных компаний.

Рассмотрим концепцию построения модуля защиты от ложных вызовов для IP-АТС Elastix. Алгоритм защиты от подобных атак должен строиться на периодическом анализе статистики входящих/исходящих звонков. Пример статистики представлен на рис. 1.

В данной статистике приведены все звонки с указанием результата вызова. Ниже приведена расшифровка полей базы данных:

– src – номер вызывающего абонента;

– dst – номер вызываемого абонента;

– clid – номер вызываемого абонента в полном формате;

– channel – используемый канал;

– dstchannel – канал направления;

– duration – продолжительность соединения, в секундах (целое), от набора номера до отключения;

– billsec – продолжительность соединения, в секундах (целое), от ответа до отключения;

– disposition – результат звонка: ANSWERED, NO ANSWER, BUSY, FAILED.

calldate	clid	src	dst	channel
2017-10-07 20:37:31	"1448" <1448>	1448	1488	SIP/1448-00000004
2017-10-07 20:39:00	"1448" <1448>	1448	1488	SIP/1448-00000006
2017-10-07 21:36:18	"1488" <1488>	1488	1448	SIP/1488-00000000
2017-10-07 21:38:46	"1488" <1488>	1488	1448	SIP/1488-00000002

dstchannel	duration	billsec	disposition
SIP/1488-00000005	7	0	BUSY
SIP/1488-00000007	9	8	ANSWERED
SIP/1448-00000001	8	5	ANSWERED
SIP/1448-00000003	5	2	ANSWERED

Рис. 1. Пример статистики звонков IP-АТС Elastix

К разрабатываемому модулю защиты от ложных вызовов предъявляются следующие требования:

1. Работа в фоновом режиме без участия системного администратора.
2. Минимальная нагрузка на ресурсы системы.
3. Возможность вносить корректировки в установленные параметры модуля.
4. Отображение заблокированных номеров.
5. Техническая поддержка.

На текущий момент способов защиты от подобных атак не так много, при этом требуется участие специалистов, а также дополнительные временные затраты для формирования базы запрещенных номеров.

Сейчас используются несколько подходов для защиты от ложных вызовов на номера горячей линии:

1. Черный список по стране, городу, оператору, реализованный на стороне оператора или клиента.
2. Ограничение канальности линий, подключенных к 8-800.
3. Установка лимита ежедневных расходов на линию 8-800.

Все это может быть эффективно для относительно небольших атак и требует оперативного вмешательства персонала компании.

Для устранения данного недостатка, разрабатываемый модуль должен иметь автоматический режим работы. Необходимо реализовать периодиче-

ский анализ статистики входящих звонков на номера 8-800, а номера обнаруженных нарушителей автоматически помещать в черный список (ЧС). Такой подход, по предварительной оценке, будет занимать гораздо меньше времени, а также сможет работать в случае неопределенности, так как номера нарушителей заранее могут быть неизвестны.

Рассмотрим предлагаемый алгоритм, представленный на рис. 2, где: K – число входящих звонков от выбранного номера M за N минут; D – порог, который не должно превышать легитимное число вызовов от номера M за время N; B – время блокировки номера нарушителя, мин.

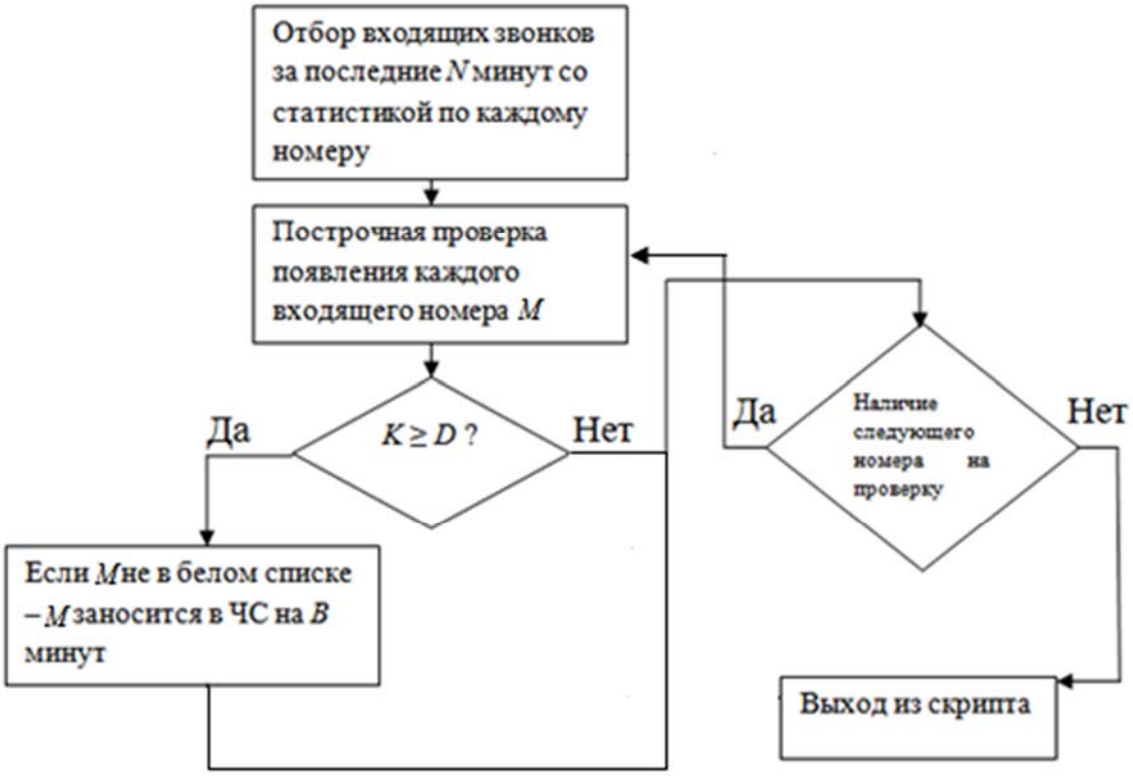


Рис. 2. Алгоритм работы модуля

Каждые t минут запускается скрипт, реализующий представленный алгоритм. Для каждого из номеров определяется число K их появлений в статистике и выполняется проверка, превысило ли K конкретного номера M заранее установленный порог D. При превышении порога номер M заносится в черный список на B минут. Если нет – проверяется следующий номер. Как только проверка по всем входящим вызовам закончена – происходит выход из скрипта.

Существуют еще некоторые параметры, которые необходимо учесть на этапе тестирования модуля:

- модуль не должен блокировать легитимные звонки;
- модуль должен работать только по выбранным входящим канал;

– время блокировки выбирается аргументировано;
– своевременно блокировать звонки нарушителей;
– интеграция в существующий интерфейс АТС.

Сейчас на рынке представлено несколько программных продуктов для мониторинга вызовов, проходящих через IP-АТС, однако данное программное обеспечение не имеет функции блокировки вызовов, а также затруднено использование этого ПО при внедрении протоколов безопасности IP-телефонии [2, 3]. Сравнение программных продуктов приведено в таблице.

ТАБЛИЦА. Сравнение программного обеспечения

Параметр	Разработанный модуль	VQManager	FlowMon
Удаленная поддержка	–	–	+
Поддержка старых ОС	+	–	?
Цена	Бесплатно	Демоверсия	Демоверсия
Необходимость в дополнительном оборудовании	–	–	+
Простота в использовании	+	–	–
Легкая установка	–	+	+
Поддержка безопасности IP-телефонии	+	–	–

Из представленной таблицы видно, что предлагаемый модуль отличается простотой в использовании, сохраняет работоспособность при использовании протоколов безопасности IP-телефонии, а также является бесплатным в сравнении с другими продуктами.

Дальнейшими задачами исследования являются разработка программной реализации модуля, а также тестирование разработанного ПО.

Список используемых источников

1. Какой номер выбрать 495 или номер 8800? [Электронный ресурс]. Режим доступа: https://nomer-495.ru/kakoj-nomer-vybrat-495-ili-nomer-8800/

2. Мониторинг сети VoIP с помощью VQManager [Электронный ресурс]. Режим доступа: http://www.ucexpert.ru/archives/1821/

3. Программное обеспечение по вендорам [Электронный ресурс]. Режим доступа: http://www.samara.antiviruspro.com/software/vendors/132555/

УДК 65.011.56

ЭВОЛЮЦИЯ УПРАВЛЕНИЯ ВЗАИМОДЕЙСТВИЕМ С КЛИЕНТАМИ В ТЕЛЕКОММУНИКАЦИОННОЙ СПЕЦИФИКЕ

В. А. Акишин

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
ООО «НТЦ Аргус»

Текущая конкурентная ситуация на рынке телекоммуникационных услуг заставляет операторов связи разворачивать вектор своего развития к клиенту, в частности, ориентировать в сторону клиента свои бизнес-процессы, а также среду выполнения этих процессов. В докладе рассматриваются основные вехи развития методов и подходов к управлению взаимодействием оператора связи и клиента, в частности предпосылки и перспективы перехода от классического подхода управления взаимоотношения с клиентом к новому этапу – управлению клиентским опытом.

клиентский опыт, CEM, TM Forum.

О причинах и предпосылках

Когда-то Илья Ильф, на открытии одной радиовыставки в далеком 1933 г. сказал такую замечательную фразу: «В фантастических романах главное это было радио. При нем ожидалось счастье человечества. Вот радио есть, а счастья нет». Эта замечательная цитата очень точно описывает современные реалии в части управления взаимоотношениями клиента и оператора связи. Еще вчера подход к управлению взаимоотношениями клиента и оператора связи ограничивался лишь процессами учета клиентов и их заявок (концепция CRM), но уже сегодня, рынок диктует операторам связи необходимость организовывать управление взаимоотношениями с клиентами в рамках новой парадигмы клиентского опыта и клиентских впечатлений (концепция CEM).

Безусловно, подобная потребность вызвана объективными характеристиками современного рынка телекоммуникаций, в частности:

– высокий уровень проникновения сервисов. Например, уровень проникновения сотовой связи на сегодняшний день достигает 170 % [1].

– стоимость привлечения каждого нового клиента в 5–7 раз дороже, чем удержание старого [2].

Кроме того, последние исследования говорят о том, что сегодня изменился сам клиент оператора связи. В частности, можно выделить следующие тезисы, характеризующие современного клиента:

– цифровизация клиентов. Например, сегодня становится очевидным, что с ростом социальной активности поколений Z и Y, повышается популярность использования Digital-каналов для коммуникации клиентов с поставщиками услуг. В частности, исследования [3] говорят о следующем:

- 74 % проводят в социальных сетях несколько часов в день;
- 99 % пользуются социальной сетью «Вконтакте», а 90 % считают ее основной;
- 74 % решают свои вопросы через социальные сети (в мире показатель 78 %);
- 63 % будут решать свой вопрос по телефону;
- 55 % будут решать свой вопрос через мессенджеры.

– клиент хочет и может быть самостоятельным. С ростом информационной грамотности клиентов, все большее их количество предпочитает решать возникающие проблемы самостоятельно с использованием инструментария Self-Service. Например, исследования Amdocs, говорят о важности проактивного взаимодействия с клиентами и мобильных приложениях [4]. В числе прочего, существует следующая статистика:

- 83 % для решения возникающих проблем готовы следовать инструкциям, изложенным в проактивных уведомлениях, вместо того, чтобы обращаться в контакт-центр;
- 76 % отдают предпочтение мобильным приложениям перед звонком в контакт-центр.

– клиент ценит простоту сервиса. Например, исследования Amdocs, говорят о влиянии качественных инструментов клиентских Self-Service в т. ч. мобильных приложений на лояльность клиентов – таким образом, 83 % рекомендовали бы своего оператора, если бы он предлагал простые в использовании комплексные мобильные приложения для самообслуживания [4]. Кроме того, исследования [5], говорят о причинах оттока современных клиентов, решаемых внедрением элементов Customer Experience в клиентское обслуживание В числе прочего:

- 70% клиентов ожидают от компании удобного сервиса, в частности элементов Self-Service в Личном кабинете;
- 56% клиентов уходят из-за проблем с первичными элементами самообслуживания на Web-сайте компании;

– клиент, осознавая свою значимость, ожидает персонализации при взаимодействии с компанией;

– современный клиент ценит возможность влиять на компанию и её процессы.

О современных подходах

Исходя из описанных выше тезисов, была сформулирована функциональная схема, описывающая современную информационную среду выполнения процессов взаимодействия с клиентами (рис.) в телекоммуникационной специфике.

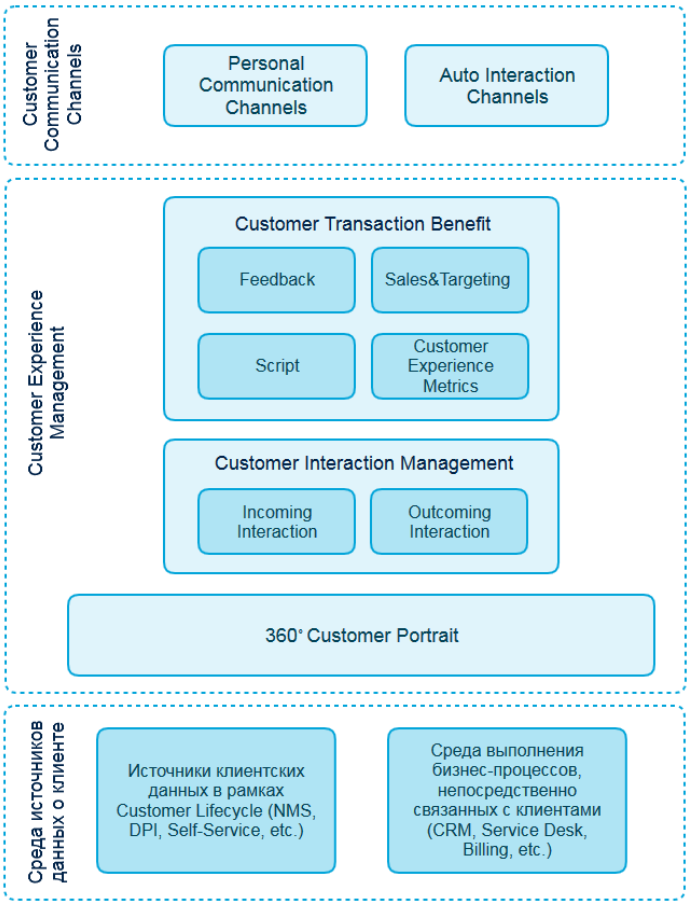


Рисунок. Функциональная карта информационной среды взаимодействия с клиентами

Рассмотрим данную схему подробней.

В основе всего, на нижнем уровне существует среда источников данных о клиенте. В общем случае, она делится на 2 составляющие:

– среда выполнения бизнес-процессов, непосредственно связанных с клиентами. Данная среда представляет собой комплекс информационных систем, в рамках которых происходит обработка бизнес-процессов, интересных клиенту и, в частности, где необходимо организовывать взаимодействие с клиентами (например, процесс обработки заявки на подключение, заявки на техническую поддержку и т. д.) В общем случае, это системы класса CRM, Service Desk, Billing и т. д. В контексте телеком специфики – это традиционная OSS/BSS-среда оператора связи;

– источники клиентских данных о Customer Experience в рамках Customer Lifecycle. Это некоторая совокупность информационных систем, в которых агрегируются данные о Customer Experience клиента, вне контекста бизнес-процесса оператора связи. Например, это могут быть NMS системы, в рамках которых агрегируется информация о состоянии услуг клиента и/или это могут быть системы, анализирующие трафик абонента в контексте использования интернета/цифрового телевидения. В дальнейшем эти данные могут быть использованы для построения оптимальной стратегии взаимодействия с клиентом (например, для формирования таргетированных предложений).

Далее, на основе уровня источников данных о клиенте строится функциональный концепт для управления клиентским опытом – Customer Experience Management (CEM). Функциональная среда CEM состоит из следующих уровней:

– уровень «Потрет 360 градусов» – данный уровень реализует комплекс средств управления и анализа клиентских данных, полученных от уровня источников. Ключевая цель данного уровня – сформулировать оценку некоторого результирующего значения интегрального Customer Experience, который состоит из совокупности факторов, влияющих на впечатления клиента на всех этапах его жизненного цикла. В частности, для анализа клиентских данных могут быть использованы различные математические методы и модели, такие как:

- нейронные сети;
- байесовская сеть;
- *PageRank*,
- нечеткие когнитивные карты.

– Customer Interaction Management, который по сути представляет собой некоторую Omni-платформу, обеспечивающую омниканальное взаимодействие клиента и компании с использованием различных каналов взаимодействия.

– уровень Customer Satisfaction Management, представляющие собой комплекс средств для получения некоторой дополнительной выгоды от взаимодействия с клиентом, выраженной, например, в получении обратной связи (*Feedback*), допродажи (*Sales&Targeting*), а также, в управлении оттоком, например, с использованием проактивных скриптов для взаимодействия с клиентом (*Script*).

Верхний уровень представленной функциональной модели – каналы коммуникации клиентов. Данный уровень включает в себя комплекс средств, реализующих общение клиента и компании. Сюда входят как средства прямой коммуникации клиента со специалистом компании (чат, звонок), так и средства автоматизированного взаимодействия (например, инструментарий *Self-Service*).

Сформированная подобным образом функциональная схема позволяет обеспечить оптимальную информационную и процессную среду для взаимодействия оператора связи и клиента, и, в частности, учесть аспекты и характеристики современного клиента.

Список используемых источников

1. Ланкевич К., Хабаев Н., Скоринов М. OSS комплекс как инструмент контроля лояльности клиентов оператора связи // T-Comm – Телекоммуникации и Транспорт. 2015. № 5. С. 36–40.

2. Гольдштейн А., Скоринов М., Феноменов М. Big Data – как выпустить джинна из бутылки? // Технологии и средства связи. 2015. № 5. С. 34–38.

3. Adindex.ru – сайт о рекламе и маркетинге в России и мире [Электронный ресурс]. Режим доступа: https://adindex.ru/publication/analitics/search/2017/05/18/159832.phtml, свободный. – Загл. с экрана.

4. CNews – Интернет-издание о высоких технологиях [Электронный ресурс]. Режим доступа: http://www.cnews.ru/news/line/proaktivnye_uvedomleniya_i_mobilnye, свободный. – Загл. с экрана.

5. SuperOffice – CRM for Better Customer Relationships [Электронный ресурс]. Режим доступа: https://www.superoffice.com/blog/customer-experience-statistics/, свободный. – Загл. с экрана.

Статья представлена научным руководителем, доктором технических наук, профессором Б. С. Гольдштейном.

УДК 65.011.56

МЕТОДЫ ОЦЕНКИ КЛИЕНТСКОГО ОПЫТА НА РАЗЛИЧНЫХХ ЭТАПАХ ЖИЗНЕНОГО ЦИКЛА КЛИЕНТА

В. А. Акишин, А. А. Кормановская

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

Клиентский опыт – понятие, формирующееся из множества факторов и представляет собой совокупность впечатлений и ощущений, получаемых клиентом на протяжении всего жизненного цикла. Одним из важнейших аспектов при грамотном построении процесса взаимодействия с клиентом – является совокупный анализ клиентского опыта с помощью математических методов. В данной работе рассматриваются различные математические методы для оценки клиентского опыта, в частности, нечеткие когнитивные карты.

Customer Experience, Customer Experience Management, когнитивные карты, нечеткая логика.

За последние несколько десятилетий рынок телекоммуникаций претерпел большие перемены. С каждым днем конкуренция между компаниями становится все более напряженной. И на сегодняшний день рынок диктует операторам необходимость пересматривать свой подход к бизнесу и ставить на первый план задачи по увеличению лояльности, удержанию клиентов, а также построению грамотной работы с существующими клиентами. Согласно оценкам TM–Forum, привлечение нового клиента стоит оператору в 5–7 раз дороже, чем удержание существующего [1]. Поэтому многие компании все активнее внедряют в свои бизнес-процессы концепцию Customer Experience Management – управление клиентским опытом, которая включает в себя совокупность процессов, методов и технологий, ориентированных на управление впечатлениями, которые клиент получает в процессе взаимодействия с компанией.

При этом понятие клиентский опыт – Customer Experience (CE) складывается из множества факторов, и представляет собой совокупность впечатлений, желаний и ощущений, которая возникает в процессе взаимодействия компании оператора с клиентом на протяжении всего жизненного цикла клиента (*Customer Lifecycle*), начиная от поиска информации об услуге, а заканчивая окончанием ее использования. Customer Lifecycle состоит из девяти этапов:

1. Be Aware – описывает деятельность клиента и оператора, которые относятся к маркетинговым аспектам работы с клиентом;

2. Interact – определяет маркетинговые аспекты работы с клиентом, но уже начинается двустороннее взаимодействие клиента и оператора. На данном этапе определяется, каким образом клиент запрашивает детали услуги и предложения для бронирования или предварительного заказа;

3. Choose – описывает выбор предложения для покупки. На данном этапе клиент окончательно определяется с конфигурацией и выбором услуги. Так же на данном этапе описываются и такие важные аспекты, как инсталляция и первичная настройка выбранной клиентом услуги;

4. Consume – характеризует аспекты, связанные с использованием сервиса, а именно с удовлетворенностью клиента, качества предоставляемого сервиса и др.;

5. Manage – определяет возможности управления сервисом, получение помощи при использовании сервиса, а также запросы, связанные с устранением неисправностей работоспособности сервиса;

6. Pay – характеризует жизненный цикл клиента с точки зрения возможностей и удобства оплаты уже подключенного сервиса, его тарификации, управления тарификацией, получения и управления счетами;

7. Renew – описывает аспекты, связанные с обновлением соглашения на использование сервиса (возобновлением договорных отношений клиента и оператора);

8. Recommend – характеризует аспекты, связанные с упоминаний сервиса и компании в различных источниках. На данном этапе также рассматриваются вопросы, связанные с наращиванием оператором лояльности клиента.

9. Leave – определяет аспекты, связанные с прекращением взаимоотношений между клиентом и оператором, включает в себя процедуру отключения сервиса.

Если проанализировать весь жизненный цикл клиента, можно сделать вывод, что факторами, формирующие клиентский опыт, являются различные аспекты деятельности компании оператора, например, технические характеристики сети оператора связи, разнообразие предоставляемых услуг, качество и возможности предоставляемого сервиса, уровень развития каналов взаимодействия с клиентом и т. д. Становится очевидно, что именно агрегация и совокупный анализ данных позволит операторам построить грамотную политику взаимодействия с клиентом, но без специализированных математических методов это сделать просто невозможно [1].

На данный момент для анализа клиентского опыта применяют различные методы, из них можно выделить такие как:

- нейронная сеть;
- байесовская сеть;
- PageRank;
- когнитивные карты.

Все приведенные выше методы используются для решения широкого круга задач, связанных с моделированием слабо структурированных (формализованных) процессов, их прогнозированием и поддержкой принятия решений.

В данной статье рассматривается применение когнитивных карт и нечеткой логики в процессе оценки клиентского опыта. В качестве исследования были выбраны метрики, стандартизованные организацией TM Forum, которые позволяют оценивать клиентский опыт на различных этапах жизненного цикла клиента, а именно на этапах «Choose», «Consume» и «Manage».

Безусловно, для построения нечеткой когнитивной карты необходимо выделить по выбранным этапам ключевые факторы, определить взаимосвязь и степень влияния между ними [2]. Процесс выделения ключевых факторов состоит из последовательности определенных шагов – проведение SWOT и PEST анализа предметной области, выделение наиболее важных факторов, оказывающие различные влияния на исследуемую область [3]. В результате анализа формируется проблемное поле в виде совокупности

ключевых факторов. Когнитивное отображение проблемного поля осуществляется в виде нечеткого ориентированного графа:

$$G = \langle V, E \rangle,$$

где V – множество факторов; $V_i \in V,\ i = 1, 2, \ldots, k$; E – набор связей между элементами данного множества.

Дуга $eij \in E$, $i, j = 1, 2, \ldots, n$ соединяет вершины графа, которые соответствуют ключевым факторам проблемного поля, наиболее значимым для управления проблемой [4]. Влияние факторов друг на друга может быть:

– положительным (+) – характеризует влияние фактора *A* на фактор *B*, при этом, если фактор *A* изменяется в большую сторону, то непосредственно и фактор *B* также изменяется в большую сторону и наоборот;

– отрицательным (–) – характеризует влияние фактора *A* на фактор *B*, при этом, если фактор *A* изменяется в большую сторону, то фактор *B* изменяется в меньшую сторону, если фактор *A* изменяется в меньшую сторону, то фактор *B* измениться в большую сторону;

– нулевым (0) – характеризует отсутствие влияния фактора *A* на фактор *B*.

Для исследования ключевыми показателями были выбраны следующие метрики:

- этап «Choose»: CH-C-1 (Customers Acquired), CH-C-3 (*Orders Successful*), CH-C-11 (*Hours to Deliver, from Request to Delivery*), CH-F-2 (% *Orders of Enquiries*), CH-F-25 (*Seconds per Account Activation, from Request to Activation*);
- этап «Consume»: CO-C-4 (*Seconds per Call Origination, from CM Service Request to Alerting*), CO-C-7 (% Calls Dropped Perceived), CO-C-8 (% *Call Good Voice Quality*), CO-E-7 (*Product Subjective Score* (*Enterprise*)), CO-E-10 (% *Streaming Sessions Disconnected*), CO-F-1 (Network NPS), CO-F-7 (*Service Interruptions*), CO-C-104 (% *Bandwidth Utilisation*), CO-C-107 (# *Minutes Between Service Interruptions – Minimum*), CO-E-100 (# *ms SDH Peer-to-Peer Transfer Delay – Mean*), CO-E-102 (% *Packets Lost*);
- Этап «Manage»: M-C-5 (# *First Contact Resolutions*), M-C-6a (*Incidents Resolved*), M-C-6c (*Incidents Due Closure*), M-C-9a (# *Minutes to Resolve Incident, from Incident Opened to Incident Resolved*), M-C-12 (# *Repeat Contacts*), M-F-3 (*Support Hotline Subjective Score – Manage Service/Profile*), M-F-8 (*Online Channel Subjective Score – Receive Help*), M-F-23 (% *Service Configurations Failed*), M-F-24 (# *Minutes per Service Configuration, from Request to Configuration*) [5].

После этапа выделения ключевых факторов, необходимо оценить, как они взаимосвязаны между собой и как влияют на целевой фактор (поло-

жительно, отрицательно, не влияют). Для наглядности связь факторов представлена в виде матрицы взаимовлияния в таблице, которая отображает ключевые факторы этапа «*Consume*» жизненного цикла клиента.

ТАБЛИЦА. Матрица взаимовлияния факторов когнитивной модели

Ключевой фактор / Влияющий фактор	CO-C-4	CO-C-7	CO-C-8	CO-E-7	CO-E-10	CO-F-1	CO-F-7	CO-C-104	CO-C-107	CO-E-100	CO-E-102	Целевой
CO-C-4	x	0	0	0	–	0	0	0	0	0	0	+
CO-C-7	–	x	–	–	0	–	0	0	0	0	0	–
CO-C-8	0	+	x	+	0	0	0	+	0	0	0	+
CO-E-7	0	0	0	x	0	+	0	0	0	0	0	+
CO-E-10	0	0	+	+	x	0	0	+	0	0	0	+
CO-F-1	0	0	0	0	0	x	–	0	0	0	0	+
CO-F-7	0	0	0	+	0	0	x	0	0	0	0	–
CO-C-104	0	0	+	–	0	0	0	x	0	0	0	+
CO-C-107	0	0	0	–	0	–	0	0	x	0	0	–
CO-E-100	0	0	0	0	0	+	+	0	0	x	0	–
CO-E-102	0	0	0	0	0	0	+	0	0	0	x	–

Далее ключевые и целевые факторы, их взаимосвязь, а также влияние друг на друга можно визуализировать в виде нечеткой когнитивной карты (рис.).

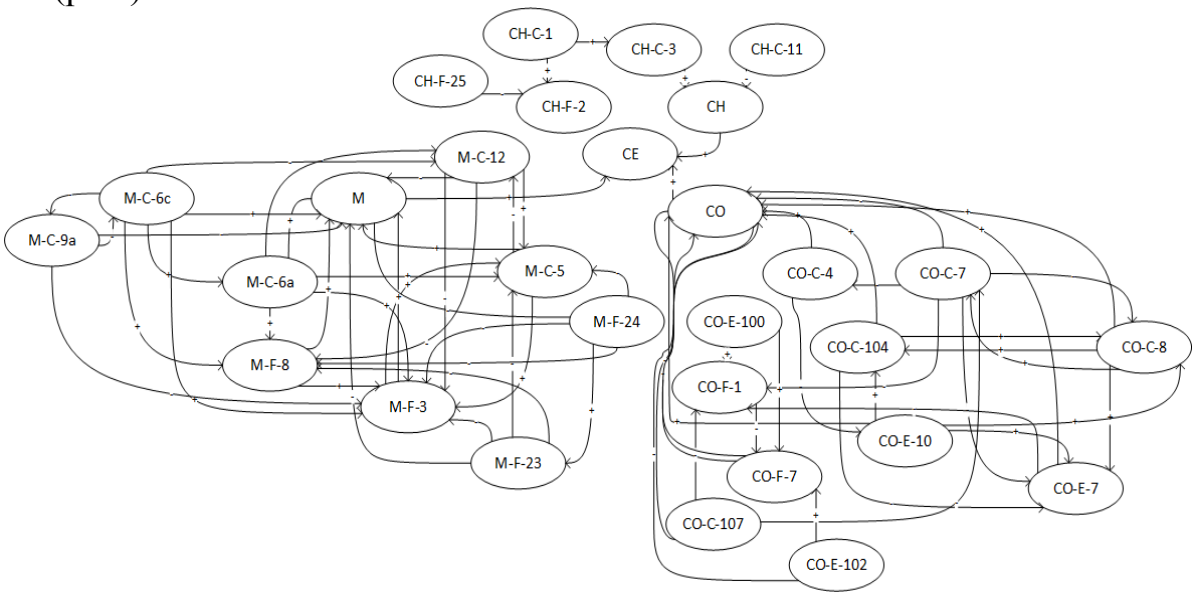


Рисунок. Когнитивная карта моделируемой области

В рамках данной статьи были рассмотрены возможности использования когнитивных карт и нечеткой логики применительно к оценки клиентского опыта на различных этапах жизненного цикла клиента. Именно применение нечетких когнитивных карт позволяет реализовывать эффективное управление Customer Experience. Зная матрицу взаимовлияний факторов, можно вполне с высокой точностью моделировать и визуализировать возможные результаты воздействия на один или несколько факторов. Развитием данной работы является расширение набора ключевых факторов и их дальнейшая декомпозиция, например, оценка клиентского опыта в рамках определенного сегмента.

Список используемых источников

1. Акишин В. А. Пользовательский опыт в когнитивной модели управления сетью оператора связи // T-Comm – телекоммуникации и транспорт. 2017. Т. 11, № 10. С. 10–15.

2. Пожарский Н., Лихачев Д., Кисляков С. Использование когнитивных карт и нечёткой логики в разработке OSS/BSS решений для операторов связи // T-Comm – телекоммуникации и транспорт. 2017. Т. 11, № 1. С. 21–25.

3. Маренко М., Мальцева М. Применение когнитивного моделирования для анализа проблем малого бизнеса // Известия Иркутской государственной экономической академии. 2015. Т. 25, № 6. С. 1014–1024.

4. Палюх Б. В. Какатунова Т. В. Нечеткая когнитивная карта как инструмент моделирования инновационной деятельности на региональном уровне // Программные продукты системы. 2012. № 4. С. 128-132.

5. TM FORUM. GB962A_Lifecycle_Metrics_R15.0.1. TM Forum; Декабрь, 2015.

Статья представлена доцентом кафедры, кандидатом технических наук А. Б. Гольдштейном.

УДК 004.056

АНАЛИЗ МЕХАНИЗМОВ ЗАЩИТЫ WI-FI СЕТЕЙ

Е. С. Александрова, Г. Н. Иванов, М. М. Ковцур

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

В последнее время всё чаще применяется технология беспроводного доступа в интернет. Крупные компании, рестораны, гостиницы, университеты, а также государственные и частные организации, имеющие зачастую большой список сотрудников, вместо проводной корпоративной сети используют беспроводную. Самым распространённым способом является передача данных через Wi-Fi сети, что позволяет сотрудникам подключаться в любой точке в зоне действия. Однако существует проблема

по обеспечению конфиденциальности и целостности данных, передаваемых при использовании сетей семейства стандартов IEEE802.11. В данной статье рассматривается анализ возможных атак на пользователей со стороны злоумышленника. Предложена модель защищенной беспроводной сети, с использованием современных технологий.

Wi-Fi сети, сетевые атаки, фишинг, спуфинг, рукопожатие, сниффинг, безопасность Wi-Fi сетей, многофакторная аутентификация, биометрия, модель системы защиты данных.

В настоящее время беспроводные сети применяются всё чаще и чаще. Наиболее важной и актуальной проблемой на данной момент является защита беспроводной сети. Развивается инфраструктура, повышаются возможности информационной технологии, и чем больше становится объектов, использующих беспроводную Wi-Fi сеть, тем острее встает вопрос защиты беспроводной сети от злоумышленника.

В последние годы исследователи обнаружили значительное число уязвимостей в механизмах обеспечения безопасности беспроводных сетей – в протоколах WEP/WPA, популярном механизме WPS, о чем неоднократно сообщается в разных статьях [1, 2].

Основные задачи данной работы следующие:

1) анализ проблем, связанных с попытками несанкционированного доступа в сеть;

2) анализ атак на беспроводные сети Wi-Fi;

3) Разработка защищенной Wi-Fi сети с использованием биометрической аутентификации.

Уязвимость Wi-Fi сетей можно продемонстрировать различными способами. Например, подслушиванием, где злоумышленник пассивно прослушивает трафик беспроводной сети и путём анализа и запросов извлекает полезную информацию. Фишинг (*fishing*), позволяет получить несанкционированный доступ путём дополнительной точки доступа (AP), при этом обычный сотрудник компании выступает в роли жертвы, подключаясь к неизвестной точке доступе в своем офисе, которая визуально ничем не отличается от оригинальной, не понимая, что, сообщая и вводя какой-то пароль или данные, предоставляет угрозу корпоративной сети. Эту атаку еще называют атакой MITM – человек посередине [3].

Сниффинг (*Sniffing*). Данный термин обозначает перехватывание пакетов, или данных, проходящих по сети. Для реализации данной атаки, т. е. для перехвата пакетов данных, которые проходят через сети Wi-Fi, проводится постоянный мониторинг сети. Захваченные пакеты с данными могут быть проанализированы и использованы для определенных целей.

Спуфинг DNS – это способ подделать адрес хоста, который доступен через сеть. Реализуется путем отправки ложной информация об IP-адресе

хоста. Цель – переадресация трафика на пакеты данных с фактического хоста на ложный. Этот метод можно также использовать для того, чтобы изменить адрес DNS сервера и весь трафик был перенаправлен на неверный адрес либо сделать так, чтоб адрес был недоступен [4].

MITM, «человек посередине» – это активная атака, предполагает вход в систему через других пользователей или чужие операционные системы. Злоумышленник выступает в роли посредника. В ходе работы, удалось перехватить имя пользователя и пароль при входе пользователя в систему, если, при этом использовалась двухфакторная авторизация. Чтобы разорвать подключение, было использовано приложение ettercap [5].

Проанализировав возможные атаки сделан вывод, что действительно, проблема защита Wi-Fi сетей до сих пор решена не полностью. Любой ключ не защищен от атаки перебора, а сети, зачастую, имеют уязвимости, позволяющие злоумышленнику внедриться и при этом остаться незамеченным [2].

Предлагается разработать модель защищенной Wi-Fi сети с помощью биометрической аутентификации [7]. Модель должна обладать следующими функциями и характеристиками:

1) защита от известных атак;
2) обнаружение атак или попыток несанкционированного доступа в сеть;
3) простота и скорость управления безопасностью беспроводной сети;
4) постоянный программный мониторинг сети;
5) удобства использования сети;
6) доступность реализации, снижение трудозатрат на организацию сети;
7) снижение финансовых затрат путём использования ПО, вместо конкретных физических устройств.

Для защиты от атак предлагается применить аутентификацию на основе биометрических данных. К биометрическим данным предъявляются следующие критерии:

1) Всеобщность: данный признак должен присутствовать у всех людей без исключения.
2) Уникальность: биометрия отрицает существование двух людей с одинаковыми физическими и поведенческими параметрами.
3) Простота и скорость управления безопасностью беспроводной сети.
4) Постоянство: для корректной аутентификации необходимо постоянство во времени.
5) Измеряемость: специалисты должны иметь возможность измерить признак каким-либо устройством для дальнейшего занесения в базу данных, а сотрудники легко передавать.

6) Приемлемость: общество не должно быть против сбора и измерения биометрического параметра.

Проведя анализ биометрических данных – отпечатка пальца, радужной оболочки и голоса, как показано в таблице – голосовая аутентификация, удовлетворяет всем критериям [8].

ТАБЛИЦА. Сравнение биометрических аутентификаций

Критерии	Fingerprint authentication	Rainbow shell authentication	Voice authentication
Всеобщность	+	+	+
Уникальность	+	+	+
Постоянство	–	+	+
Измеряемость	–	–	+
Приемлемость	+	–	+

При разработке модели предлагается использование ПО, разработанное компанией ООО «ЦРТ», активно работающей в области речевых технологий, VoiceKey [9]. Данное ПО в текущей модели позволяет производить авторизацию пользователя по голосу, затем сравнивать её с базой данных голосов и в зависимости от точности совпадения голоса с оригиналом либо пропустить пользователя, либо заблокировать [10]. Также в данной модели при несовпадении голоса предполагается срабатывание сигнализации, оповещения сотрудникам безопасности о попытке входа в сеть недоверенного лица – злоумышленника.

Общая концепция модели представлена на рисунке. Модель обладает характеристиками, описанными выше.

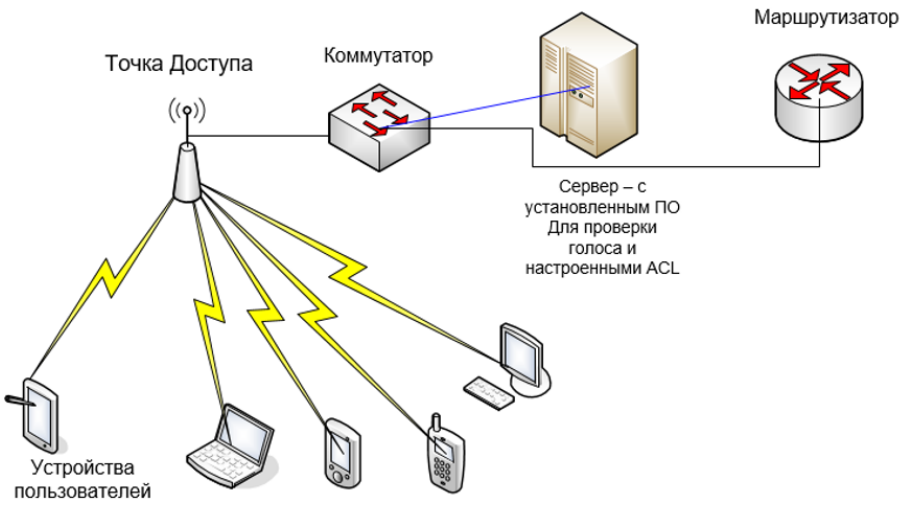


Рисунок. Модель защищенной Wi-Fi сети с использованием биометрической аутентификации

В исследовании представлены атаки типа фишинг, спуфинг и «человек посередине». Разработана концепция модели защищенной беспроводной сети с использованием аутентификации, основанной на биометрических данных, что позволяет защититься от атак. В данной модели предлагается возможность мгновенного уведомления службы безопасности в случае обнаружения мошенника, возможность настройки прав доступа (ACL). При помощи голосовой аутентификации достигается высокая скорость авторизации.

Дальнейшими задачами планируется работа с детальным описанием модели, описанием используемых протоколов и реализация модели в виртуальной среде для тестирования и подробного анализа.

Список используемых источников

1. Таненбаум Э., Уэзеролл. Д. Компьютерные сети, 5-е изд. СПб. : Питер, 2012. 960 с.

2. Dorothy Stanley. Working Group for WLAN Standards, 2018. pp. 14. URL: http://www.ieee802.org/11

3. Губсков Ю. А., Манюхин В. А., Киселёв М. Д., БОЛДЫРЕВ А. В., Верещагин Д. Ю. Анализ методов защиты Wi-Fi сетей и их уязвимостей // Информация и безопасность. 2017. Т. 20. № 1–1 (4). С. 73–80.

4. Antichat. Форум о безопасности беспроводных сетей и их уязвимостей. 2018. С. 12-15. URL: https://forum.antichat.ru/forum113.html

5. Варлатая С. К., Рогова О. С., Юрьев Д. Р. Анализ методов защиты беспроводной сети Wi-Fi от известных способов взлома злоумышленников // Молодой ученый. 2017. № 1. С. 36–37. URL: https://moluch.ru/archive/81/14770

6. Makalish V. O. Comparative analysis of information security systems in Wi-Fi Network: National Technical University of Ukraine “Kiev Polytechnic Institute”, 2016. pp. 20–23.

7. Ковалев Д., Ковцур М. Механизмы аутентификации управления ключами стандарта IEEE802.11-2012 // Первая миля. 2014. № 3 (42). С. 72–77.

8. Джейн А. Виды и системы биометрической аутентификации // СУБД «Открытые системы». 2016. С. 1–5. URL: https://www.osp.ru/os/2012/10/13033122

9. Техническая документация и описание ПО VoiceKey, 2017. 12 с. URL: https://www.speechpro.ru/product/sistemy-upravleniya-kachestvom-i-avtomatizatsii/voicekey/specification.

10. Дешевых Е. А., Конюхов В. М., Крылов К. Ю., Ушаков И. А. Исследование методов защиты от инсайдерских атак // Актуальные проблемы инфотелекоммуникаций в науке и образовании. IV Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 2-х т. 2015. С. 310–313.

УДК 621.396.2

ОСОБЕННОСТИ ПРАКТИЧЕСКОЙ РЕАЛИЗАЦИИ КВАЗИСОЛИТОННЫХ ВОЛОКОННО-ОПТИЧЕСКИХ СИСТЕМ СВЯЗИ

Е. И. Андреева, М. С. Былина, С. Ф. Глаголев

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

Проведены расчеты и выполнено моделирование солитонных волоконно-оптических систем связи, в которых поддержание квазисолитонного режима передачи сигналов реализуется методом управления потерями. Рассмотрены два способа управления потерями с помощью дискретных и распределенных оптических усилителей. Показаны преимущества использования распределенного усиления. Приведены инженерные формулы для проектирования солитонных систем связи.

волоконно-оптические системы связи, оптическое волокно, хроматическая дисперсия, дисперсия групповых скоростей, затухание, нелинейные оптические эффекты, оптические солитоны, фазовая самомодуляция, оптическое усиление.

Основной тенденцией развития волоконно-оптических систем связи (ВОСС) является повышение эффективности использования каждого оптического волокна (ОВ). Это требует увеличения скорости в канале и увеличения числа каналов, что реализуется в магистральных и транспортных ВОСС с использованием технологии плотного мультиплексирования в волновой области (DWDM) [1]. ВОСС большой протяженности, соединяющая узлы сети, обычно состоит из усилительных участков (УУ). Каждый усилительный пункт обеспечивает компенсацию затухания и хроматической дисперсии (ХД) в телекоммуникационном ОВ, например, использованием компенсирующего ОВ, включаемого между двумя каскадами оптического усилителя (ОУ).

Существует другой способ компенсации искажений сигналов с амплитудной двоичной модуляцией и бинарным кодированием с возвращением к 0 (RZ). Компенсация искажений за счет ХД возможна в ОВ с отрицательным значением дисперсии групповых скоростей (ДГС) β_2 за счет фазовой самомодуляции (ФСМ), которая возникает в ОВ при больших мощностях сигналов. ФСМ характеризуется коэффициентом нелинейности γ [1, 2, 3]. Исследование решений нелинейного уравнения Шредингера, описывающего процессы распространения оптических импульсов по ОВ без потерь, предсказывает возможность существования импульсов определенной формы и длительности $2T_0$, так называемых временных фундаментальных

солитонов первого порядка ($N = 1$), которые не искажаются при распространении в ОВ вдоль оси Z. Также были предсказаны солитоны более высоких порядков (с целым значением $N > 1$), которые по мере распространения периодически изменяют свою форму, возвращаясь к исходной.

Установлено [1, 2, 3], что фундаментальный солитон имеет огибающую в форме гиперболического секанса. Его распространение вдоль оси Z по ОВ без потерь описывается функцией:

$$u(z,\tau) = sec\ h(\tau)\cdot exp(i\cdot z/2),\ z = Z/L_D,\ \tau = T/T_0,\ L_D = T_0^2/|\beta_2|,$$

где z, τ – нормированные расстояние и время, L_D – дисперсионная длина ОВ, P_0 – пиковая мощность импульса на входе в ОВ. Запишем условие существования солитонов первого и более высоких порядков [2, 3]:

$$N^2 = L_D/L_{NL} = \gamma\cdot P_0\cdot T_0^2/|\beta_2| = \gamma\cdot W_0\cdot T_0/(2|\beta_2|),\ L_{NL} = 1/(\gamma P_0),$$

где W_0 – энергия солитона N-го порядка, L_{NL} – нелинейная длина ОВ.

В процессе распространения солитона в ОВ с коэффициентом затухания α его энергия уменьшается и солитон разрушается, преобразуясь в обычный импульс, подверженный дисперсионным искажениям. ВОСС, в которых энергия солитонов поддерживается на необходимом уровне с помощью ОУ, называют солитонными системами с управлением потерями.

Возможны два способа поддержания солитонного режима, которые реализуются установкой дискретных ОУ через некоторое расстояние Z_A или использованием распределенного усиления в ОВ, например, с помощью вынужденного комбинационного рассеяния (ВКР) Рамана. При этом источники накачки устанавливаются через расстояние Z_A [2, 3].

Учитывая, что фундаментальный солитон возникает при условии $L_D = L_{NL}$, будем характеризовать влияние потерь в ОВ на режим работы солитонной ВОСС безразмерным параметром Γ, характеризующим потери на дисперсионной длине L_D:

$$\Gamma = 0.5\cdot\alpha\cdot L_D.$$

В первом приближении мы можем полагать, что фундаментальные солитоны могут существовать в ОВ, если [3] $\Gamma < 1$.

На рис. 1 приведены результаты расчетов пиковой мощности P_0 для возникновения фундаментальных солитонов секансной формы и параметра затухания Γ на дисперсионной длине для двух типов ОВ: стандартного (SF) и со смещенной дисперсией (DSF). Параметры этих ОВ на длине волны 1550 нм приведены в таблице 1 [1].

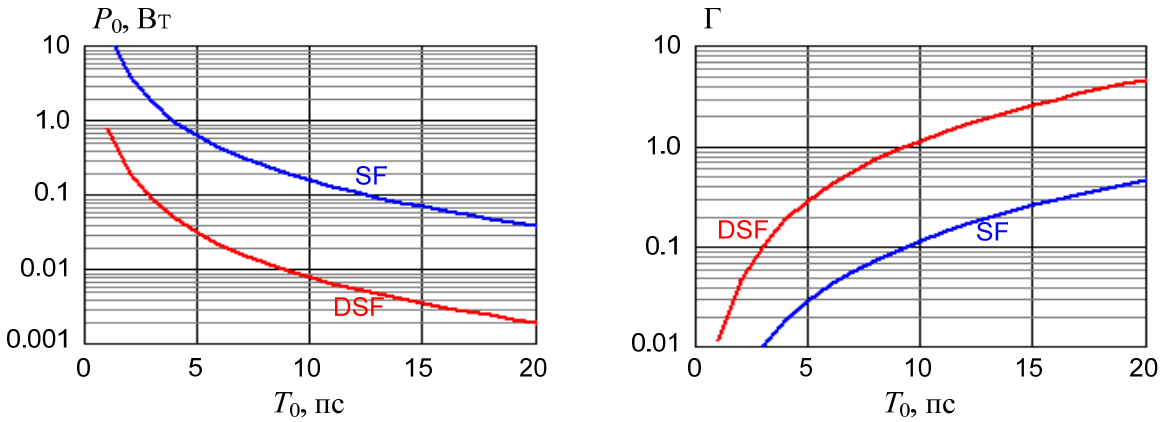


Рис. 1. Результаты расчетов зависимостей P_0 (а) и Г (б) на дисперсионной длине от полуширины секансного импульса

ТАБЛИЦА 1. Параметры ОВ

№	Параметр	SF	DSF
1	Хроматическая дисперсия, пс / (нм·км)	15,7	1,57
2	Коэффициент нелинейности, $Вт^{-1}\cdot км^{-1}$	1,25	2,5
3	Коэффициент затухания, $км^{-1}$ (дБ/км)	0,046 (0,2)	0,046 (0,2)

Рассмотрим квазисолитонную ВОСС, которая состоит из большого количества УУ, каждый из которых содержит ОВ длиной $Z_A < L_D$ и дискретный ОУ. В [3] показано, что форма и длительность солитона в ОВ на УУ слабо меняется, а пиковая мощность меняется существенно. В этом случае можно заменить пиковую мощность $P(Z)$ на ее среднее значение

$$\overline{P} = P_{0e} \cdot z_A^{-1} \cdot \int_0^{z_A} exp(-2 \cdot \Gamma \cdot z) \cdot dz = P_{0e} \cdot \overline{p},$$

где $z_A = Z_A / L_D$ – нормированная длина УУ, P_{0e} – пиковая мощность на входе в ОВ, которая должна быть больше P_0 в $1/\overline{p}$ раз.

Установив коэффициент усиления ОУ $G = \exp(2\Gamma \cdot z_A)$, определим коэффициент увеличения пиковой мощности на входе в ОВ солитона с управляемыми потерями по выражению

$$K_e = P_{0e}/P_0 = 1/\overline{p} = 2 \cdot \Gamma \cdot z_A / [1 - exp(-2 \cdot \Gamma \cdot z_A)] = G \cdot ln(G)/(G-1).$$

Было проведено моделирование квазисолитонной ВОСС со скоростью B = 10 Гбит/с в ОВ DSF. Были рассчитаны пиковая мощность P_0 = 8 мВт и полуширина солитонного импульса T_0 = 10 пс, что соответствует рекомендуемой для солитонных импульсов скважности q_0 = 5. Расстояние между ОУ было выбрано равным Z_A = 40 км (Γ = 0.8 и L_D = 50 км). Были рассчитаны

коэффициент усиления ОУ $G = 8$ дБ, коэффициент $K_e = 2{,}19$ и пиковая мощность на входе P_{0e} = 17 мВт. На рис. 2 показаны входные (комбинация 010110) и выходные импульсы после прохождения 400 км (10 УУ). Солитонный режим практически сохраняется.

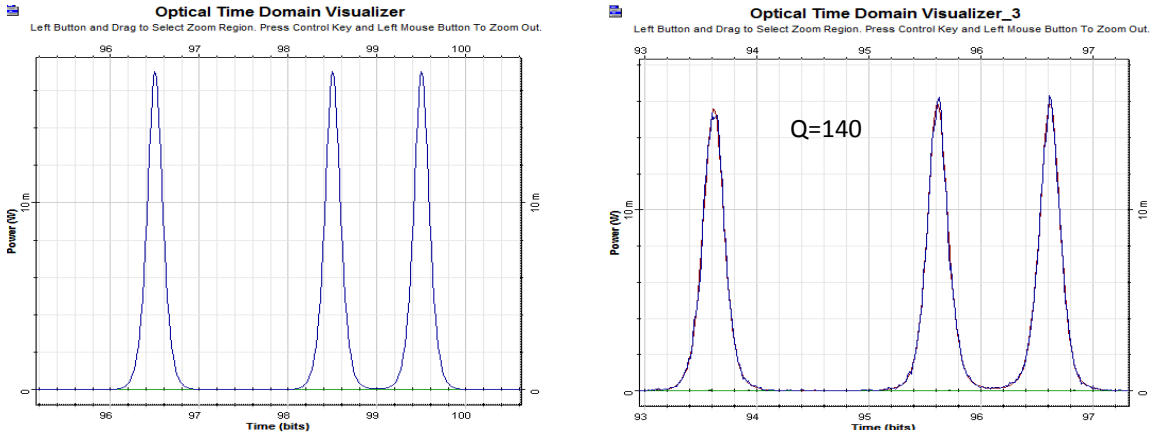


Рис. 2. Входные (а) и выходные оптические импульсы (б) в солитонной ВОЛС

Рассмотрим солитонную ВОСС с распределенным усилением. Запишем уравнение описывающее изменение пиковой мощности P в ОВ обладающим усилительной способностью $g(Z)$

$$dP/dZ = \left[g(Z) - \alpha\right] \cdot P \,. \tag{1}$$

Если $g(Z)$ постоянна и равна α для любых Z, пиковая мощность и энергия солитона остаются постоянными вдоль ОВ. Это полностью соответствует ОВ без потерь. Практически распределенное усиление реализуется периодическим введением накачки в телекоммуникационное ОВ. Т. к. мощность накачки не сохраняется из-за потерь в ОВ и ее истощения, $g(Z)$ зависит от Z. Однако, хотя потери в ОВ нельзя компенсировать в каждой точке, возможна общая компенсация на расстоянии Z_A между ОУ при условии [3]:

$$\int_0^{Z_A} g(Z) \cdot dZ = \alpha \cdot Z_A \,.$$

Для распределенного ВКР усиления обычно используют встречную или двунаправленную накачки. Если пренебречь истощением накачки, то для $g(Z)$ в (1) можно записать (α_p – коэффициент затухания ОВ для накачки):

встречная:
$$g(Z) = g_0 \cdot exp\left[-\alpha_p \cdot (Z_A - Z)\right], \tag{2}$$

двунаправл.:
$$g(Z) = g_1 \cdot exp\left(-\alpha_p Z\right) + g_2 \, exp\left[-\alpha_p (L_A - Z)\right], \tag{3}$$

где g_0, g_1 и g_2 связаны с мощностями источников накачки. Запишем нормированные решения уравнения (1) с учетом (2) для встречной и с учетом (3)

для двунаправленной накачек, обеспечивающие на выходе ОУ пиковую мощность фундаментального солитона P_0 [3] (g_0, g_1 и g_1 выбраны так, чтобы $p(Z_A) = 1$ для обеих схем) [3]:

$$p(Z) = P(Z)/P_0 = exp\{\alpha \cdot Z \cdot [exp(\alpha_p Z - 1)/exp(\alpha_p Z_A - 1)] - \alpha \cdot Z\},$$

$$p(Z) = \frac{P(Z)}{P_0} = exp\left\{\alpha \cdot Z_A \cdot \left[\frac{sh[\alpha_p \cdot (Z - Z_A/2)] + sh(\alpha_p \cdot Z_A/2)}{2 \cdot sh(\alpha_p \cdot Z_A/2)}\right] - \alpha \cdot Z\right\}.$$

На рис. 3 показаны нормированные зависимости пиковой мощности $p(Z)$ вдоль ОВ при L_A = 40 км, α = 0,2 дБ/км, α_p = 0,25 дБ/км.

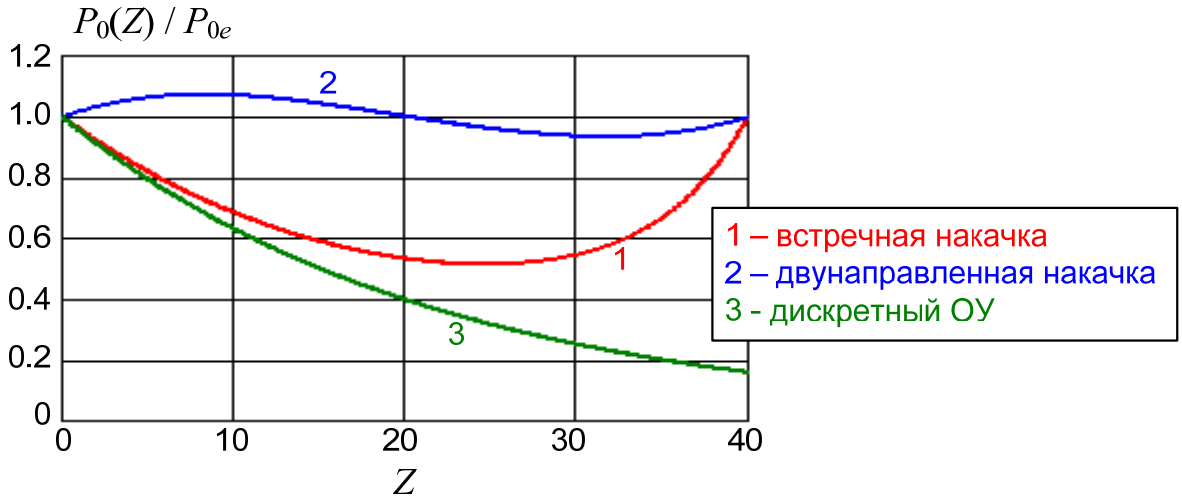


Рис. 3. Нормированные изменения пиковой мощности в пределах УУ

Изменения пиковой мощности на УУ не превышают 50 % при встречной и 10 % при двунаправленной накачке. Для сравнения показано изменение пиковой мощности при использовании дискретных ОУ, которое показывает несомненное преимущество солитонных ВОСС с распределенным управлением потерями.

Список используемых источников

1. Листвин В. Н., Трещиков В. Н. DWDM – системы. М. : Техносфера, 2017. 352.с.
2. Агравал Г. Нелинейная волоконная оптика. М. : Мир, 1996. 323 с.
3. Кившарь Ю. С., Агравал Г. П. Оптические солитоны. От волоконных световодов до фотонных кристаллов. М. : Физматлит, 2005. 648 с.

УДК 654.9

ВОЛОКОННО-ОПТИЧЕСКАЯ СИСТЕМА ВИДЕОНАБЛЮДЕНИЯ ПРОИЗВОДСТВЕННОГО ОБЪЕКТА: ФУНКЦИИ ОХРАНЫ И ТЕХНОГОЛИЧЕСКОГО КОНТРОЛЯ. ЧАСТЬ 1. АКТИВНОЕ ОБОРУДОВАНИЕ

Е. И. Андреева[1], В. Д. Купцов[2], В. П. Валюхов[2]

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

Разработан, исследован и конструктивно исполнен комплект модулятора и демодулятора с использованием частотной модуляции оптического сигнала для пассивных оптических систем передачи изображения. Реализован волоконно-оптический канал передачи полного цветового высококачественного телевизионного изображения со звуковым сопровождением. Построена разветвленная волоконно-оптическая сеть видеонаблюдения, выполняющая функции управления технологическими процессами и охраны складских и производственных подразделений.

охранные системы, видеосистемы.

На сегодняшний день потребность в системах видеонаблюдения является одной из самых актуальных для большинства предприятий [1, 2, 3]. При большом выборе аппаратных и программных решений, физической среды передачи видеосигнала возникает резонный вопрос, что же выбрать, ведь у продуктов различные функциональные возможности и стоимость. Подходы к построению современной системы видеонаблюдения могут быть различными, но одно можно сказать с уверенностью: не зависимо от масштаба объекта, она должна соответствовать главному критерию – это надежность системы в целом. Задача обеспечения надежности разбивается на два аспекта. Во-первых, техническое решение. Максимальную защищенность от несанкционированного доступа, защиту от электромагнитных помех, максимальную дальности и скорость передачи информации обеспечивают оптические системы [4, 5, 6, 7]. Во-вторых, компонентная база отечественного производства. Рабочие параметры как самого оптического кабеля, так и модемов, соединительного оборудования приближены к условиям эксплуатации в нашем регионе.

Система безопасности предприятия разрабатывается и создается как часть информационной инфраструктуры, а, следовательно, подчиняется тем же законам. Инвестиции в информационную инфраструктуру относятся

к разряду долгосрочных, поэтому при ее проектировании выбираются наиболее передовые технологии, дающие экономический эффект в расчете на многолетнюю эксплуатацию.

Активное оборудование для передачи видеосигнала по оптическому кабелю

Большинство видеомодемов широкого применения используют амплитудную модуляцию оптического сигнала. Их преимущество в относительно низкой стоимости. Однако для достижения высокой надежности передачи сигнала и его стабильности в условиях электромагнитных помех предпочтительно использование частотной модуляции.

Волоконно-оптический канал передачи полного цветового высококачественного телевизионного изображения со звуковым сопровождением с использованием частотной модуляции (ЧМ) состоит из блоков модулятора, волоконно-оптического кабеля и демодулятора. Структурная схема модулятора представлена на рис. 1.

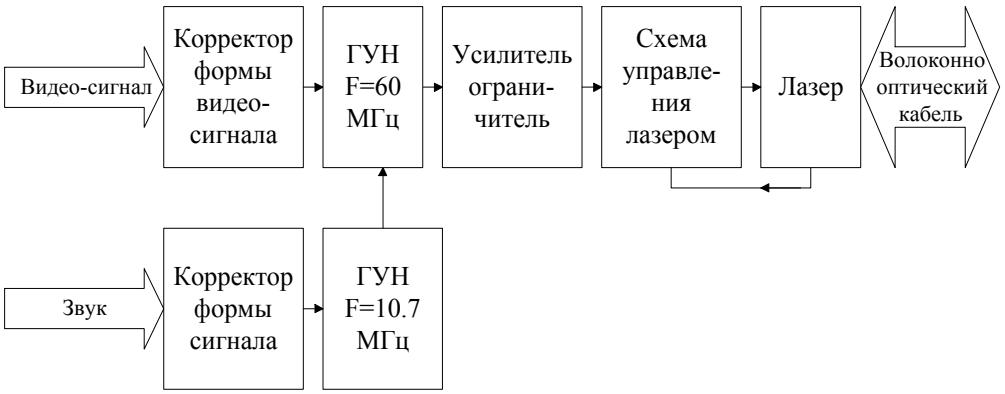


Рис. 1. Структурная схема модулятора

В состав модулятора сигнала изображения входят корректор формы видеосигнала, генератор высокой частоты, управляемый напряжением, усилитель-ограничитель уровня сигнала, схема управления полупроводниковым лазером и источник оптического излучения (лазер или светодиод). Сигнал звукового сопровождения через корректор формы сигнала поступает на генератор, управляемый напряжением, в котором осуществляется частотная модуляция сигнала на частоте поднесущей звука 10,7 МГц.

Корректор формы видеосигнала вносит низкочастотные предискажения и одновременно служит для устранения влияния высокочастотных помех на работу генератора управляющего напряжения (ГУН). ГУН канала звукового сопровождения формирует частотно-модулированный сигнал на поднесущей звука. Значение частоты поднесущей звука определяется гармониками цветовых поднесущих видеосигнала и принята равной 10,7 МГц.

Девиация частотно-модулированного сигнала звукового сопровождения составляет 50 кГц. Частотно-модулированный сигнал звукового сопровождения суммируется с видеосигналом на входе ГУН ТВ-сигнала. ГУН представляет собой быстродействующий мультивибратор, управляемый током. Несущая частота составляет 60 МГц, девиация частоты 30 МГц. Усилитель-ограничитель уровня служит для уменьшения амплитудных искажений частотно-модулированного сигнала. Схема управления лазерным диодом служит для устранения влияния температуры и срока службы на выходные характеристики излучателя. Входной сигнал для схемы управления снимается с фотодиода обратной связи. Ток фотодиода, пропорциональный выходной оптической мощности излучателя, после усиления и преобразования позволяет поддерживать уровень выходной мощности стабильным.

В качестве источника оптического излучения в волоконно-оптическом канале применяется полупроводниковый лазер. Выходная оптическая мощность при токе смещения 30 мА составляет величину порядка 1 мВт. Рабочая длина волны оптического излучения равна 1,3 мкм. Лазерные источники позволяют увеличить дальность передачи сигнала до 10 км. В качестве дополнительного варианта возможно применение светодиодных излучателей (длина волны оптического измерения 0,85 мкм и 1,3 мкм). Светодиодные излучатели используются в волоконно-оптических линиях небольшой протяженности (до 6 км) и способны обеспечить более долгий срок службы.

Структурная схема демодулятора волоконно-оптического канала передачи ТВ-сигнала представлена на рис. 2.

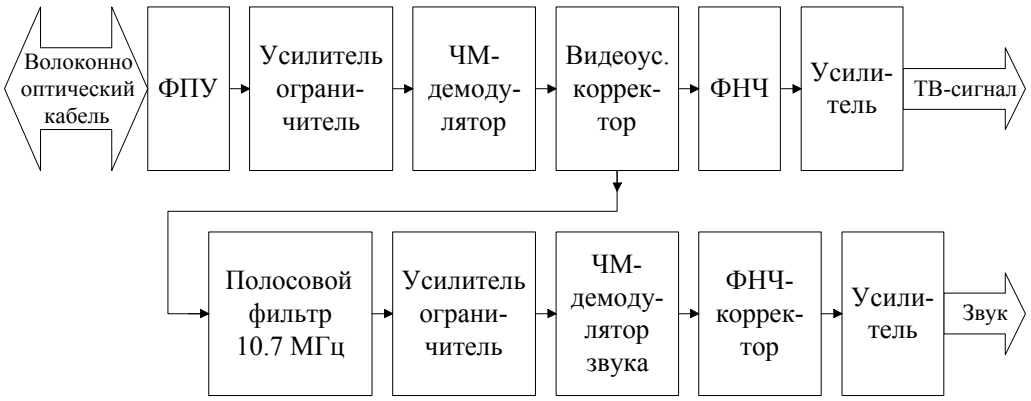


Рис. 2. Структурная схема демодулятора волоконно-оптического канала передачи ТВ-сигнала

Внешний вид аппаратурных блоков модема представлен на рис. 3.

Основные характеристики модема ОМД-1:

- модуляция видео сигнала при передаче – частотно-импульсная;
- длина волны оптического излучения – 1,3 мкм;
- дальность передачи – 6 км (ММ волокно); 10 км (SM волокно);

– энергетический бюджет линии – 16 дБ;
– отношение сигнал/шум по видео сигналу – 60дБ;
– напряжение питания – +9В (нестабилизированное);
– ток потребления каждого блока – 250 мА;
– габаритные размеры (без источника питания) – 130×70×30 мм;
– температурный диапазон – (–25°С ÷ +55°С).

Подключение видеосигналов к блокам осуществляется через BNC-разъёмы, волоконно-оптического кабеля – через ST-разъём.

Рис. 3. Внешний вид аппаратурных блоков модема

Волоконно-оптический кабель, применяемый в канале связи, имеет потери (3–5) дБ/км на длине волны оптического излучения λ = 0,85 мкм и (0,5–0,8) дБ/км на длине волны 1,3 мкм. Мощность излучения полупроводникового лазера (λ = 1,3 мкм) при токе накачки порядка 30 мА составляет 1 мВт (0 дБм), чувствительность ФПУ-ВЧ по оптическому сигналу (0,7–1,5) мкВт (~30 дБм). Потери в волокне обеспечивают длину ретрансляционного участка оптической телевизионной связи до 40 км и выше. При использовании светоизлучающего диода на длине волны λ = 1,3 мкм длина ретрансляционного участка составляет ~6 км, что для большого числа практических приложений является достаточной величиной.

С использованием разработанных модемов на Череповецком сталепрокатном заводе (ЧСПЗ), входящем в холдинг «Северсталь», смонтирована волоконно-оптическая сеть видеонаблюдения, выполняющая функции управления технологическими процессами и охраны складских и производственных подразделений. Сеть охватывает производства комбината и его инфраструктуру. В рамках первого этапа на территории установлено 40 видеокамер.

Особенность описанной системы – исполнение на отечественной элементной базе. Не только модемы, кроссы, кабели и даже приборы для тестирования – все произведено в Санкт-Петербурге. Выбор обусловлен требованием надежности системы. Эксплуатация подтвердила качество установленного оборудования, удобство обслуживания, правильность технического решения. Позднее аналогичные видеомодемы были поставлены также на объекты специального назначения, в том числе в проекты, проводимые ФГУП ГКНПЦ имени М. В. Хруничева. Получены позитивные отзывы.

Список используемых источников

1. Андреева Е. И., Купцов В. Д., Валюхов В. П., Пономарев Л. В. Волоконная оптика в системах видеонаблюдения и охранной сигнализации // Сети. Network world. 2000. № 3.

2. Гришачев В. Фотоника в системах безопасности и защиты информации // Фотоника. 2011. № 6. С. 58–63.

3. Денисов В. И., Гришачев В. В., Косенко О. А. Волоконно-оптические технологии в системах безопасности и защиты информации // Специальная техника. 2010. № 4. С. 47–51.

4. Карпуков Л. М., Щекотихин О. В., Сметанин И. Н. Методы защиты информации в ВОЛС // Фотон-экспресс. 2009. № 4 (76). С. 34–35.

5. Кутурга В. В. Интеллектуальная система видеонаблюдения // Научное обозрение. Технические науки. 2017. № 1. С. 75–77.

6. Глущенко А., Глущенко Л., Тупота В. Оценка защищенности информации, циркулирующей в ВОЛП // Фотоника. 2010. № 4. С. 36–39.

7. Попова А. В., Тупота В. И. Методика обоснования требований по защите информации, циркулирующей в волоконно-оптических системах передачи данных// Телекоммуникации. 2009. № 11. С. 24–27.

УДК 654.9

ВОЛОКОННО-ОПТИЧЕСКАЯ СИСТЕМА ВИДЕОНАБЛЮДЕНИЯ ПРОИЗВОДСТВЕННОГО ОБЪЕКТА: ФУНКЦИИ ОХРАНЫ И ТЕХНОЛОГИЧЕСКОГО КОНТРОЛЯ. ЧАСТЬ 2. ТЕСТИРОВАНИЕ

Е. И. Андреева[1], В. Д. Купцов[2], В. П. Валюхов[2], В. Р. Сумкин[1]

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

Тестирование - один из наиболее важных вопросов при обслуживании разветвленной волоконно-оптической сети. На примере построенной волоконно-оптической системы, позволяющей осуществить надежное наблюдение территории распределенного объекта, в том числе условиях высоких электромагнитных помех, рассмотрены особенности и возможности мониторинга системы с помощью приборов с расширенными возможностями.

охранные системы, видеосистемы, оптические измерительные приборы.

Системы видеонаблюдения и охранной сигнализации предполагают большое количество сравнительно коротких сегментов оптического кабеля. Обслуживание таких сетей имеет свои особенности [1]. Разветвленный характер кабельной разводки делает ее уязвимой для повреждения. Перебои в работе системы могут приводить к серьезным потерям. Поэтому такие сети требуют регулярного технического обслуживания, оперативного выявления проблем и их быстрого устранения.

Система видеонаблюдения объекта

Структурная схема сети предприятия представлена на рис. 1. Сеть охватывает производства комбината и его инфраструктуру. Основными сегментами сети являются производственные подразделения и охрана периметра территории. Каждый их этих сегментов имеет свой диспетчерский пункт, на который подаются сигналы с точек видеонаблюдения. Все видеокамеры обладают повышенной четкостью и чувствительностью, снабжены объективами с автодиафрагмами со средними значениями углов обзора от 60° до 90°.

Рис. 1. Структурная схема сети производственного предприятия

Базовая часть системы видеонаблюдения построена по топологии звезда. Волоконно-оптические линии сведены к Единому Центру Управления технологическими процессами и обеспечения безопасности комбината. Видеосигналы поступают в центр с основных производств и охраняемых объектов – складов, проходных, хранилищ – всего по десяти направлениям. По территории комбината трассы проложены многожильным волоконно-оптическим кабелем, преимущественно бронированным. На длинных участках смонтированы соединительные короба для проведения дальнейшей модернизации сети и оперативного ремонта в случае повреждения кабеля. Общее количество волоконно-оптических ТВ линий – 57, из них 17 относятся к местным сетям управления производством.

Протяженности трасс варьируются от 200 метров до 1,2 км. Суммарная длина волокна в сети ~26 км. Предусмотрено ограниченное количество резервных волокон с целью повышения живучести системы. Оптические сигналы поступают в Единый Центр на демодуляторы ОД-1, в которых преобразуются в электрическую форму. Сгруппированные по функциональному признаку телевизионные изображения поступают на 9-ти канальные детекторы выделения движения в кадре. В нерабочее время устанавливается режим «охрана» – в этом режиме детектор движения выдает сигнал тревоги при наличии перемещений в зоне наблюдения любой из видеокамер. По сигналу тревоги автоматически на экран монитора с большим экраном выводится видеоизображение камеры в зоне нарушения крупным планом. Одновременно подается звуковой сигнал тревоги. Видеоизображение демонстрируется на экранах отдельных мониторов одновременно. Один монитор имеет больший размер экрана (25 дюймов) и служит для детального визуального рассмотрения зоны, в которой замечен несанкционированный доступ. Данная система позволяет осуществить надежное наблюдение территории объекта с учетом любой возможности проникновения на объект через имеющиеся пути доступа.

Тестирование

Обслуживание таких систем предполагает в первую очередь их тестирование [1]. Для этих целей используются обычно оптические тестеры, рефлектометры и визуальные локаторы дефектов [1, 2, 3]. Преимущество оптического тестера – его цена. Обслуживающий персонал может иметь эти приборы в нужном количестве. Обычно измерения тестером проводятся с двух сторон линии: на одном конце подключается источник, а на втором – приемник. Возможны измерения методом шлейфа: попарная коммутация световодов на втором конце линии и измерение суммарных потерь с одной стороны. Тестер позволяет определить затухание сигнала в действующей

линии, но не может помочь в случае обрыва. Задача поиска места повреждения кабеля предполагает использование рефлектометра. Это прибор существенно более дорогой и не всегда «под рукой».

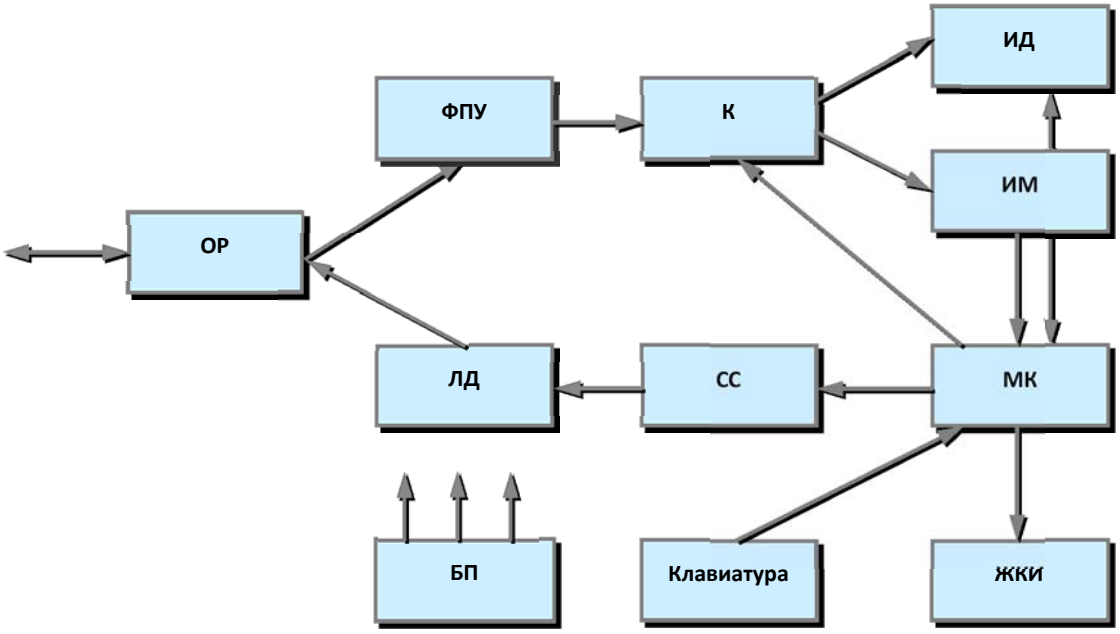


Рис. 2. Функциональная схема тестера РУБИН 501. Элементы конструкции: ФПУ – фотоприемное устройство, МК – микроконтроллер, К – коммутатор, ОР –оптический разветвитель, ЛД – лазерый диод, ИД – измеритель длины волоконного световода, ИМ – измеритель мощности, СС – схема стабилизации, БП – блок питания, ЖКИ – жидкокристаллический индикатор

Большинство вопросов удается решить использованием прибора «Рубин 501», совмещающего в себе функции оптического тестера и измерителя длины линии [2]. Как измеритель прибор может использоваться как «классический» тестер. Основное его преимущество – дополнительные функции, в первую очередь – измерение длины линии и контроль уровня потерь в ней с одного конца. Функциональная схема тестера «Рубин 501» приведена на рис. 2. Прибор может работать в непрерывном и импульсном режиме. Предположим, проводится плановая проверка системы и карта – схема этой сети есть. Включая непрерывный режим работы, используем «Рубин-501» для измерения затухания. Учитываем, что при малых длинах оптического кабеля основные потери вносят соединения отдельных сегментов, они же и фактор риска, требующий обслуживания. Прибором можно проводить измерения потерь как в абсолютных, так и в относительных единицах, при этом результат измерений – суммарные потери на входном и выходном концах. Важно, что тестирование проводится с одной стороны линии. Результат – проверка соответствия паспортным данным. Если полученные результаты значительно превосходят исходные, требуется или чистка разъемов, или замена соединительных шнуров. Второй – импульсный – режим

используется для определения длины участка линии. Если полученное значение соответствует паспортному, переходим к следующему сегменту. В противном случае прибор покажет расстояние до обрыва или ближайшего к метрологу поврежденного участка. Диапазон измерений по длине от 2 метров до10 км. В отличие от оптического рефлектометра нет «картинки» тестируемой трассы, но самые необходимые параметры прибор позволяет определить. Внешний вид прибора представлен на рис. 3.

Для экспресс-анализа целостности линии применяется визуальный локатор дефектов (рис. 3). Модель ОТМ-1 снабжена двумя выходами, один из которых работает в непрерывном, а второй – в импульсном режиме. При засветке сразу двух волокон на входе линии удается идентифицировать их с другой стороны. Если же произошел обрыв, импульсным сигналом зачастую легче его идентифицировать. Мощность сигнала 2 мВт, что достаточно для тестирования линий до 8 км.

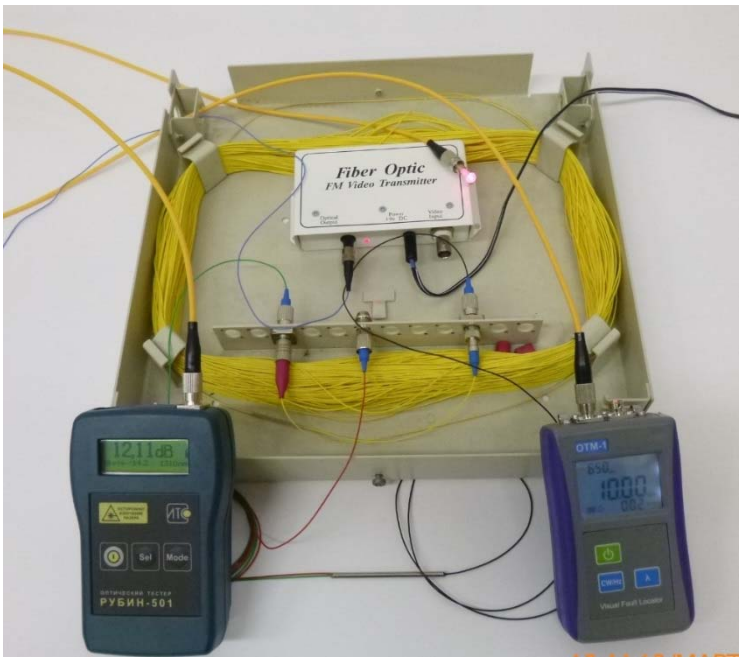


Рис. 3. Тестер оптический «Рубин 501» и визуальный локатор дефектов «ОТМ 1»

Заключение

Таким образом проработана методика оперативного тестирования распределенной волоконно-оптической сети видеонаблюдения промышленного предприятия. Подобраны измерительные приборы, позволяющие точно и быстро проводить контроль параметров системы. Приборы прошли апробацию при прокладке новых сетей широкого доступа в северо-западном регионе, в частности, в рамках проекта «Безопасный город», где длина отдельных сегментов одномодовой оптической сети варьировалась от нескольких сотен метров до единиц километров. Приборы, включая «Рубин

501», внесены в единый Госреестр измерительных инструментов для оптических кабельных систем, имеют гарантию отечественного производителя.

Список используемых источников

1. Рудницкий В. Б., Сумкин В. Р., Салтыков А. Р. Тестирование абонентского участка PON // Фотон- Экспресс. 2013. № 5.

2. www.fibertest.ru

3. Купцов В. Д., Валюхов В. П. Чувствительность фотоприемных устройств волоконно-оптических линий связи // Научно-технические ведомости СПбГПУ. 2010. Т. 113. № 6. С. 31−37.

4. Андреева Е. И., Сергеев А. Н. Измерители мощности для волоконно-оптических систем // Мир связи Connect. 2001. № 10. С. 78–83.

УДК 621.391

5G ГРАНИЧНЫЕ ВЫЧИСЛЕНИЯ НА БАЗЕ D2D КОММУНИКАЦИИ

А. А. Атея, А. С. Мутханна, М. И. Филимонова

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

Динамичное развитие беспроводных технологий и увеличивающиеся объемы трафика создают предпосылки для создания все новых стандартов связи. В настоящее время широкое обсуждение получает разработка мобильной системы 5G. Для реализации этой системы необходимы, помимо высокой надежности и хорошего качества связи, сверхмалая задержка и высокая пропускная способность, а также улучшение охвата сигнала. Предлагается использовать технологию MEC, подразумевающую перенос вычислительных ресурсов стационарного облака на границу сети радиодоступа. Это увеличит пропускную способность облака и обеспечит разгрузку сети. Также предлагается использовать D2D-коммуникацию, что положительно скажется на развитии IoT. Кроме того, перспективным считается использование туманных вычислений, в которых некоторые задачи стационарных облаков передаются в обработку на облачко (cloudlet), являющееся рядовым пользовательским интерфейсом. Данная технология позволит увеличить скорость принятия решений системой.

облако, туманные вычисления, структура.

Введение

5G – технология мобильной связи, а туманные вычисления – распределенная вычислительная инфраструктура, способная обрабатывать миллиарды подключенных к Интернету устройств [1]. Поэтому комбинируя

туманные вычисления с 5G, мы представляем новый и эффективный динамический механизм маршрутизации с использованием облачных вычислений для решения проблемы энергосбережения разрывов каналов. Для каждого мобильного устройства мы создаем временный файл для записи его идентификационной информации и информации маршрута в определенное время. Кроме того, в качестве многообещающей технологии 5G используется D2D-коммуникация в качестве способа связи между мобильными устройствами [2], поскольку она может улучшить способность обмена информацией между мобильными устройствами. Облака можно рассматривать как небольшие центры данных, и мы создаем таблицу отношений обмена данными и механизм сотрудничества между облаками (рис. 1). Затем, опираясь на них, мобильные устройства могут быстро маршрутизировать и искать запрошенные услуги независимо от частого перемещения мобильных устройств. Экспериментальные результаты показывают, что облако может сэкономить большой объем времени и энергии по сравнению с стандартной моделью сети, следовательно, облако сможет предоставлять услуги, которые актуальны для будущих приложений мобильной сети.

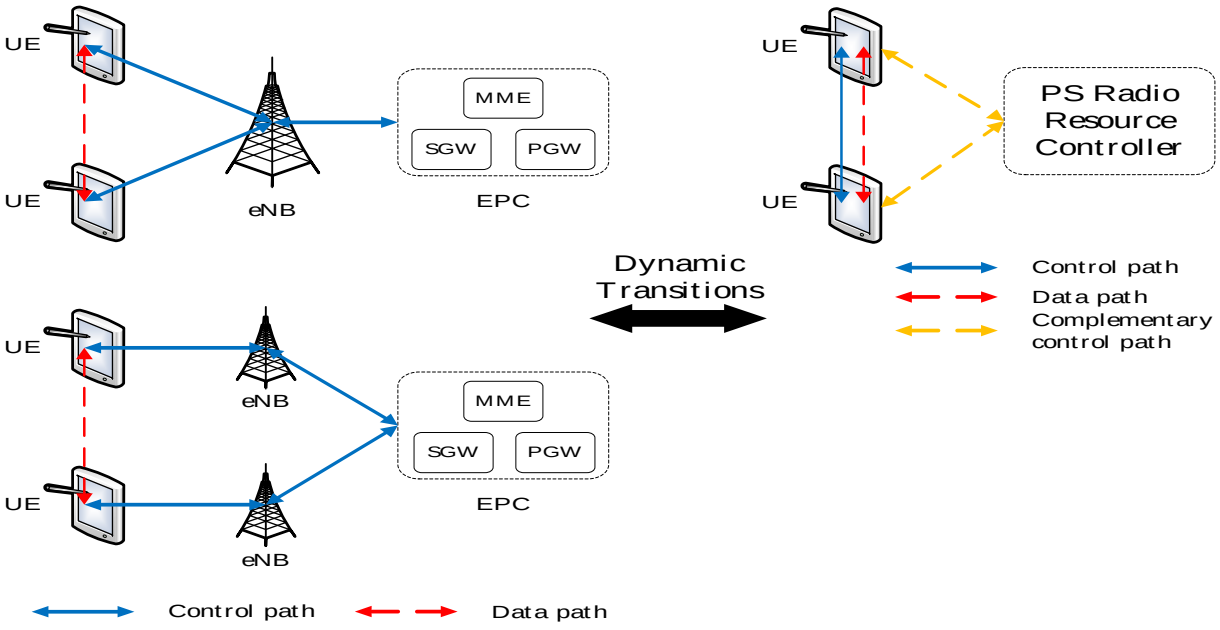


Рис. 1. Взаимодействие D2D-коммуникации

Вопрос энергопотребления стал по-настоящему актуален в XXI веке. Все чаще предлагается реализовывать «зеленые» системы связи, поскольку с развитием уровня жизни населения увеличивается количество затрат на энергопотребление сети в каждой стране. Энергопотребление сети связи представляет собой большой счет расходов на сетевые операции. Поэтому из-за экономических и экологических причин необходимо создать системы

связи, которые будут мощнее, но при этом будут энергосберегающими. Требование имеет важное значение для беспроводных сетей связи, и некоторые новые системы беспроводной связи должны быть разработаны или улучшены.

Архитектура граничных вычислений на базе D2D-коммуникации

В последние годы появились новые модели, такие как 5G и туманные вычисления, решающие две проблемы энергосбережения. D2D-коммуникация – это технология передачи данных с малой дальностью передачи, основанная на сотовой системе, которая имеет потенциал для улучшения производительности системы, улучшая работу пользователей, уменьшая нагрузку базовой станции и улучшая использование частотного спектра. В будущих сетях 5GD2D является одной из ключевых технологий, которые могут быть развернуты как в разрешенных полосах частот, так и в нелицензированных полосах частот. Таким образом, 5G сделает технологию D2D высоко применимой, поскольку D2D может улучшить связь между узлами и помочь уменьшить задержки. Таким образом, как D2D, так и облака могут обеспечить лучшую приводит к с точки зрения энергосберегающего эффекта, чем облако.

В этой статье мы предлагаем архитектуру разгрузки задач в туманных вычислениях, где пользователи устройств имеют гибкость в выборе нескольких вариантов выполнения задачи, в том числе локальное мобильное исполнение, Device-to-Device (D2D) [3], и выгрузку в облако (рис. 2).

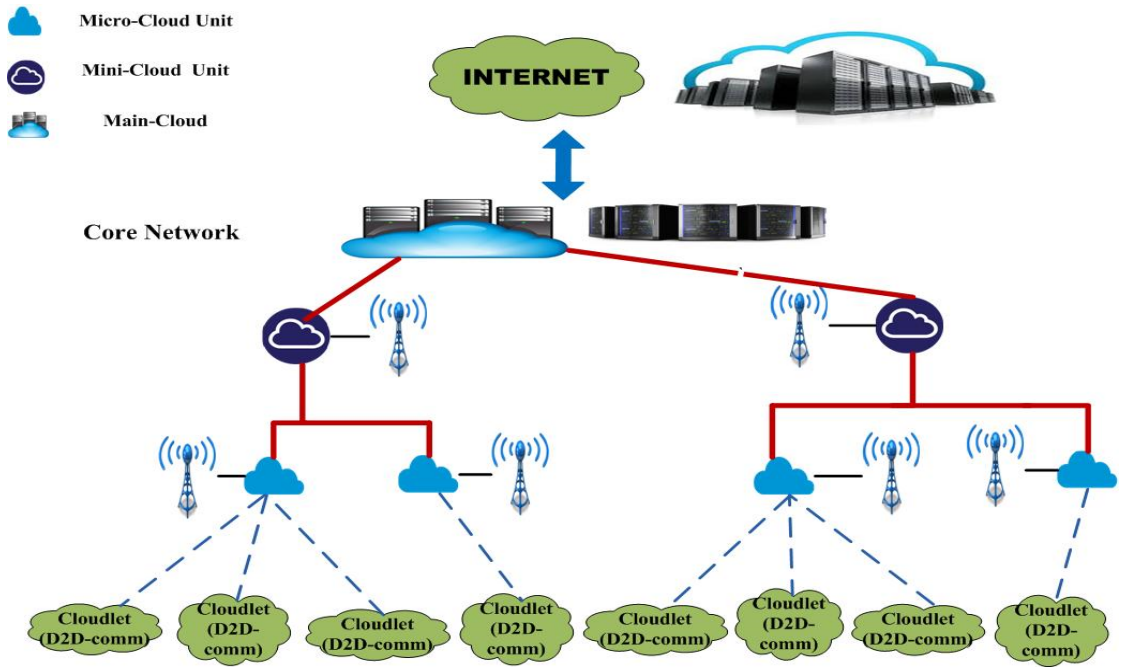


Рис. 2. 5G на основе D2D-коммуникации и многоуровневых облачных модулей на границе сети

Поскольку смартфоны набирают огромную популярность, многие новые мобильные приложения, такие как распознавание лиц, естественный язык обработки, интерактивные игры и VR привлекают все больше внимания. Этот вид мобильных приложений, как правило, ресурсоемкий и требует интенсивных вычислений и высокое потребление энергии. В связи с ограничением физического размера мобильные устройства в целом ограниченны по ресурсам и временем автономной работы. В качестве интересного и перспективного решения для разгрузки сети, выгрузка задачи стала ключевой задачей как в академических кругах, так и в промышленности. В последнее десятилетие многие исследователи сосредоточены на мобильных облачных вычислениях [4, 5], где мобильные пользователи могут решать вычислительные задачи для удаленных облаков через беспроводной доступ. Хотя эта парадигма уже используется как форма коммерческих облачных сервисов, таких как WindowsAzure, она часто страдает от типичных проблем беспроводных соединений (например, слабый сотовый сигнал) и задержки глобальной сети между мобильными устройствами и облаками. Мобильные граничные вычисления являются возникающей парадигмой, которая использует множество совместных конечных пользователей и устройств, работающих поблизости, для осуществления существенного количество задач вычисления. Поскольку Fog-вычисления реализованы на краю сети, это может обеспечивать малую задержку, а также гибкое вычисление, дополняющее услуги для пользователей устройств.

D2D-коммуникации, поскольку устройства в непосредственной близости на краю сети, могут выгодно делиться вычислительными ресурсами между собой путем разгрузки задачи;

Облако, где его выгрузка представляет собой мощную вычислительную способность: с помощью мобильного облака, можно увеличить производительность разгрузки задачи;

Локальное мобильное исполнение, в котором пользователь устройства может также выбрать выполнение задачи локально на своем мобильном устройстве, чтобы избежать чрезмерных накладных расходов в вопросах разгрузки (рис. 3).

Предположим, что устройства B и C хотели бы выполнить вычислительная задача (например, сжатие видео), в то время как в настоящее время их ресурсы ЦП сильно заняты другими приложениями. Поскольку устройство B имеет плохую сотовую связь, в этом случае устройство B может решить разгрузить свою задачу через высокопроизводительная D2D-связь с ближайшим устройством A, которое обладает большим количеством незанятых ресурсов ЦП для облегчения выполнение задачи. Для устройства C, поскольку он имеет хороший сотовый соединение, в этом случае он может выбрать разгружать свою задачу на облако через сотовую связь для ускорения выполнения задачи.

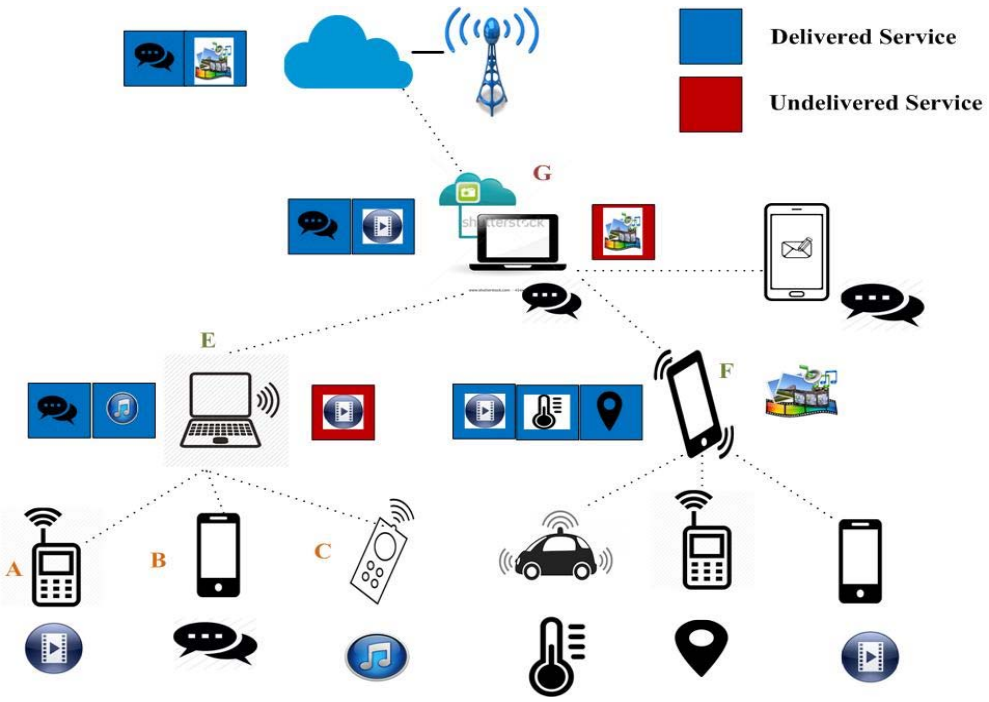


Рис. 3 Пример применения архитектуры

Заключение

В этой статье мы предложили схему разгрузки гибридных задач в туманных вычислениях, что обеспечивает гибкость локального мобильного исполнения, выгрузку с устройства на устройство (D2D), и облако, выгружающее выполнение задач. Мы также разработали трехслойный алгоритм сопоставления графов для эффективной гибридной выгрузки задачи и решили проблему минимизации общей стоимости выполнения задачи, переведя ее в минимизацию пути в построенном трехслойном графе.

Список используемых источников

1. Бородин А. С., Кучерявый А. Е. Сети связи пятого поколения как основа цифровой экономики // Электросвязь. 2017. № 5. С. 45–49.

2. Muthanna A., Masek P., Hosek J., Fujdiak R., Hussein O., Paramonov A., Koucheryavy A. Analytical Evaluation of D2D Connectivity Potential in 5G Wireless System // Lecture Notes in Computer Science. 2016. Vol. 9870. pp. 395–403.

3. Ateya A., Muthanna A., Gudkova I., Abuarqoub A., Vybornova A., Koucheryavy A. Development of intelligent core network for tactile internet and future smart systems // Journal of Sensor and Actuator Networks. 2018. 7. № 1. PP. 1.

4. Филимонова М. И., Мутханна А. С. А., Атея А. А. Исследование облачных вычислений в сотовых сетях // Информационные технологии и телекоммуникации. 2017. Том 5. № 3. С. 45–59.

5. Masek P., Muthanna A., Hosek J. Suitability of MANET Routing Protocols for The Next-Generation National Security and Public Safety Systems // Lecture Notes in Computer Science . 2015. Т. 9247. pp. 242–253.

УДК 621.391

ИСПОЛЬЗОВАНИЕ ПОСЛЕДОВАТЕЛЬНОГО СТАТИСТИЧЕСКОГО АНАЛИЗА ДЛЯ ВЫДЕЛЕНИЯ СЕГМЕНТОВ ОБРАБОТКИ РЕЧЕВОГО СИГНАЛА

А. А. Афанасьев, Р. С. Власов

Академия Федеральной службы охраны Российской Федерации

Выделение сегментов обработки речевого сигнала, на основе последовательном статистическом анализе в сочетании с непараметрическими методами оценки плотности распределения вероятностей мгновенных значений отсчетов, позволяет наиболее полно использовать статистическую избыточность речи при ее низкоскоростном кодировании, за счет использования зависимостей в речевом сигнале, выявление которых затруднительно при обычно применяемых способах, в основе которых лежит допущение о нормальном законе распределения мгновенных значений отсчетов.

речевой сигнал, сегмент анализа, сонанта, критерий Акаике, критерий Вальда.

В настоящее время при разработке систем низкоскоростного речевого кодирования основным методом, лежащим практически в основе всех алгоритмов, является линейное предсказание. Фиксированная длительность сегментов обработки (20–30 мс), используемая в современных системах обработки речевого сигнала на основе линейного предсказания, имеет существенный недостаток, а именно наличие в речи гласных и согласных звуков (фонем), длительность которых значительно превышает принятую [1]. В связи с чем, возникает необходимость использования переменной длины сегмента анализа при обработке речи на таких фрагментах речи. При адаптивном изменении границ участка анализа речевого сигнала, количество наблюдаемых отсчетов, может принимать различные значения в зависимости от особенностей произносимой речи. Поэтому, для определения границы необходимо применять методы последовательной проверки статистических гипотез.

Исходя из вышеизложенного, для определения границы предлагается применять методы последовательной проверки статистических гипотез, суть которых сводится к определению т. н. «эффективных» и «абсолютно эффективных» выборок, при которых будет иметь место продолжение эксперимента, и как следствие увеличение набора отсчетов. При этом основная гипотеза имеет вид: $H_0 : (F(X,m) = F_0(X,m)$, альтернативная – $H_1 : (F(X,m) = F_1(X,m).$ Для проверки этих гипотез используется метод, основанный на последовательном критерии отношения вероятностей (критерий

Вальда). То есть вычисляется отношение вероятностей получения выборок (функций правдоподобия) на каждом этапе эксперимента. В данном случае, для более полного использования статистических зависимостей, в том числе распределённых по закону отличному от нормального. Функция плотности вероятности, необходимая для вычисления правдоподобия, оценивается методом непараметрического ядерного сглаживания Парзена [2]:

$$f_я(X) = \sum_{i=1}^{n} K\left[\frac{x - x_i}{h}\right], \quad (1)$$

где $f_я$ – ядерная оценка плотности, $K(u)$ – ядерная функция (окно), h – ширина окна, ($h = \frac{x_{\max} - x_{\min}}{m}$, m – количество окон сглаживания), x – среднее значение величины отсчетов в сегменте, x_i – текущее значение отсчета. В качестве ядерной функции используется гауссов профиль: $K(u) = \frac{1}{\sqrt{2\pi}} e^{\left(-\frac{u^2}{2}\right)}$ [3].

Количество окон сглаживания m для каждого начального сегмента анализа, напрямую зависящее от их ширины, является статистически обоснованным и определяется с помощью информационного критерия Акаике (AIC) [4], на основе оценённой по соотношению (1) кривой плотности вероятности, следующим образом:

$$m_{опт} = \arg\max_m \left[\ln\left(\prod_{i=1}^{n} f_0(x_i, m) \right) - m \right],$$

где f_0 – кривая плотности вероятности при справедливости гипотезы H_1.

Определенное таким образом, оптимальное число окон сглаживания используется и для оценивания кривой плотности распределения для вновь получаемого сегмента, при справедливости гипотезы H_0, на каждом этапе эксперимента f_1.

При каждом увеличении сегмента на величину 5 мс с принятием границы вблизи «нуля» (следующая стадия эксперимента), на основе вновь полученного набора отсчетов вычисляется статистика Вальда [5]:

$$\ln \frac{\prod_{i=1}^{n} f_1(x_i, m)}{\prod_{i=1}^{n} f_0(x_i, m)} = \ln\left(\prod_{i=1}^{n} f_1(x_i, m) \right) - \ln\left(\prod_{i=1}^{n} f_0(x_i, m) \right) = Z[X].$$

Расширение границы сегмента происходит при выполнении следующих условий:

$$\ln B\big|_{n<n'} < Z[X] < \ln A\big|_{n<n'} \quad (2)$$

$$Z[X] < \ln B\big|_{n<n'} \quad (3)$$

где n – общее количество отсчетов в анализируемом сегменте, n' – максимально возможное число отсчетов в сегменте.

Ограничительные константы α и β, определяются на основании ошибок первого α и второго β рода: $\ln A = \ln\frac{1-\beta}{\alpha}$; $\ln B = \ln\frac{\beta}{1-\alpha}$. На рис. 1 представлено поведение статистики Вальда $Z[X]$ при сдвиге сегмента анализа на 5 мс с принятием границы вблизи «нуля», относительно приходящего РС.

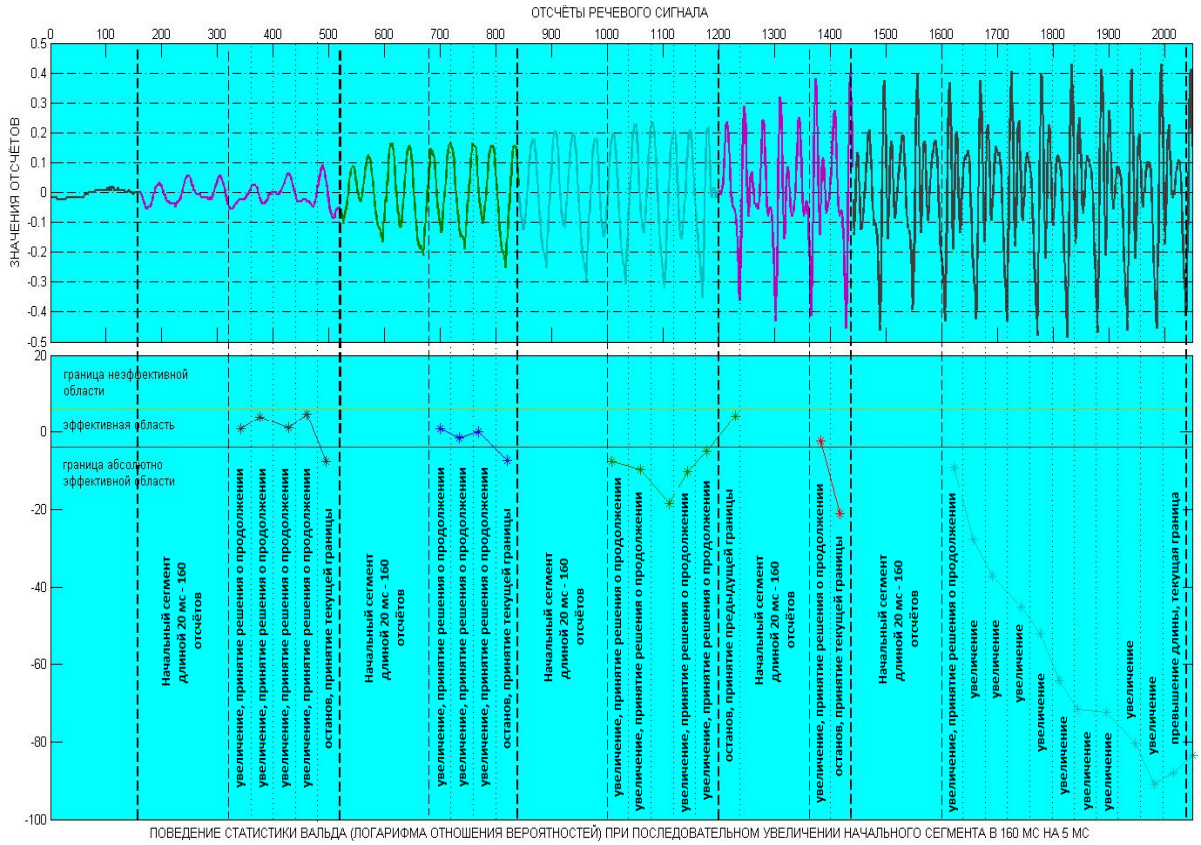


Рис. 1. Поведение функции отношения вероятности при анализе речевого сигнала

Анализ рис. 1 позволяет сделать вывод о том, что при расширении границ сегмента анализа на однородных (подобных) фрагментах РС значения статистики Вальда лежат в области либо принятия гипотезы H_0, либо продолжения эксперимента. Применительно к анализу речевого сигнала, принятие основной гипотезы также является признаком продолжения увеличения набора отсчётов. При этом в случае перехода от условия (2) к условию (3) граница сегмента сохраняется на данном этапе эксперимента. В случае же перехода от (3) к (2) граница сегмента определяется по данным предыдущего этапа эксперимента. Данный факт полностью соотносится с природой образования вокализованных и шумоподобных сигналов [6]. Максимально возможный сегмент одновременно анализируемых данных составляет 80 мс, что связано с требованиями по задержке РС при передаче,

определяемыми рекомендаций G.114 Международного союза электросвязи. Если на протяжении 80 мс не произошло перехода между областями, то расширение границы прекращается. Экспериментально установлено, что выполнение условия (2), соответствует переходному процессу при излучении так называемых *сонант*, – промежуточных между гласными и согласными звуков. В этом случае, при достижении 80 мс процесс заканчивается принятием основной гипотезы. Использование такого подхода к формированию сегментов обработки речи позволяет наиболее полно использовать статистическую взаимосвязь между случайными значениями РС для выделения сегментов анализа, имеющих одинаковую природу формирования в речевом аппарате человека. Оценка эффективности предложенного подхода выполняется на участках речевого сигнала, которые содержат сегменты со смешанным возбуждением, т. е. там, где распределение мгновенных значений речевого сигнала заведомо отличается от нормального. На остальных данный подход даёт схожий результат, что и способ выделения сегментов на основе анализа автокорреляционной функции [7]. В качестве оцениваемого параметра использовалось количество сегментов анализа, N одного и того же участка речевого сигнала после обработки его способом на основе последовательного статистического анализа, и способом на основе анализа корреляционных зависимостей. С учетом заявленной эффективности второго подхода по отношению к обычно применяемым способам с фиксированной длиной сегмента в 20 мс, и минимальной длительностью сонантных звуков в 60 мс, а также частотой появления сонант в речевом сигнале, было получено следующее соотношение для оценки эффективности предлагаемого способа:

$$\frac{N_{kor} - N}{N_{kor}} = \frac{9D}{8 + 4D} \times 100\% \qquad (4)$$

где N_{kor}, N – количество сегментов анализа, получаемых при использовании подхода на основе корреляционных зависимостей, и способа, с использованием последовательного статистического анализа, фрагмента речевого сигнала одинаковой длины, D – доля участков речевого сигнала со смешанным возбуждением (сонант).

Из статистических наблюдений звукового состава русской речи известно, что сонантные звуки занимают до 20,675 % – средние значения – от 0,635 % до 20,94 % (0,00635 до 0,2094)) русской речи [8]. Выражение (4), с учетом статистического распределения сонант в речи, дает множество значений выигрыша (кривую эффективности) от применения заявленного способа.

Таким образом, информация об эффективности рассматриваемого подхода включает в себя не только значение показателей выигрыша, но и мно-

жество значений вероятности достижения определенных значений эффективности. На рис. 2 изображен график значения показателя эффективности данного подхода. Анализ рис. 2 показывает, что с вероятностью 100 % достигается значение показателей эффективности функционирования в 0,7 %, при этом с вероятностью 50 % эффективность заявленного способа составит 6 %.

Таким образом, переход к переменной длительности сегмента анализа при обработке речевого сигнала дает возможность сокращения средней скорости передачи данных в канале связи, так как вычисление параметров формирующей модели будет реализовано на более длительных интервалах анализа по сравнению с существующими техническими решениями.

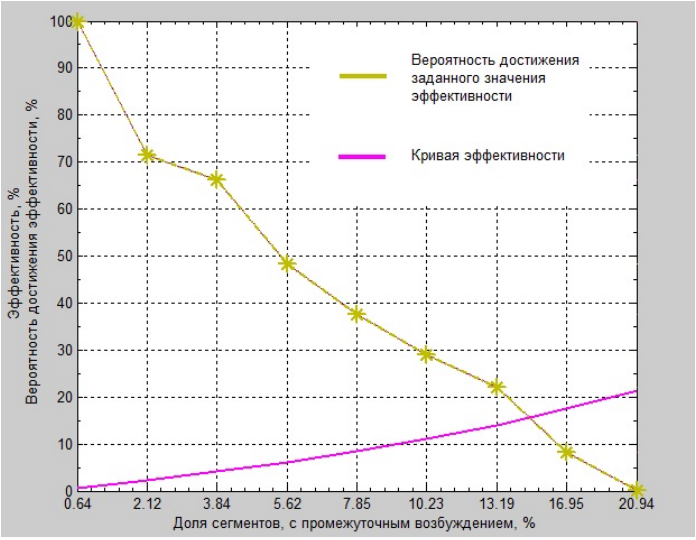


Рис. 2. Кривая эффективности

Список используемых источников

1. Прохоров Ю. Н. Статистические модели и рекуррентное предсказание речевых сигналов. М. : Радио и связь, 1984. 240 с.

2. Вапник В. Н. 1979. Восстановление зависимостей по эмпирическим данным. М.: Наука. 448 с.

3. Косарев Е. Л. Методы обработки экспериментальных данных. М. : ФИЗМАТЛИТ, 2008. 208 с.

4. Akaike H. Likelihood of a model and information criteria // Journal of Econometrics. 1981. Vol. 16. pp. 3–14.

5. Вальд А. Последовательный статистический анализ: под ред. А. Ф. Лапко, Государственное издательство физико-математической литературы. М., 1960. 328 с.

6. Афанасьев А. А., Рыжков А. П. Использование взаимозависимостей параметров линейного предсказания при реализации процедур обработки речевых данных // Телекоммуникации. 2012. N 13. С. 32–36.

7. Афанасьев А. А., Новиков Е. И., Трубицын В. Г., Титов О. Н. Способ выделения сегментов обработки речи на основе анализа корреляционных зависимостей в речевом сигнале. Пат. 2445718 Российская Федерация; заявитель и патентообладатель Академия ФСО России. – № 2010136618/08; заявл. 31.08.2010; опубл. 20.03.2012.

8. Михайлов В. Г., Златоустова Л. В. Измерение параметров речи. М. : Радио и связь, 1987. 168 с.

УДК 004.021

ОСОБЕННОСТИ ПРИМЕНЕНИЯ ПРОСТОЙ ЛИНЕЙНОЙ КОЛЛИЗИИ ДЛЯ УДАЛЕНИЯ ПРЕДПОЛАГАЕМЫХ СТЕГОВЛОЖЕНИЙ В ЦИФРОВЫХ ВИДЕОПОСЛЕДОВАТЕЛЬНОСТЯХ

К. А. Ахрамеева, Л. Г. Попов

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

В работе обоснованы возможность и актуальность применения алгоритма простой линейной коллизии для получения исходной цифровой видеопоследовательности (покрывающего объекта) из видеопоследовательности с возможным наличием стеговложения. Проведены эксперименты по реализации атаки удаления (2-го типа) предполагаемой стегосистемы, осуществлена оценка качества изображения, приведены рекомендации по оптимальным условиям и выбору параметров и др. Все полученные результаты исследования представлены в форме таблиц и выводов.

стеганография, стегоанализ, цифровая видеопоследовательность, линейная коллизия, временные корреляции, коллизии 1-го и 2-го типов, разложение на кадры, линейное сложение, битрейт, уровни избыточности и шума, сжатие, фильтр.

Известно, что большое количество исследований над стегоанализом сосредоточено на обнаружении стеганографии в неподвижных изображениях [1, 2, 3].

Прямые применения методов стегоанализа изображений к видеопоследовательностям на покадровой основе обычно имеют низкую эффективность и производительность. Поэтому необходимо разрабатывать и использовать схемы стегоанализа, ориентированные непосредственно на видеопоследовательности, то есть учитывающие особенности их формирования.

Одной из таких схем является линейная коллизия множества кадров [4, 5, 6, 7]. Коллизия может быть линейной или нелинейной, используя в своих интересах сходства и различия среди кадров, чтобы уменьшить энергию стегосигнала по отношению к тому, что является покрывающим объектом (ПО), то есть видеофайлу без вложения.

Линейная коллизия

Линейная коллизия первого типа возникает, когда огромное количество визуально непохожих видеокадров помечены линейной комбинацией

схожих цифровых стегосигналов. Это обычно встречается во многих существующих стегосистемах (СГС) для видео [8, 9, 10].

Коллизия второго типа возникает, когда огромное количество визуально похожих кадров помечены линейной комбинацией различных цифровых стегосигналов. Примером такой атаки может служить усреднение кадров. Этот случай соответствует, например, вложениям, которые используют разные двумерные псевдошумовые последовательности, для того чтобы произвести вложение в каждый кадр [11].

Допустим, дан ряд видеокадров с вложением $X_k = U_k + \alpha_k W_k,\ k = 1, \dots, n$, где U_k – исходный k-ый кадр, α_k – глубина вложения для k-го кадра, W_k – k-ый компонент стеговложения. Тогда линейная коллизия – это процесс формирования линейной комбинации видеокадров [12]:

$$\bar{X} = \sum_{k=1}^{n} \beta_k X_k = \sum_{k=1}^{n} \beta_k U_k + \sum_{k=1}^{n} \beta_k \alpha_k W_k, \quad (1)$$

где β_k – некоторый коэффициент (обычно $\beta_k = 1/n$).

При этом $\bar{X}$ представляет собой оценку с ϵ-оптимальной среднеквадратической ошибкой:

1) стеговложения $\bar{W} = \sum_{k=1}^{n} \beta_k \alpha_k W_k$;

2) покрывающего объекта $\bar{U} = \sum_{k=1}^{n} \beta_k U_k$.

В случае 1) возникает атака коллизии 1-го типа; в случае 2) – атака коллизии 2-го типа.

Целью данной работы является проверка актуальности и изучение особенностей частного случая линейной коллизии, который называется простая линейная коллизия, так как коллизионные веса (*collision weights*) применяются для всех кадров одинаковые.

Имеется скользящее окно, чтобы обозначить временное соседство, используемое для усреднения кадров. Предполагается, что это окно содержит визуально похожие кадры. Берётся окно размером $2L + 1$ кадров сосредоточенное на кадре k, чтобы усреднить видеопоследовательность. Оценка k-го видеокадра определяется следующим выражением:

$$\widehat{U}_k = \mathfrak{C}_P(Y_k) = \begin{cases} \frac{1}{2L+1} \sum_{i=1}^{2L+1} Y_i, & 1 \le k \le L; \\ \frac{1}{2L+1} \sum_{i=k-L}^{k+L} Y_i, & L < k \le N - L; \\ \frac{1}{2L+1} \sum_{i=N-2L}^{N} Y_i, & N - L < k \le N, \end{cases} \quad (2)$$

где $\mathfrak{C}_L$ – оператор коллизии с параметром P, являющимся длиной окна коллизии, Y_i – кадры, в которых предположительно могут быть вложения, $\widehat{U}_k$ – оценка исходного кадра U_k, N – общее количество кадров в видеопоследовательности, L – некоторое число.

Если коллизия применяется к данной видеопоследовательности Y_k, которая может содержать, а может и не содержать стеговложение, то полагается, что в обоих случаях для медленно меняющегося контента и соответственно выбранного значения L, результат будет аппроксимацией (приближением) U_k. Таким образом, если стегосигнал погружён в видео, то вычитание $\widehat{U}_k$ из Y_k даёт $Y_k - \widehat{U}_k \approx Y_k - U_k = \alpha W_k$ – оценку масштабированного Гауссовского стеговложения с нулевым матожиданием.

Фильтр Collision

С целью практического исследования эффективности линейной коллизии по удалению стеговложения (атака 2-го типа), погружённого в видеопоследовательность, был создан программный фильтр под названием Collision (рис. 1).

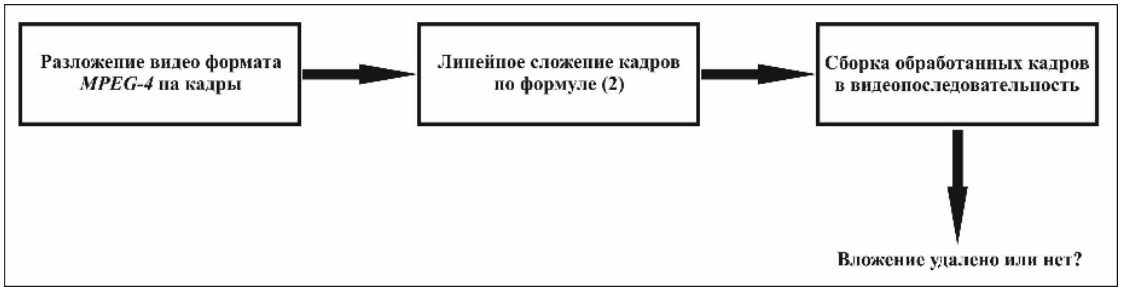


Рис. 1. Общая схема реализуемого алгоритма фильтрации видеопоследовательностей

С помощью свободно распространяемой утилиты MSU StegoVideo [13] создаётся СГС со «слепым» декодером, так как на приёмной стороне при извлечении скрытой информации покрывающее сообщение неизвестно. Алгоритм вложения также не известен («черный ящик»).

Сначала в видеопоследовательность погружается сочетание слов «Удаление вложения» и затем она сжимается с параметрами, которые можно непосредственно задавать в программе MSU.

Данными параметрами являются битрейт, уровень избыточности и уровень шума, вносимого в видеопоследовательность вложением, который влияет на устойчивость водяного знака к преобразованиям. Чем больше избыточность информации, тем больше вероятность отсутствия неправильных бит в результирующем файле, но тем меньшее количество информационных бит можно погрузить в видео. Если сжимать видео с низким битрейтом, то избыточность нужно увеличить, и наоборот.

В результате экспериментов по вложению текста с последующим сжатием кодеком H.264 выяснилось, что информация теряется полностью вне зависимости от используемого битрейта и уровня избыточности.

Поэтому было решено использовать кодек Xvid с различными профилями, а также кодек Lagarith Lossless, осуществляющий сжатие без потерь.

Атака фокусируется на временных корреляциях между видеокадрами, чтобы оценить оригинальную видеопоследовательность.

После обработки видеопоследовательностей извлечение смысловой информации с помощью программы MSU становится затруднительным или полностью невозможным (рис. 2).

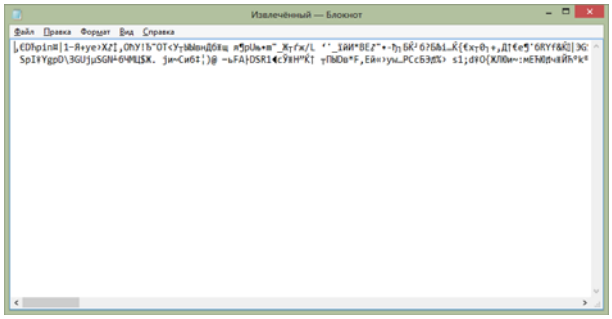


Рис. 2. Результат извлечения

Стоит отметить, что время, затрачиваемое на осуществление атаки достаточно мало (не более 1 минуты для 15 секунд видео). Для скорости отображения 30 кадров в секунду наблюдается временная задержка в 1/10 секунды.

Кроме того, видны лишь незначительные искажения исходного изображения, приемлемые с точки зрения стороннего наблюдателя. Ниже в таблицах 1–5 приведены результаты моделирований. На рис. 3 представлено сравнение качества изображения до и после атаки соответственно.

Рис. 3. Сравнение качества изображения

ТАБЛИЦА 1. Сравнение кодеков

№ (название видеоролика)	Название видеокодека					
	Xvid 1.3.4				**Lagarith Lossless**	
	Xvid Home		DivX 720HD			
	Ошибки до атаки, %	Ошибки после атаки, %	Ошибки до атаки, %	Ошибки после атаки, %	Ошибки до атаки, %	Ошибки после атаки, %
1. (busta – kamennye cvety.avi)	17,64	100	11,76	100	0	100
2. (chas pik.avi)	5,88	100	11,76	100	0	100
3. (simon i muha.avi)	94,08	пустой файл	100	пустой файл	0	100
4. (kolyaska.avi)	52,92	100	82,32	100	0	100
5. (ozvuchka.avi)	17,64	100	23,52	100	0	100

ТАБЛИЦА 2. Битрейт (низкая скорость смены сцен)

Битрейт, kbit/s	Название видеокодека					
	Xvid 1.3.4					
	Xvid Home		Xvid HD 720		DivX 720HD	
	Ошибки до атаки, %	Ошибки после атаки, %	Ошибки до атаки, %	Ошибки после атаки, %	Ошибки до атаки, %	Ошибки после атаки, %
250	23,52	100	23,52	100	23,52	100
500	23,52	100	23,52	100	23,52	100
1000	23,52	100	23,52	100	23,52	100
1500	23,52	100	23,52	100	23,52	100
2000	23,52	100	23,52	100	23,52	100
2500	23,52	100	23,52	100	23,52	100
3000	23,52	100	23,52	100	23,52	100

ТАБЛИЦА 3. Битрейт (высокая скорость смены сцен, пониженный коэффициент корреляции *R* между кадрами)

Битрейт, kbit/s	Название видеокодека	
	Xvid 1.3.4	
	Xvid Home	
	Ошибки до атаки, %	Ошибки после атаки, %
250	0	100
500	17,64	100
1000	11,76	100
1500	0	100
2000	0	100
2500	0	100
3000	0	100

В фильтре Collision не учитываются в полной мере такие статистические параметры, как коэффициенты корреляции между кадрами исходной видеопоследовательности и между элементами цифрового стеговложения, дисперсия оригинальных кадров и самого стеговложения, глубина вложения. Всё это может являться предметом дальнейшей работы и исследований, направленных на повышение эффективности атаки.

ТАБЛИЦА 4. Количество кадров в секунду (fps – frames per second)

Frames per second (fps)	Название видеокодека	
	Xvid 1.3.4	
	Xvid Home	
	Ошибки до атаки, %	Ошибки после атаки, %
24	23.52	100
25	23.52	100
30	0	100
60	0	100
120	0	100
200	0	100

ТАБЛИЦА 5. Возможный объём вложения в зависимости от битрейта

Битрейт, kbit/s	Название видеокодека	
	Xvid 1.3.4	
	Xvid Home	
	Количество символов без пробелов, зн.	Количество символов с пробелами, зн.
250	782	1694
500	807	1694
1000	974	1695
1500	974	1696
2000	1070	1696
2500	1229	1697
3000	1303	1702
5000	1359	1705
10000	1359	1705

Стоит заметить, что использование простой линейной коллизии освобождает нас от трудоёмкой процедуры предсказания движения с целью оценки исходной видеопоследовательности, что обеспечивает преимущество в скорости по сравнению с некоторыми алгоритмами, основанными на схеме компенсации движения, используемой в современных подходах сжатия видео.

Таким образом, мы видим, как статистическая избыточность (в данном случае временная) в покрывающем видео может помочь стегоаналитику в обнаружении (в нашем случае удалении) стеговложений. Увеличенная межкадровая корреляция улучшает производительность коллизии.

Рассмотренный метод простой линейной коллизии подходит для практической реализации в приложениях реального времени и показывает хорошие результаты по удалению (для типовых видеофайлов).

В заключение выделим следующее:

– чем больше избыточности в видео, тем больший объём информации можно вложить при меньших потерях;

– предпочтительнее использовать lossless кодеки;

– с увеличением битрейта при извлечении наблюдается уменьшение количества нераспознанных символов (при быстрой смене сцен);

– ниже 5000 kbit/s увеличивается количество ошибок;

– выше 5000 kbit/s ошибок нет, но отсутствует увеличение количества вложенных бит;

– для большего объёма вложения разумнее увеличивать количество кадров при сохранении приемлемого значения битрейта.

Список используемых источников

1. Fridrich J., Goljan M., Du R. Reliable Detection of LSB Steganography in Color and Grayscale Images // Proc. of the ACM Workshop on Multimedia and Security, 2001, pp. 27–30. URL: https://citeseer.ist.psu.edu/article/fridrich01reliable.html.

2. Memon N., Avcibas I., Sankur B. Steganalysis Based on Image Quality Metrics, SPIE, San Jose, California, USA, 2001, vol. 4314. URL: https://citeseer.ist.psu.edu/523259.html.

3. Sullivan K., Madhow U., Chandrasekaran S., Manjunath B.S. Steganalysis for Markov Cover Data With Apllications to Images // IEEE Transactions on Information Forensics and Security., June 2006, vol. 1, pp. 275–287/

4. Budhia U., Kundur D., Zourntos T. Digital Video Steganalysis Exploiting Statistical Visibility in the Temporal Domain // IEEE Transactions on Information Forensics and Security, December 2006, vol. 1, no. 4, pp. 502–516/

5. Ахрамеева К. А., Попов Л. Г. Сравнительный анализ эффективности подходов видеостегоанализа // Региональная информатика и информационная безопасность сборник научных трудов. Санкт-Петербургское Общество информатики, вычислительной техники, систем связи и управления. 2017. С. 287–302.

6. Небаева К. А., Попов Л. Г. Анализ методов стегоанализа цифровых видеопоследовательностей // Телекоммуникации. 2017. № 1. С. 33–40.

7. Небаева К. А., Попов Л. Г. Исследование методов стегоанализа цифровых видеопоследовательностей // Актуальные проблемы инфотелекоммуникаций в науке и образовании. Международная научно-техническая и научно-методическая конференция: сб. научных статей. СПб. : СПбГУТ, 2016. С. 489–493.

8. Hartung F., Eisert P., Girod B. Digital watermarking of MPEG-4 facial animation parameters, Comput. Graph., Jul.-Aug. 1998, vol. 22, no. 4, pp. 425–435.

9. Kalker T., Depovere G., Haitsma J., Maes M. A video watermarking system for broadcast monitoring // in Proc. SPIE, vol. 3657, Jan. 1999, pp. 103–112.

10. Cox I. J., Kilian J., Leighton F. T., Shamoon T. Secure spread spectrum watermarking for multimedia // IEEE Trans. Image Process., vol. 6, pp. 1673–1687, Dec. 1997.

11. Mobasseri B. G. Exploring CDMA for watermarking of digital video // Proc. SPIE, Jan. 1999, vol. 3657, pp. 96–102.

12. Su K., Kundur D., Hatzinakos D. Statistical invisibility for collusion-resistant digital video watermarking // IEEE Trans. Multimedia, Feb. 2005. vol. 7, no. 1, pp. 43–51.

13. Всё о сжатии данных, изображений и видео // Проект, идеи: Ватолин Д., реализация: Петров О. MSU StegoVideo – уникальная утилита для встраивания информации в видео (фильтр для VirtualDub/отдельная программа) [Электронный ресурс]. Режим доступа: http://www.compression.ru/video/stego_video/filter_settings.html

УДК 004.732

РАДИООБСЛЕДОВАНИЕ ОТКРЫТОЙ ГОРОДСКОЙ WI-FI СЕТИ НА НЕВСКОМ ПРОСПЕКТЕ

И. А. Баландин, Р. А. Дунайцев

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

В статье представлены результаты радиообследования открытой городской Wi-Fi сети на Невском проспекте. Проводится анализ количества установленных точек доступа, используемых частотных диапазонов, каналов и версий стандарта IEEE 802.11. Приводятся результаты исследования качества радиопокрытия, а также тестирования скорости передачи данных по протоколу TCP в направлении от сети к пользователю.

Wi-Fi, IEEE 802.11, радиообследование, беспроводная локальная сеть, точка доступа.

Хот-спот (*hot-spot*) – это территория снаружи или внутри помещения, где при помощи мобильного устройства, оснащенного Wi-Fi адаптером, любой желающий может получить доступ в глобальную сеть Интернет. Доступ может предоставляться на платной или бесплатной основе, а в качестве пользовательского устройства обычно выступает смартфон, планшет или ноутбук. Хот-спот может быть организован как на базе всего одной точки доступа (ТД), так и множества ТД с централизованной системой управления. Согласно прогнозу компании Cisco, число общедоступных Wi-Fi хот-спотов в мире, включая домашние, коллективные и коммерческие, за 5 лет увеличится примерно в 6 раз: с 94,0 млн в 2016 до 541,6 млн в 2021 г. [1]. Хот-споты часто создаются в заведениях общепита, торговых и развлекательных центрах с целью привлечения клиентов и повышения их лояльности, увеличения продаж и продвижения бизнеса [2]. Другим применением

хот-спотов стало создание на их основе открытых городских Wi-Fi сетей (т. н. *municipal wireless networks*). Во многих крупных городах разных стран развернуты подобные сети [3]. Не стала здесь исключением и Россия. В Москве работы над проектом «Городской Wi-Fi» начались в 2012 г. [4]. На сегодняшний день в пределах Садового кольца, в столичных парках, общежитиях ВУЗов и на транспорте установлено 10618 ТД, обслуживающих до 560 тыс. подключений ежемесячно [5]. В 2015 г. Москва уступала лишь Сеулу по количеству установленных ТД [6], а в 2016 г. городская Wi-Fi сеть получила премию «Проект года 2016» в специальной номинации «Лучший инфраструктурный проект» [7]. В Санкт-Петербурге развитие городской Wi-Fi сети также идет быстрыми темпами, хотя и с некоторым отставанием от столицы [8]. Например, в Московском метрополитене Wi-Fi сеть была полностью развернута в декабре 2014 г. [9], а в Петербургском метрополитене это случилось 3 годами позже [10]. Помимо метро, открытая городская Wi-Fi сеть сейчас доступна в Центральном, Петроградском и Василеостровском районах [11]. Согласно заявлению Лаврухина Владимира Алексеевича, руководителя проекта «Открытый Петербург», основной задачей в настоящее время является обеспечение радиопокрытия на улицах города [12]. Разумеется, уличный Wi-Fi оказывается наиболее востребован туристами и гостями города, так как позволяет быстро и бесплатно получать необходимую информацию, а также оставаться на связи. Как показывают исследования онлайн-привычек путешественников, 69% туристов для доступа в Интернет предпочитают за рубежом использовать именно общественный Wi-Fi и гораздо реже – услуги операторов сотовой связи или Интернет-кафе [13]. Таким образом, открытая городская Wi-Fi сеть в центральных районах Петербурга – это не только удобно, но и полезно для повышения туристической привлекательности Северной столицы.

Для проведения радиообследования был выбран Невский проспект как главная улица нашего города. К тому же в Сети встречаются прямо противоположные мнения о качестве работы там городского Wi-Fi: от резко отрицательных [14] до сугубо положительных [15]. Целью исследования было определить количество действующих ТД, задействованные частотные диапазоны и каналы, а также оценить качество радиопокрытия [16]. Для сбора данных использовалась программа Ekahau Site Survey версии 9.0.3, установленная на ноутбуке DNS 0164800. Так как встроенный в ноутбук Wi-Fi адаптер Realtek RTL8723AE (bgn, 1x1:1) поддерживал работу лишь в диапазоне 2,4 ГГц, для сканирования каналов в обоих диапазонах было решено использовать внешний USB-адаптер D-Link DWA-160/B2 (abgn, 2×2:2) [17]. Для отметки на карте маршрута движения применялся GPS-приемник, встроенный в смартфон Xiaomi Redmi 4 Pro, который соединялся с ноутбуком через Bluetooth. На ноутбуке использовалась программа GpsGate, а на телефоне – GPSoverBT. Обход проводился в воскресенье днем сперва

по одной стороне Невского от площади Восстания до пересечения с Адмиралтейским проспектом, а затем в обратном направлении уже по противоположной стороне.

Развернутая на Невском проспекте Wi-Fi сеть построена на базе оборудования компании Ruckus Wireless Inc. ТД установлены на домах вдоль проспекта, причем высота монтажа варьируется примерно от 3,5 до 5,5 метров (рис. 1). Некоторые из ТД оснащены двумя внешними антеннами. Специальных указателей на наличие открытой городской Wi-Fi сети, как это делается в других городах (например, в Барселоне [19]), в Санкт-Петербурге нет, пользователям предлагается ориентироваться на доступность сети «SPb Free Wi-Fi» в своем мобильном устройстве [11]. Подключиться к сети можно либо в качестве гостя, либо как клиенту Дом.ru, или же купить премиум-доступ за 99 рублей в месяц [18].

Рис. 1. Точки доступа городской Wi-Fi сети

В ходе радиообследования программа выявила 63 ТД, принадлежащие открытой городской Wi-Fi сети. Как видно из табл. 1, радиопокрытие

на Невском проспекте создается в основном ТД, работающими в диапазоне 2,4 ГГц. В качестве имени сети большинство обнаруженных ТД транслирует следующие четыре идентификатора SSID (*service set identifier*): SPb Free Wi-Fi, DOM.RU Wi-Fi, DOM.RU Mobile и один скрытый (табл. 2). Работающие в диапазоне 5 ГГц ТД используют иные идентификаторы SSID (DOM.RU_Wi-Fi, DOM.RU_Wi-Fi_5G, island-2420A0, island-2CA9D0, island-240260) и, скорее всего, задействованы в оказании коммерческих услуг по подключению к сети Интернет. Согласно данным в табл. 3, частотно-территориальное планирование в диапазоне 2,4 ГГц, вместо традиционного использования трех непересекающихся каналов 1-6-11, построено на использовании четырех каналов 1-4-8-11. В диапазоне 5 ГГц применяется исключительно канал 40. В обоих диапазонах ширина каналов составляет 20 МГц, объединение каналов (*channel bonding*) не практикуется.

ТАБЛИЦА 1. Используемые диапазоны и версии стандарта IEEE 802.11

Поддерживаемый диапазон	IEEE 802.11	Макс. Скорость и число потоков	Число ТД	Доля, %
Только 2,4 ГГц	*b, g, n*	144 Мбит/с, 2	2	3,2
	g, n	144 Мбит/с, 2	21	33,3
	g, n	130 Мбит/с, 2	31	49,2
Только 5 ГГц	*a, n*	144 Мбит/с, 2	1	1,6
Оба диапазона	*b, g, n + a, n*	144 Мбит/с, 2	2	3,2
	g, n + a, n	144 Мбит/с, 2	6	9,5
ВСЕГО			63	100

ТАБЛИЦА 2. Число используемых SSID в диапазонах 2,4 и 5 ГГц

Число SSID, 2,4 ГГц	Число радиомодулей	Доля, %	Число SSID, 5 ГГц	Число радиомодулей	Доля, %
1	6	9,7	1	6	66,7
2	5	8,1	2	3	33,3
3	3	4,8	3	–	–
4	47	75,8	4	–	–
5	1	1,6	5	–	–

Для оценки качества радиопокрытия были выбраны следующие базовые требования: уровень сигнала не ниже –75 дБм, соотношение сигнал/шум не ниже 10 дБ, эффективная скорость передачи от 1 Мбит/с и выше [1, 11, 18]. Полученные результаты представлены на рис. 2 в виде

гистограмм. Легко видеть, что лишь в 4 % случаев мощность сигнала оказывалась неудовлетворительной, тогда как примерно 87 % пройденного пути скорость загрузки по протоколу TCP была выше порогового значения.

ТАБЛИЦА 3. Используемые каналы в диапазонах 2,4 и 5 ГГц

№ канала	1	2	3	4	5	6	7	8	9	10	11	12	13	40
Число радиомодулей	16	0	0	11	3	1	2	10	4	0	16	0	0	9

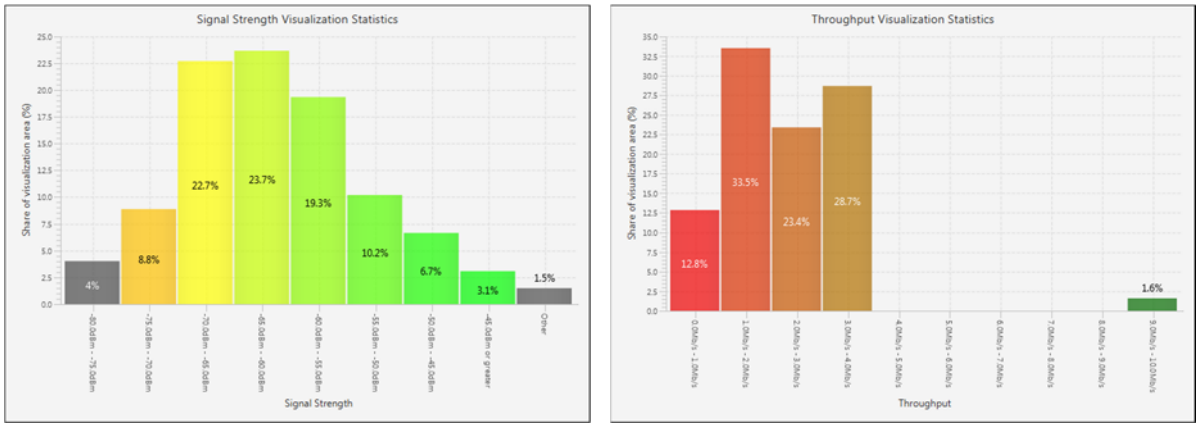


Рис. 2. Уровень сигнала в дБм и эффективная скорость передачи данных в Мбит/с

Список используемых источников

1. Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2016-2021 [Электронный ресурс]. URL: https://www.cisco.com/c/dam/m/en_in/innovation/enterprise/assets/mobile-white-paper-c11-520862.pdf (дата обращения 18.03.2018).

2. Wi-Fi hot spot (хот-спот): новые возможности для вашего бизнеса [Электронный ресурс]. URL: https://www.kp.ru/guide/hotspot.html (дата обращения 18.03.2018).

3. Municipal wireless network [Электронный ресурс]. URL: https://en.wikipedia.org/wiki/Municipal_wireless_network (дата обращения 18.03.2018).

4. Wi-Fi, умный город и интернет вещей: онлайн-технологии для столицы [Электронный ресурс]. URL: https://www.mos.ru/news/item/21107073/ (дата обращения 18.03.2018).

5. Городская сеть Wi-Fi [Электронный ресурс]. URL: https://www.mos.ru/city/projects/wi-fi/ (дата обращения 18.03.2018).

6. The Top7 Intelligent Communities of the Year [Электронный ресурс]. URL: https://www.intelligentcommunity.org/moscow (дата обращения 18.03.2018).

7. Бесплатная городская сеть Wi-Fi Москвы получила премию «Проект года 2016» [Электронный ресурс]. URL: http://tass.ru/obschestvo/3977914 (дата обращения 18.03.2018).

8. Где в Петербурге есть бесплатный Wi-Fi? [Электронный ресурс]. URL: http://www.spb.aif.ru/dontknows/1090322 (дата обращения 18.03.2018).

9. Бесплатный Wi-Fi в метро [Электронный ресурс]. URL: http://mosmetro.ru/info/wifi-v-metro/ (дата обращения 18.03.2018).

10. Бесплатный Wi-Fi с 6 декабря заработал на всех станциях метро Петербурга [Электронный ресурс]. URL: https://www.spb.kp.ru/online/news/2954180/ (дата обращения 18.03.2018).

11. Бесплатный городской Wi-Fi заработал в трех районах Петербурга [Электронный ресурс]. URL: https://www.spbdnevnik.ru/SPb-Free-Wi-Fi/ (дата обращения 18.03.2018).

12. Свободный Wi-Fi на Невском [Электронный ресурс]. URL: https://topspb.tv/programs/stories/461610/ (дата обращения 18.03.2018).

13. G DATA summer survey: 80 percent go online on holiday [Электронный ресурс]. URL: https://www.gdatasoftware.co.uk/news/g-data-summer-survey-80-percent-go-online-on-holiday (дата обращения 18.03.2018).

14. Бесплатный интернет портит имидж Петербурга [Электронный ресурс]. URL: http://www.online812.ru/2014/10/28/011/ (дата обращения 18.03.2018).

15. Свободный доступ: как работает бесплатный Wi-Fi в центральных районах Петербурга [Электронный ресурс]. URL: https://topspb.tv/news/2017/01/24/svobodnyj-dostup-kak-rabotaet-besplatnyj-wi-fi-v-centralnyh-rajonah-peterburga/ (дата обращения 18.03.2018).

16. IEEE Std 802.11-2016 (Revision of IEEE Std 802.11-2012) - 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. December 14, 2016.

17. D-Link DWA-160/B2 [Электронный ресурс]. URL: http://www.dlink.ru/ru/products/2/1158.html (дата обращения 18.03.2018).

18. На Невском – бесплатный Wi-Fi [Электронный ресурс]. URL: http://www.tdaily.ru/news/all/101/29712 (дата обращения 18.03.2018).

19. Barcelona WiFi [Электронный ресурс]. URL: http://ajuntament.barcelona.cat/barcelonawifi/en/manual.htm (дата обращения 18.03.2018).

УДК 535.8

ПРОЕКТИРОВАНИЕ АТМОСФЕРНОЙ ЛИНИИ СВЯЗИ В КАЧЕСТВЕ ОСНОВНОЙ СЕТИ С УЧЕТОМ ГОРОДСКОЙ ЗАСТРОЙКИ САНКТ-ПЕТЕРБУРГ

А. С. Безбородова, В. А. Гирш, К. И. Стахеев, И. Г. Штеренберг

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

Беспроводные лазерные системы связи быстро развиваются в связи с интенсивным развитием телекоммуникационных систем. В статье рассмотрен вопрос о применении атмосферных оптических линий для организации сети связи на базе корпоративной сети, с учетом региональных факторов на примере Санкт- Петербурга.

атмосферные оптические линии, влияние атмосферы, места установки оборудования, участок связи.

Атмосферные оптические линии связи получают все большее распространение в мире. Однако процессу их внедрения мешают некоторые вопросы связанные, в основном, с необъективной оценкой влияния погоды на надежность данного вида связи.

Для правильно установленной и настроенной атмосферной оптической линии, определяющим фактором надежности связи являются погодные условия в месте ее расположения. Сигнал, подаваемый на внутренний интерфейс блока преобразователя, переводится в оптический сигнал лазера, затем усиливается и направляется через соединительный оптоволоконный кабель в оптическую антенну, которая преобразует инфракрасное излучение (ИК) в коллимированный узконаправленный луч (излучения с очень маленьким углом сходимости или расходимости), и далее передается через атмосферу. Попадая на приемную апертуру оптической антенны с противоположной стороны, луч снова заводится в соединительный оптоволоконный кабель, по которому, передается в модуль преобразователя и преобразуется в электрический сигнал и направляется на внешний интерфейс. При передаче ИК излучение проходит различные преобразования, при этом происходит его рассеивание и поглощение в атмосфере, таким образом, излучаемая мощность в точке передачи всегда будет ниже, чем в точке отправления [1].

Распространение лазерного излучения в атмосфере сопровождается целым рядом явлений линейного и нелинейного взаимодействия света со средой. При этом ни одно из этих явлений не проявляется в отдельности. Влияние атмосферы сказывается в ослаблении луча метеорологическими факторами: ослабление на аэрозолях (пыль, дождь, снег, туман), поглощение и рассеяние молекулами газов воздуха. Дополнительными факторами уменьшения мощности излучения в плоскости приема служат турбулентные образования в атмосфере, нелинейные эффекты распространения, фоновые помехи. Это приводит к «дрожанию» луча, к его «пятнистости» в плоскости приема. Кратко остановимся на каждом из этих явлений.

Поглощение светового потока, видимого и инфракрасного диапазонов, определяется, прежде всего, молекулярным поглощением, крайне неравномерным по частоте. Оно максимально на резонансных частотах молекул воздуха, воды, углекислого газа, озона и других компонент атмосферы. Если лазерное излучение попадает в центр сильной линии спектра, то оно поглощается атмосферой на 100 % даже на небольшом расстоянии. Поэтому для АОЛС следует брать лазеры с излучением, находящимся на участках спектра атмосферы, занятых широкими окнами прозрачности (участками, где поглощение незначительно).

Вторым фактором влияния атмосферы на АОЛС является рассеяние, оно представляет собой механическую смесь из газов, паров, капель жидкости и твердых частиц. В ней всегда в переменном количестве присутствуют пыль, дым, кристаллики льда. Поэтому атмосфера является аэрозолем, состав которого непрерывно изменяется из-за перемешивания. Говоря об аэрозольном рассеянии в общем, имеют в виду аэрозольное ослабление, обусловленное не только рассеянием, но и поглощением излучения частицами аэрозоля. Все типы атмосферных аэрозолей можно объединить в следующие основные классы: облака, туманы, дымки, морозь и осадки.

Так же, значимое влияние на распространение лазерного луча оказывает турбулентность атмосферы, то есть случайные пространственно-временные изменения показателя преломления, вызванные перемещением воздуха, флуктуациями его температуры и плотности. Турбулентность атмосферы приводит к искажениям волнового фронта и, следовательно, к колебаниям и уширению лазерного пучка и перераспределению энергии в его поперечном сечении. При этом иногда возникают замирания сигнала, и связь становится неустойчивой. К атмосферным потерям следует добавить еще так называемые геометрические потери сигнала, зависящие от протяженности линии и угловой расходимости излучения [1].

Одним из дополнительных факторов уменьшения мощности излучения в плоскости приема являются фоновые помехи.

Все фоновые помехи имеют две составляющие, первая – медленно меняющаяся во времени часть, которую в данный конкретный момент времени можно считать постоянной. И вторая, быстро меняющаяся фоновая помеха (модулированная по интенсивности). Большинство природных источников фонового излучения меняют интенсивность излучения медленно, при расчетах его необходимо учитывать, как постоянную составляющую фоновых помех. Для борьбы с этим типом помех, необходимо использовать развязывающие конденсаторы. Техногенные, быстро меняющиеся фоновые помехи имеют локальный характер, для борьбы с ними необходимо использовать пространственную фильтрацию.

Незначительное воздействие на АОЛС оказывают помехи, но многие из них не требуют сложных решений на уровне управления каналом или кодирования передаваемой информации, а могут быть эффективно устранены элементами конструкции или же проигнорированы. В частности:

– нелинейными эффектами распространения можно пренебречь ввиду небольшой импульсной и средней оптических мощностей (мощности применяемых излучателей порядка менее кВт, что на несколько порядков меньше необходимых для возникновения нелинейных эффектов);

– длину волны излучаемого света необходимо выбирать с таким расчетом, чтобы она находилась в окне прозрачности даже с учетом технологических допусков и дрейфа излучателя;

– флуктуациями интенсивности оптического сигнала под действием турбулентности атмосферы можно пренебречь (естественно, при сохранении уровня сигнала достаточным для детектирования).

При распространении излучения в атмосфере наблюдаются не только его поглощение и рассеяние, но и флуктуации его параметров (интенсивности, фазы, угла прихода и др.), обусловленные турбулентными явлениями колебаниями температуры, влажности, плотности воздуха, а, следовательно, и его показателя преломления. Подробный обзор теоретических исследований по этому вопросу приведен ниже. Знание вида функции распределения плотности вероятностей флуктуаций (ФРПВФ), являющейся наиболее полной статистической характеристикой случайного процесса, необходимо при определении вероятности ошибки и надежности работы оптических линий связи. К настоящему времени установлено, что вид ФРПВФ зависит от величины универсального безразмерного параметра β_0^2, представляющего собой дисперсию логарифма флуктуаций амплитуды плоской оптической волны, вычисленную в приближении метода плавных возмущений:

$$\beta_0^2 = 1{,}23\ C_n^2\ \ k^{7/6}\ L^{11/6} \qquad (1)$$

где C_n^2 – структурная характеристика показателя преломления воздуха, отражающая степень турбулентных возмущений; $k = 2\pi / \lambda$ – волновое число; λ – длина волны; L – длина трассы в турбулентной атмосфере.

Условно все встречающиеся на практике ситуации при любой комбинации величин, входящих в соотношение (1), подразделяются на три случая флуктуаций интенсивности: $2\beta 0 \ll 1$ – слабые, $2\beta \cong 0\ 1$ – насыщенные, $2\beta 0 \gg 1$ – сильные флуктуации. Для технических приложений (связь, локация и т. п.) область насыщенных и сильных флуктуаций представляют значительный интерес, поскольку длина трассы обычно велика, в этих областях вопрос определения вида ФРПВФ достаточно сложен [2].

Важным обстоятельством для успешной работы является и правильная установка ППМ (приемно-передающего модуля). Чтобы этого достичь, необходимо пользоваться следующими рекомендациями:

– на пути луча не должно быть препятствий, причем с учетом сезонных изменений (провисания проводов в теплое время года или при обледенении, появления на деревьях лиственного покрова, рост деревьев, снежные заносы зимой и т. д.);

– не следует устанавливать ППМ на лифтовых шахтах, около вытяжных вентиляторов, обслуживающих здания машин, колебания которых могут вызывать отклонение луча;

– не следует монтировать ППМ на консольных конструкциях, металлических надстройках и других сооружениях, которые могут изгибаться под действием тепловых и ветровых нагрузок;

– при ориентации системы по направлению запад – восток необходимо учитывать возможные нарушения в работе ППМ в результате засветки приемника при восходе или заходе солнца;

– следует избегать установки систем АОЛС в непосредственной близости от мест скопления птиц, которые также могут создавать помехи для связи;

– необходимо учитывать сильное влияние тумана на надежность АОЛС и прокладывать линию на возможно большей высоте, где густота тумана меньше [1].

Объектом для исследования применимости технологии в Санкт Петербурге нами был выбран Санкт-Петербургский государственный университет телекоммуникаций им. проф. Бонч-Бруевича (СПбГУТ). В состав университета входят три учебных корпуса находящихся на значительном расстоянии друг от друга.

Для организации линии АОЛС был выбран участок от пр. Большевиков д. 22 до набережной реки Мойки д. 61. Данный участок представляет собой два здания, которые объединяют 1институт. Расстояние между ними составляет 10,2 км по прямой. Между выбранными адресами расположена река Нева и 2 ее канала, которые являются источником факторов, влияющих на доступность оптического канала связи (туман). По этим причинам участок связи между этими двумя зданиями представляет наибольший интерес в исследовании применимости технологии АОЛС. Санкт-Петербург является городом с большим количеством высотных зданий, зная это, при выборе места установки оборудования АОЛС будут рассмотрены только самые высотные сооружения, на которых будет возможна установка, с учетом всех влияющих на работу факторов.

В связи с быстрым ростом развития технологий, из-за потребности в использовании АОЛС на большие расстояния, работа линии АОЛС в настоящее время возможна на расстояние до 7000 м. за счет такого понятия как калиброванный резервный канал на основе Wi-Fi радиомаршрутизаторов со специализированным программным обеспечением (СПО). Оно характерно для оборудования модели M1-FE-L производства АО «МОСТКОМ». Мощность передатчика, входящего в комплект с калиброванным резервным каналом, варьируется от 5,2–5,8 ГГц. Именно эту модель мы будем рассматривать при проектировании нашей трассы.

Выбранная нами локальная сеть организуется с применением двух приемно-передающих модулей, у которых всепогодный герметизированный корпус с защитой от ветра (50 м/с), дождя, снега, тумана, изморози и других осадков. Рабочая температура: –40…+50 градусов Цельсия. Питание: 220 В, 50 Гц или 30–72 В постоянного тока. ППМ будут установлены на крышах зданий, находящихся на данном участке связи. Скорость линии составит

от 10–100 Мбит/с. Так как расстояние между выбранными нами точками составляет чуть больше 10 км, оборудование будет установлено приблизительно на равных расстояниях от конечных устройств, что составит по 5 км на каждый участок. Первый участок это пр. Большевиков д. 22 – ул. Подвойского д. 8, второй участок ул. Подвойского д. 8 – наб. реки Майки д. 61. Промежуточное здание для установки оборудования выбрано с учетом всех вышеизложенных рекомендаций, таким образом, лучу ничего не будет мешать при передаче информации.

С учетом всех недостатков местности рассматриваемого города, технология АОЛС применима для организации линий связи в Санкт-Петербурге. Перспективой развития этой технологии в Ленинградской области может служить организация связи на более масштабные расстояния. Так, в будущем планируется проектирование линии связи для всех трех корпусов СПбГУТ с применением оборудования с лучшими техническими показателями.

Список используемых источников

1. СНИП 2.01.07-85. Нагрузки и воздействия. Нормы проектирования. Госстрой России. М.: ГУП ЦПП, 2003. 55 с.

2. Гумбинас А. Ю., Милютин Е. Р. Статистическая теория атмосферного канала оптических информационных систем. М. : Радио и связь, 2002. 254 с.

УДК 681.7

ПСИХОФИЗИКА ВОСПРИЯТИЯ: МОДЕЛЬ ЧЕЛОВЕЧЕСКОГО ГЛАЗА КАК КОНСТРУКТИВНЫЙ ЭЛЕМЕНТ ОПТИЧЕСКОГО ПРИБОРОСТРОЕНИЯ

Е. В. Белова, Е. В. Полякова

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

В статье рассматриваются инженерно-психологические аспекты моделирования элементов оптического приборостроения и глаза человека. Проводится сравнение элементов устройства оптических приборов (на примере оптического конструктора) и анатомо-физиологических особенностей построения зрительного образа. На основе приведенной аналогии предлагаются перспективы дальнейшего повышения эффективности устройства и функционирования оптических приборов.

моделирования элементов оптического приборостроения, анатомо-физиологические особенности строения зрительного анализатора.

С каждым годом все большее количество инноваций в передовых технологических сферах возникают на основе междисциплинарных исследований и разработок. Так, согласно стратегии научно-технологического развития Российской Федерации, наша страна находится на этапе, когда умение отвечать на большие вызовы с использованием уникальных научных установок класса «мегасайенс» становится необходимой компетенцией времени. Значимыми для научно-технологического развития Российской Федерации становятся не направления исследований и разработок, актуальные для последних десятилетий прошлого века, а фундаментальная наука, обеспечивающая получение новых знаний и опирающаяся на собственную логику развития, при этом дающая эффективные для различных общественных сфер разработки. В долгосрочной перспективе особую актуальность приобретают исследования в области понимания процессов, происходящих в обществе и природе, развития природоподобных технологий, человеко-машинных систем.

Теоретики и практики мирового уровня, специализирующиеся на инновационном мышлении инноваторов и изобретателей (де Боно, Слоан и др.), отмечают специфику их системного мышления, подчеркивая идею, которая активно пропагандируется и в ведущих IT-компаниях (например, Google): мыслите масштабно, междисциплинарно, расширяйте кадровое окно, нанимая сотрудников, которые используют «комбинаторное мышление». Именно возможность мыслить на грани нескольких научных направлений, перенося знания из одной в другую (казалось бы, далекую) отрасль науки, поиск «гибридных тем» исследования по принципу У. Уотсона, а также умение расширить «окно возможностей» применения фундаментальных открытий характеризуют инновации XXI века [1]. Тем не менее, в современных исследованиях в сферах психологии и оптики междисциплинарность постулируется, но не анализируется. Построение оптических приборов с точки зрения психологии восприятия дает возможность переноса знаний из области психофизиологических и психофизических моделей на технические.

Одним из эффективных инструментов развития научной мысли является метод моделирования. Моделирование как общенаучный метод используется для двух ключевых целей: демонстрационной (в том числе в педагогике), исследовательской (с помощью которой апробируются гипотезы исследования). Рассмотрим со второй точки зрения инженерно-психологические аспекты структурно-функциональных параметров визуального восприятия. Данные параметры могут быть классифицированы в духе когнитивной психологии, использующей метафору компьютера для объяснения работы психики: на «hardware» (анатомия глаза и центральной нервной системы) и software (описание психических процессов).

Ощущение и восприятие являются чувственным отображением объективной реальности, при котором физический сигнал (стимул) превращается в психический образ. Эволюционно-функциональный смысл подобного превращения заключается в достигаемом системном эффекте, психическом образе, который дает большее количество информации за меньшее количество энергетических и временных затрат мозга. Так, еще основатель психофизики Густав Теодор Фехнер (1801–1887) рассматривал соотношения психических и физических явлений, связанных между собой функционально. Г. Гельмгольц (1821–1897) полагал, что живой организм представляет собой физико-химическую среду, в котором выполняется закон сохранения энергии [2, 3].

Не останавливаясь на психофизической дилемме, отражающей проблему поиска закономерности трансформации физического стимула в психический образ (закон Бугера-Вебера, основной психофизический закон Вебера-Фехнера, закон Стивенса, обобщенный психофизический закон Ю. М. Забродина), рассмотрим подробнее анатомические и физиологические особенности зрительных ощущений, которые возможно применить для моделирования элементов оптического приборостроения. Следует отметить, что уже на уровне элементарных ощущений возникают интересные психофизические закономерности и эффекты. Так, анатомо-физиологической основой зрительных ощущений является деятельность сложных комплексов анатомических структур (названных И. П. Павловым анализаторами), которые состоят из трех частей [4]: 1) периферического отдела – рецептора с химическим веществом, реагирующим на свет, благодаря чему происходит трансформация физического сигнала (определенных диапазонов электромагнитных колебаний) в электрический импульс (зрительные рецепторы расположены тонким слоем на внутренней стороне глаза); 2) проводящих нервных путей; 3) корковых отделов анализатора (проекция периферии в коре головного мозга). Для возникновения ощущения необходимо задействовать все составные части анализатора, при разрушении хотя бы одной части анализатора возникновение соответствующих ощущений становится невозможным. Зрительные ощущения прекращаются и при повреждении глаз, и при нарушении целостности зрительных нервов, и при разрушении затылочных долей обоих полушарий.

Тем не менее, оптические приборы конгруэнтны по возникающим эффектам более обобщенному психическому процессу восприятия. Существенное отличие физической модели оптического прибора от психологической модели глаза и зрительной системы состоит в том, что биологическая структура адаптивна, активна и действуют по принципу обратной связи. Так, уже анализатор – это активный орган, рефлекторно перестраивающийся под воздействием раздражителей, ощущение включает в себя

двигательные компоненты в форме вегетативных или мышечных реакций (например, поворот глаз). Рецепторы обладают способностью кодировать интенсивность (с помощью числа нервных импульсов в единицу времени, временного паттерна следования импульсов, абсолютного числа активированных нейронов) и качественные параметры раздражителя (через тип нервных волокон, паттерны импульсов или через форму электрического сигнала).

Эффективность зрительной системы апробирована эволюционно: академик С. И. Вавилов экспериментально установил, что человеческий глаз может различать световой сигнал в 0,001 свечи на расстоянии километра. Энергия данного раздражителя настолько мала, что потребовалось бы 60 000 лет, чтобы с его помощью нагреть 1 $см^3$ воды на 1°. Интересно, что сенсорная система человека (как измерительный прибор) обладает определенным диапазоном: так, раздражения, лежащие ниже порога ощущения (которые мы не осознаем), могут вызывать изменение электрической активности мозга и расширение зрачка («субсенсорная область» по Г. В. Гершуни или «подпороговое восприятие»).

Сенсорная адаптация (изменение чувствительности, происходящее вследствие приспособления органа чувств к действующим на него раздражителям) также является характеристикой живой системы: чувствительность глаза в темноте обостряется в 200 000 раз, но для того чтобы зрение в темной комнате приобрело нужную чувствительность, должно пройти около 30 мин. Адаптация наших ощущений главным образом зависит от процессов, происходящих в самом рецепторе: под влиянием света разлагается (выцветает) зрительный пурпур, находящийся в палочках сетчатки глаза, при длительным раздражении кора головного мозга отвечает внутренним охранительным торможением. Взаимодействие ощущений создает интересный синергетический эффект: П. П. Лазарев и С. В. Кравков установили, что освещение глаз делает слышимые звуки более громкими, звуковое раздражение (например, свист) может обострить работу зрительного ощущения, повысив его чувствительность к световым раздражителям.

Исследования различительных порогов физиками П. Бугером и М. Вебером еще в XIX веке показали, что человек воспринимает не различия между объектами, а отношение различия к величине сравниваемых объектов (если исходная освещенность комнаты составляет 100 люксов, то необходимая прибавка освещенности должна составлять не менее одного люкса). Согласно закону Бугера-Вебера, порог различий ощущений определяется соотношением:

$$\Delta I / I = \text{const},$$

где ΔI – величина, на которую должен быть изменен исходный, уже вызвавший ощущение стимул, чтобы человек заметил, что он действительно изменился; I – величина действующего стимула; const – постоянная величина, характеризующая порог различия ощущения (константа Вебера для ощущения изменения яркости света равна 0,017). Относительная величина, характеризующая порог различения, является постоянной для конкретного анализатора (для зрительного анализатора это соотношение составляет приблизительно 1/1000).

Подобная эффективность зрительной системы обусловлена принципом ее работы. Изначальная идея дуги (рецептор – афферентные пути – центр (мозг) – эфферентные пути – мышцы), благодаря исследованиям Н. А. Бернштейна, превратилась в рефлекторное кольцо (т. к. к данному контуру добавилась обратная связь от мышц, которые подают сигнал обратно в мозг о расхождении в программе действий). В середине XX века физиолог Р. Гранит предлагает идею второго кольца, уточняющую функциональную структуру зрительного анализатора: для повышения точности работы рецепторного аппарата от центральной нервной системы в рецепторы также поступают сигналы сличения.

Зрение обоснованно считают ведущим сенсорным анализатором и, однозначно, роль зрительного восприятия в жизни человека трудно переоценить. Глаз, как оптический прибор, созданный самой природой, постоянно интересует человечество с двух точек зрения: как самостоятельная оптическая система и как приемник изображения, с которым работают многие оптические приборы. В соответствии с таким подходом сформирована одна из важнейших задач оптики − получение изображений, соответствующих оригиналам как по геометрической форме (геометрическая оптика), так и по распределению яркости (фотометрия). Геометрическая оптика дает ответ на вопрос, как следует строить оптическую систему для того, чтобы каждая точка объекта изображалась в виде точки изображения и сохранялось геометрическое подобие изображения объекту. Геометрическая оптика указывает на источники искажений изображения и их уровень в реальных оптических системах.

Для наглядного понимания процессов формирования изображения в оптической системе глаза человека и оптических системах, корректирующих аберрационные проблемы, удобно пользоваться моделью оптической системы человеческого глаза, созданной на элементной базе оптического конструктора (рис.). Несомненным преимуществом такого моделирования является возможность получения ярких и достаточно четких распределений интенсивностей световых потоков в исследуемых оптических системах и, как следствие, физические процессы становятся доступными и понятными.

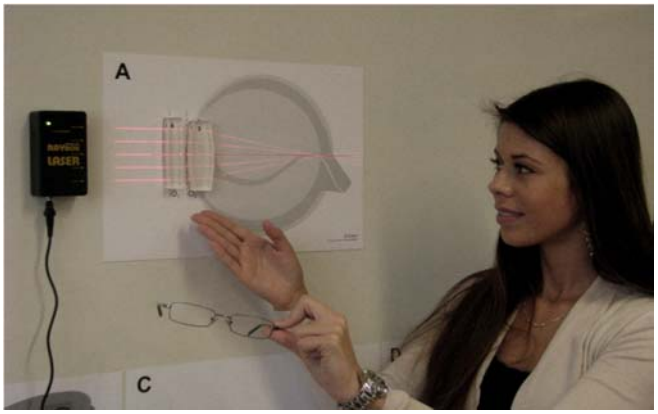


Рисунок. Модель человеческого глаза
на элементной базе оптического конструктора

Перспективы моделирования психических явлений и взаимной трансляции знаний из области психологии в область оптики связаны с тремя междисциплинарными направлениями: совершенствованием пока еще слабого математического аппарата, разработанного для психологических исследованиях (большинство математических методов в психологии, например, факторный анализ Ф. Гальтона, были предложены еще в XIX веке для задач того времени); использованием современных устройств и материалов для физического моделирования психических явлений (психология создавалась физиками и физиологами в первых лабораториях В. Вундта и потом Ф. Фехнера как естественнонаучное направление, моделирующее психофизические проблемы восприятия); системным подходом к исследованию сложных психических явлений, которые объективно не наблюдаемы (только опосредованно) и не обладают четкими пространственно-временными границами. Системная природа психических процессов (даже простейших), анатомическая структурно-функциональная сложность организации субстрата психики (нервной системы) требует от исследователей новой методологической аналогии в объяснении природы психики как объективной реальности. Так, А. Г. Шмелев, не видя в текущем состоянии математической и естественно-научной базы перспективы для моделирования психики, отмечает, что необходимо использовать новые, практико-ориентированные математические модели, например, позаимствованные из различных языков программирования (*Pascal*, *Java*, C++). Психические явления (в духе компьютерной метафоры когнитивной психологии) могут быть представлены в терминах объектно-ориентированного программирования, требующего не только описания самих признаков объекта, но и процедур (правил) обращения к ним.

В XXI веке с развитием современных технологий и оптических лазерных устройств открываются возможности физического моделирования ранее недоступных для визуализации явлений. Законы развития психики, которая нематериальна, возможно доказать с помощью создания физических моделей, адекватно отражающих психологические механизмы ощущения и восприятия.

Список используемых источников

1. Белова Е. В. Формирование системного мышления и лидерских компетенций у студентов и аспирантов технических вузов : монография; СПбГУТ. СПб., 2018. 198 с.
2. Андреева Н. Г. Структурно-функциональная организация нервной системы: учебное пособие / Под. ред. А. С. Батуева. СПб. : Изд-во С.-Петерб. Ун-та, 2003. 264 с.
3. Душков Б. А., Ломов Б. Ф., Рубахин В. Ф., Смирнов Б. А. Основы инженерной психологии / Под ред. Б. Ф. Ломова. М. : Высшая школа, 1986. 448 с.
4. Маклаков А. Г. Общая психология. СПб. : Питер, 2001. 592 с.

УДК 004.72 (004.77)

OTT УСЛУГИ В СЕТЯХ LTE

И. А. Белозерцев, В. С. Елагин

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

В мобильных сетях четвертого поколения LTE операторы связи могут предложить свои услуги для передачи голосового трафика. Но пользователи предпочитают использовать услугами OTT провайдеров. В этом случае оператор связи используется как транспортная среда, из-за чего страдает качество голосового трафика абонента. Поэтому важно идентифицировать трафик OTT услуг и обеспечить качество его передачи.

Quality of Service, QoS, Quality of Experience, QoE, OTT сервисы.

Over-The-Top (OTT) – термин, обозначающий предоставление аудио, видео и других видов услуг, передаваемых через Интернет. Доставка контента осуществляется от провайдера контента до оборудования пользователя через сеть оператора связи, но без прямого контакта с ним.

Как видно из определения, OTT услуги являются самостоятельной единицей, которая не контролируется оператором связи. Для пользователей это является преимуществом: не требуется тратить деньги на голосовые услуги. Необходим только безлимитный доступ в Интернет.

Но, как и во всех услугах для передачи голоса, есть некоторые проблемы при использовании:

- задержки и нечеткое звучание;
- качество связи не гарантируется;
- скорость передачи данных;
- пропускная способность на краю соты;
- эффективность передачи коротких сообщений.

Чтобы показать, что OTT сервисы не соответствуют стандартам качества, представленные ITU в рекомендации G. 114 [1], и несут в себе большое неудобство для конечного пользователя, был проведен эксперимент, где совершался вызов с помощью OTT приложения Skype с мобильного терминала на ПК. Сам мобильный терминал был зарегистрирован в сети LTE оператора связи. Помимо этого, важным элементом связи для Skype в данном случае является его сервер, через который и происходит обмен пакетами. На рис. 1 представлена схема для измерения основных характеристик качества связи.

Рис. 1. Установка для измерения показателей качества

В ходе эксперимента измерялись 3 важных показателя качества для оценки того или иного сервиса: джиттер, задержка и потери пакетов. Были проведены несколько экспериментов для наиболее полной картины. Ниже (рис. 2–4) представлены наиболее показательные результаты измерений, согласно которым и можно сказать, что OTT сервисы далеки от идеалов качества, которым должны соответствовать услуги связи.

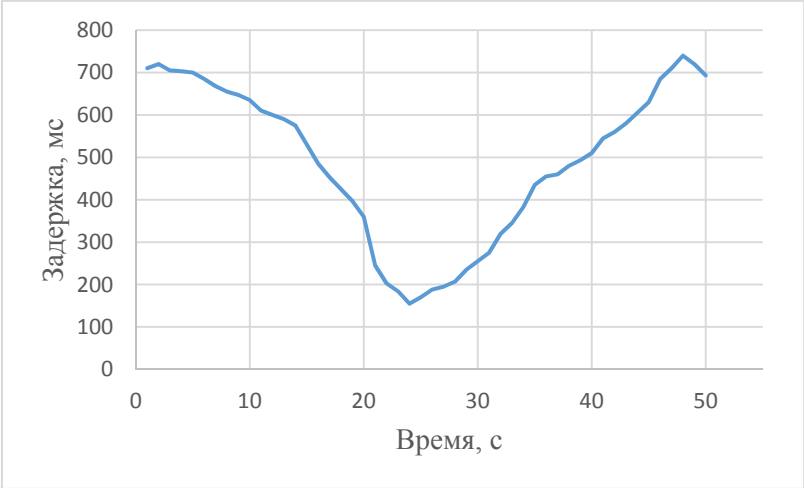


Рис. 2. Показатели задержки

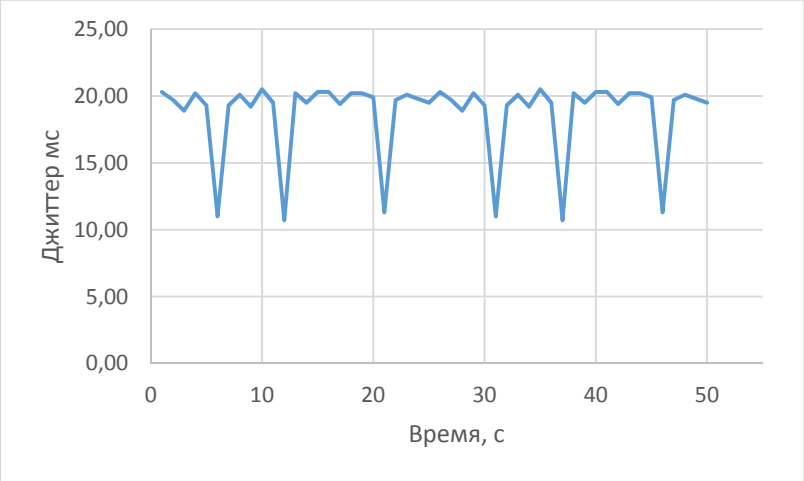


Рис. 3. Показатели джиттера

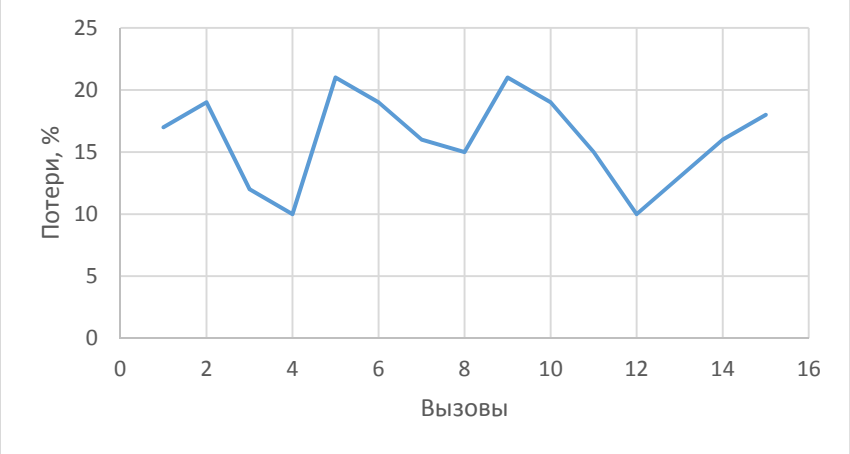


Рис. 4. Показатели потерь

В соответствии с приведёнными измерениями, можно подтвердить, что услуги, предоставляемые OTT провайдерами, не соответствуют требованиям качества связи для голосовых услуг в IP сетях. Из-за этого отклонения от показателей качества связи будет страдать конечный пользователь.

OTT услуги являются доступными и распространёнными, но не являются гарантом качества для своих пользователей. Помимо этого, для операторов связи представленные услуги несут свои неудобства, связанные с недобором прибыли. Поэтому важно найти способы идентификации услуг и гарантировать достойный уровень обслуживания со стороны оператора мобильной связи.

Имея результаты измерений задержки сигнала при передаче голосовой информации OTT сервисов, получим закон распределения случайно величины задержки. Эти значения, измеренные в мс, представлены в виде вариационного ряда в таблице. Необходимо построить статистический ряд, где число измерений $n = 50$.

ТАБЛИЦА. Результаты измерений задержки

i	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
x_i	155	167	170	184	195	203	207	223	235	246
i	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**
x_i	250	275	287	296	305	317	328	345	360	383
i	**21**	**22**	**23**	**24**	**25**	**26**	**27**	**28**	**29**	**30**
x_i	417	435	453	455	460	483	493	510	530	545
i	**31**	**32**	**33**	**34**	**35**	**36**	**37**	**38**	**39**	**40**
x_i	560	575	580	590	600	610	630	635	647	655
i	**41**	**42**	**43**	**44**	**45**	**46**	**47**	**48**	**49**	**50**
x_i	668	685	685	693	700	705	710	720	720	740

Любое измерение рассматривается как процесс, в результате которого уменьшается исходная неопределённость в сведениях об измеряемой величине – x. Количественной мерой неопределённости является энтропия – H(x). Чаще мы сталкиваемся с дискретными значениями случайной величины x_1, $x_2 \ldots x_n$, что обусловлено широким распространением средств вычислительной техники. Для таких величин приведём формулу, которая многое объясняет [2]:

$$H(x) = -\sum_{i=1}^{n} p_i * \lg(p_i),$$

где p_i – вероятность того, что случайная величина x приняла значение x_i. Поскольку $0 \le p_i \le 1$, а при этом $\lg(p_i) < 0$, то для получения $H(x) \ge 0$ перед суммой в формуле стоит знак минус.

В процессе измерения исходная неопределённость величины x уменьшается, поскольку знание о величине x возрастает. Однако и после измерения остаётся остаточная неопределённость $H(\Delta)$, которая связана с погрешностью измерений Δ.

Остаточную энтропию $H(\Delta)$ можно определить по приведенной формуле, при этом использовав энтропийное значение погрешности Δ для любого закона распределения:

$$\Delta = \pm\frac{1}{2}e^{H(\Delta)}.$$

Для того, чтобы определить закон распределения случайной величины, необходимо для его вычисления применить энтропийное значение погрешности:

$$\Delta = \frac{1}{2}\mathrm{e}^{H(\Delta)} = \frac{1}{2} * h * n * 10^{-\frac{1}{n}*\sum_1^y n_i * \lg(n_i)}.$$

Для окончательного решения нашей задачи нам понадобятся ещё два значения энтропийного коэффициента k и контрэксцесса χ [3]:

$$k = \frac{\Delta}{\sigma}, \quad (1)$$

$$\chi = \frac{\sigma^2}{\sqrt{\mu_4}}. \quad (2)$$

Используем (1) и (2) и получим значения k = 1,411 и χ = 0,83. После этого, зная значения энтропийного коэффициента k и контрэксцесса χ, используем [4, 5] для определения закона распределения случайно величины. В итоге получился двухмодальный закон распределения (рис. 5).

По полученным данным можно утверждать, что значения задержки при использовании OTT услуг много значений, которые предлагает ITU в рекомендации G. 114. При этом пакет проходит через множество элементов сети связи на своем пути: радио часть, оборудование LTE на опорной сети оператора связи, оборудование на транспортной сети, сервера самого OTT провайдера. То есть множество вещей влияют на время и качество доставки самого пакета. Поэтому, используя информацию, полученную с помощью результатов эксперимента, и полученный закон распределения, в дальнейшем стоит задача поиска механизмов или моделей для переноса задержи из области критических значений в область, которая будет удовлетворять стандартам ITU.

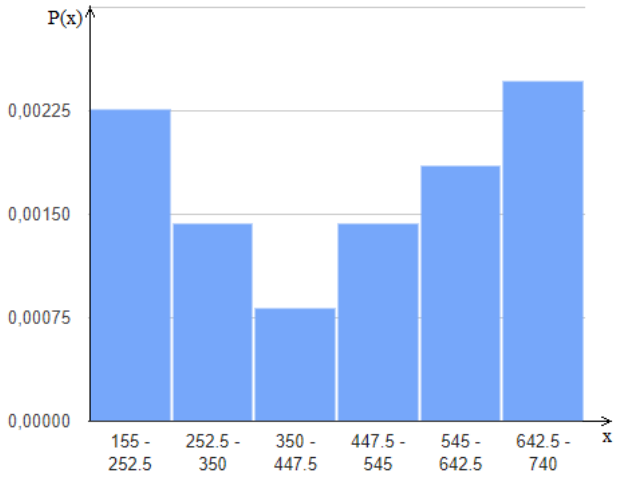


Рис. 5. Двумодальное распределение

Список используемых источников

1. Recommendation G.114: One-way transmission time. International Telecommunication Union, 2003. 20 p.

2. Тарасенко. Ю. Вероятностный и информационный анализ результатов измерений на Python [Электронный ресурс] // Хабрахабр. 2017. 1 июля. URL: https://habrahabr.ru/post/332066/ (дата обращения 15.08.2017).

3. Новицкий П. В., Зограф И. А. Оценка погрешностей результатов измерений. 2-е изд., перераб. и доп. Л. : Энергоэмиздат, 1991. 576 с.: ил. ISBN 5-283-04513-7.

4. Новицкий П. В. Основы информационной теории измерительных устройств. Л. : Энергия, 1968. 248 с.

5. Алексеева И. У. Теоретическое и экспериментальное исследование законов распределения погрешностей, их классификация и методы оценки их параметров : дис. … канд. техн. наук. Ленинград, 1975. 20 с.

УДК 004.056.5

СОВРЕМЕННЫЕ ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ ВНУТРЕННЕЙ БЕЗОПАСНОСТИ РАСПРЕДЕЛЕННОЙ СЕТИ ОРГАНОВ ГОСУДАРСТВЕННОЙ ВЛАСТИ

Э. В. Бирих[1], А. С. Гаврилов[1], Е. Н. Сацук[2]

[1]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
[2]Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций

При выполнении своих задач государственные организации все больше зависят от функционирования информационных систем и их безопасности. Обратной стороной использования информационных технологий являются угрозы, количество которых в распределенных сетях неуклонно растет. В статье рассмотрены некоторые рекомендации обеспечения безопасности.

информационная безопасность, распределенные сети, риски ИБ, внешние угрозы, внутренние угрозы, модель нарушителя.

При выполнении своих задач государственные организации все больше зависят от функционирования информационных систем и их безопасности. В эпоху цифрового общества они должны уметь быстро реагировать на изменения и устранять коммуникационные барьеры, предоставляя сотрудникам из всех подразделений возможности для эффективного взаимодействия в реальном времени и совместного использования информации, оборудования и сервисов, при этом быстром развитии систем и расширении функционала очень важно обращать внимание на безопасность этих систем.

Государственные органы, которые имеют филиалы в пределах города, региона или страны, стремятся объединить их в единую структуру, чтобы сотрудники могли пользоваться одной системой документооборота, иметь общие контакты, тратить как можно меньше ресурсов на телефонные разговоры, пересылку документов, командировки. Система конференцсвязи, функционирующая в правильно настроенной сети с достаточной пропускной способности каналов, способна заменить собрания руководителей филиалов и поездки сотрудников. Территориально-распределенные сети могут стабильно функционировать только при наличии высокопроизводительных сетей передачи данных. Кроме того, такие ИВС должны обеспечивать безопасную передачу данных, быть удобными в использовании и администрировании [1].

Важной частью управления информационной безопасностью является создание исчерпывающего перечня всех возможных угроз для определенных активов организации. Модель угроз должна содержать ранжированные данные о существующих угрозах, их актуальности, возможности реализации и последствий. Это позволяет выработать экономически эффективные защитные меры, повысить уровень информационной безопасности. Спектр угроз, который определяется особенностями конкретной информационной системы, её объектов и характером потенциальных действий источника, будет разным для различных ИС. Наиболее оптимальным вариантом для территориально распределенной сети является создание базовой модели угроз и разработка частных моделей угроз для конкретных объектов [2].

Под угрозами информационной безопасности понимается множество условий и факторов, которые создают опасность несанкционированного, в том числе случайного, доступа к данным, следствием которого может стать утечка конфиденциальной информации, уничтожение или ее изменение [3].

Данные угрозы присутствуют на любом участке распределенной сети. Многие организации в первую очередь защищаются от внешних угроз и часто забывают о наличии внутренних нарушителей. Исходя из отчетов по информационной безопасности, именно халатное поведение сотрудников является причиной 50 % утечек конфиденциальной информации [4].

Действия сотрудника организации, связанные с нарушением режима безопасности, разделяют на две категории: умышленные и неумышленные действия.

Умышленные действия подразумевают под собой: кражу корпоративной информации, ее модификацию, либо ее уничтожение (диверсия). Диверсия – это крайний случай и с ним необходимо бороться, привлекая сотрудников внутренних дел.

К неумышленным действиям можно отнести утрату носителя информации, искажение данных либо полное уничтожение информации по неосторожности и т. д. Во многих случаях именно неумышленные действия чаще всего наносят ущерб информационной безопасности.

Ограниченные ресурсы и постоянно меняющийся ландшафт угроз и уязвимостей делают невозможным полное снижение всех рисков. Специалисты по безопасности должны иметь набор средств, который поможет оценить воздействие рисков на деятельность организации и, если необходимо, снизить их до приемлемого уровня.

Для формирования понимания приоритетности мероприятий, направленных на повышение уровня ИБ, должна разрабатываться модель угроз, которая позволяет направить все усилия на защиту от наиболее вероятных угроз, снизить вероятность потерь и минимизировать затраты. Это делается

потому, что бессистемное и выборочное внедрение защитных мер не может обеспечить необходимого уровня защищенности.

Для решения данных проблем предлагается [5]:

1) Разрабатывать политику безопасности в соответствии с необходимыми требованиями для обеспечения информационной безопасности, которая безоговорочно должна выполняться сотрудниками организации в любой ситуации.

2) Описание прав доступа в помещения/к устройствам. Есть определенные помещения, например, серверные, доступ к которым должен быть только для ограниченного круга лиц. В данном помещении возможно узнать что-то о функционировании существующей сети и т. д., что можно использовать для нанесения угроз информационной безопасности или просто случайно повредить/сломать

3) Сохранение в тайне документов с информацией о защищаемой сети. Источником информации могут служить: документы, содержащие информацию о защитных средствах, отчеты по внутреннему и внешнему аудиту.

4) Проведение различных мероприятий для определения вероятности нанесения угроз тем или иным сотрудником, а в соответствии с этим выполнять расстановку и ротацию кадров, распределение прав доступа и т. д.

5) Использование автоматических систем мониторинга, позволяющих анализировать трафик и выявлять угрозы своевременно (например, *siem*).

Заключение

Информационная безопасность на предприятии в значительной степени зависит от персонала, который представляет значительную угрозу информационной системе предприятия, и, как следствие, влечет за собой причинение ущерба деятельности предприятия.

С целью снижения рисков информационной безопасности предприятия формируется модель нарушителя, разрабатывается политика безопасности. Режимные мероприятия и организационно – технические меры направлены на предотвращение и пресечение несанкционированных действий; подбор и расстановку кадров; допуск физических лиц в контролируемую зону и к средствам вычислительной техники; контроль за порядком проведения работ.

Защита информации от потерь, искажений и, самое главное, от утечки по всем возможным каналам должна осуществляться комплексно и системно. Применение различных способов и методов защиты информации, как и организация работ в области обеспечения информационной безопасности проводятся, как правило, в рамках определенной политики безопасности предприятия.

Список используемых источников

1. Орлов С. Распределенная сеть под защитой [Электронный ресурс] // Журнал сетевых решений/LAN. 2015. № 11 (224). URL: https://www.osp.ru/lan/2015/11/13047560/
2. Приказ ФСТЭК России от 13.02.2013 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».
3. Доктрина информационной безопасности Российской Федерации: Утверждена Указом Президента от 5 декабря 2016 г. № 646.
4. Исследование утечек конфиденциальной информации в первом полугодии 2017 год [Электронный ресурс] // Отчет INFOWATCH за первое полугодие 2017. URL: https://www.infowatch.ru/report2017_half
5. Приказ ФСТЭК России от 11.02.2014 «Меры защиты информации в государственных информационных системах».

Статья представлена научным руководителем, кандидатом технических наук, доцентом Д. В. Сахаровым.

УДК 004.056.2

ИССЛЕДОВАНИЕ ВОПРОСОВ ПОВЫШЕНИЯ УРОВНЯ ЗАЩИЩЕННОСТИ ОРГАНОВ ИСПОЛНИТЕЛЬНОЙ ВЛАСТИ

Э. В. Бирих, А. Д. Кошурин, Д. В. Кушнир, Д. Д. Стародубова

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

Информационная безопасность органов исполнительной власти включает в себя обеспечение безопасности информации и информационных ресурсов, безопасности телекоммуникаций и информационного обмена. В статье рассматриваются вопросы, связанные с обеспечением технической защиты информации в органах исполнительной власти.

информационная безопасность, исполнительная власть, техническая защита, требования, нормативные документы.

В настоящее время особенно важным с точки зрения защиты информации организаций системы исполнительной власти является повышение уровня защищенности путем анализа рисков, связанных с осуществлением угроз безопасности, оценку текущего уровня защищенности, локализацию узких мест в системе защиты, оценку соответствия требованиям нормативных документов и стандартов в области информационной безопасности.

Информатизация во всех сферах деятельности на базе широкого использования программно-аппаратных средств зарубежного производства, при отсутствии единой централизованной методологии по построению ведомственных и территориальных информационно-коммуникационных систем, привела к бесконтрольному созданию и дублированию информационных ресурсов, появлению множества трудно выявляемых точек доступа к ним. Эти обстоятельства, в условиях хорошо развитых технических средств разведки и широких возможностей, практически официального их использования, а также низкое качество существующих средств защиты, привели к возникновению широкого спектра угроз, формированию нетрадиционных технических и иных каналов утечки информации, равно как и способов несанкционированного доступа к ней.

Актуальность проблемы обеспечения безопасности информации в структурах органов исполнительной власти обусловлена, кроме того, необходимостью принятия эффективных, адекватных политическим задачам, управленческих решений. Во-первых, зависимость от информации и информационных технологий становится одним из качественных состояний формирующегося общества. Обладание своевременными, точными, достоверными данными служит чрезвычайно важным фактором эффективности принятия управленческих решений, как на государственном уровне, так и на уровне субъектов Федерации. Качество функционирования и безопасность информационной сферы, как и состояние правового регулирования отношений в данной сфере определяют уровень развития государства. Как стратегический ресурс информация требует особого государственного отношения не только в смысле её развития и накопления, но и защиты. Во-вторых, обеспечение информационной безопасности сопряжено с вопросами обеспечения технологической безопасности страны. Представляет также значительный интерес рассмотрение проблемы соотношения возможностей средств защиты и средств несанкционированного сбора, обработки и доступа к информационным ресурсам, наличия протоколов взаимодействия пользователей и информации, с учётом степени её важности и секретности, состояния социально-экономической и общественно-политической обстановки в стране и её субъектах. Все это, как и научный поиск комплексных мер, средств и методов совершенствования системы информационной безопасности политических структур, повышения управленческого потенциала, главным образом органов исполнительной власти, обусловливает высокую степень актуальности затронутой темы.

В основу процесса исследования повышения уровня защищенности органов исполнительной власти легли вопросы, связанные с обеспечением защиты информации от утечки по техническим каналам при её обработке, хранении и передачи. Вместе с этим, повышение информационной безопасности органов исполнительной власти тесно связано с рядом нормативных

правовых актов, обеспечивающих их информационные потребности, безопасность информации и информационных ресурсов, а также безопасность телекоммуникаций и информационного обмена.

Так, пункт 5 статьи 6 ФЗ № 187 «О безопасности критической информационной инфраструктуры Российской федерации», определяет следующее: «Федеральный орган исполнительной власти, осуществляющий функции по выработке и реализации государственной политики и нормативно-правовому регулированию в области связи, утверждает по согласованию с федеральным органом исполнительной власти, уполномоченным в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, порядок, технические условия установки и эксплуатации средств, предназначенных для поиска признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов критической информационной инфраструктуры» [1].

Безопасность информации, находящейся в обороте органов исполнительной власти, обеспечивается различными мерами: организационными, техническими, правовыми. Согласно ст. 16 Федерального закона от 27 июля 2006 г. № 149 «Об информации, информационных технологиях и о защите информации» указанные меры по защите информации направлены: на обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации; соблюдение конфиденциальности информации ограниченного доступа; реализацию права на доступ к информации [2].

Перечисленные выше меры отображают установление в отношении конкретных видов информации правового режима и обеспечение его соблюдения.

Безопасность телекоммуникаций и информационного обмена – одна из составляющих информационной безопасности органов исполнительной власти. Информационные технологии нашли широкое применение в управлении важнейшими объектами жизнеобеспечения, которые становятся более уязвимыми перед случайными и преднамеренными воздействиями. Повышение уязвимости связано с целым рядом факторов, основными из которых являются снижение уровня международной безопасности; развитие международного терроризма; увеличение количества потенциально опасных объектов, многие из которых расположены в крупных городах [3].Один из принципиальных факторов – существенная зависимость национальных инфраструктур России от зарубежных технологий, что обусловило возникновение новых угроз, которые связаны, прежде всего, с возможностью использования информационно-коммуникационных технологий в целях,

несовместимых с национальными интересами. Государством на ближайшее будущее предусмотрены разработка и запуск специальной программы импортозамещения продукции в сфере информационных технологий для решения задач отдельных государственных структур и организаций, включающий запуск разработки широкой номенклатуры продукции, обладающей высоким уровнем информационной безопасности.

На базе одного из последних документов, посвященных информационной безопасности, Указа Президента РФ от 22 мая 2015 г. № 260 «О некоторых вопросах информационной безопасности Российской Федерации» [4]. На основании документа, сегмент международной компьютерной сети Интернет для федеральных органов государственной власти и органов государственной власти субъектов РФ, находящийся в ведении Федеральной службы охраны РФ, должен быть преобразован в российский государственный сегмент информационно-телекоммуникационной сети Интернет. Согласно указу, подключение российских государственных органов к Интернету должно происходить по защищенным каналам связи с использованием средств шифрования.

Таким образом, угроза защиты информации сделала направление по обеспечению информационной безопасности одним из обязательных аспектов работы органов исполнительной власти.

Список используемых источников

1. О безопасности критической информационной инфраструктуры Российской федерации: федер. закон от 26 июля 2017 №187. URL: http://www.consultant.ru/document/cons_doc_LAW_220885/

2. Об информации, информационных технологиях и о защите информации: федер. закон от 27 июля 2006 № 149. URL: http://www.consultant.ru/document/cons_doc_LAW_61798/

3. Еремеев М. А., Ломако А. Г., Овчаров В. А., Акулов С. А., Коротков В. С., Свергун Н. В. Метод адаптивного управления активным сетевым оборудованием телекоммуникационной сети в условиях компьютерных атак // Информационное противодействие угрозам терроризма. 2012. № 19. С. 136–146.

4. О некоторых вопросах информационной безопасности Российской Федерации: указ Президента РФ от 22 мая 2015 № 260. URL: http://www.consultant.ru/document/cons_doc_LAW_179963/

УДК 004.056

К ВОПРОСУ ОБ АУДИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

Э. В. Бирих, С. С. Ферапонтова

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

В настоящий момент защита персональных данных является одной из актуальных задач многих российских компаний. Это происходит вследствие увеличения количества проверок со стороны органов надзора и увеличение жалоб от субъектов персональных данных. В статье рассматриваются категории обработки персональных данных, а также требования по обработке и защите персональных данных в информационных системах обработки персональных данных, предъявляемые операторам в зависимости от их вида, для прохождения аудита политики безопасности персональных данных.

информационная безопасность, аудит, персональные данные, защита информации, оператор персональных данных.

В наше время обеспечение безопасности персональных данных (ПДн) это необходимая мера для любых операторов ПДн. Аудит политики безопасности персональных данных помогает определить, качественно ли выполняется защита персональных данных и соответствует ли она актуальным требованиям законодательства [1].

Основным документом, в котором регулируется деятельность по обработке, защите и использованию персональных данных, является Федеральный закон РФ от 27 июля 2006 года № 152-ФЗ «О персональных данных». В нем говорится о том, что все операторы ПДн обязаны:

1. Уведомить уполномоченный орган по защите прав субъектов о том, что они собираются обрабатывать ПДн (за исключением некоторых случаев, предусмотренным законом).

2. Обрабатывать и защищать ПДн субъектов ПДн в соответствии с требуемыми нормами законодательства [2].

При этом операторы ПДн делятся на 4 категории: муниципальные, государственные организации, физические и юридические лица. В зависимости от категории оператора и категории ПДн, обрабатываемых оператором, к нему предъявляются различные требования по защите ПДн [3].

В таблице представлены примеры категорий персональных данных, которые обрабатывает тот или иной оператор.

ТАБЛИЦА. Примеры категорий обработки ПДн в зависимости от типа оператора

Вид оператора	Категории обрабатываемых ПДн
Государственная или муниципальная организация	*Персональные данные субъектов ПДн*
	ФИО; информация о дате и месте рождения; адрес места жительства; семейное положение; социальное положение; имущественное положение; сведения о ближайших родственниках (ФИО, степень родства, дата рождения); информация о доходах; паспортные данные (серия, номер, когда и кем выдан, код подразделения); данные Пенсионного страхового свидетельства данные ИНН; сведения о заключении/расторжении брака; место работы; должность; состав семьи; телефоны (домашний и сотовый); сведения о рождении детей; ИНН; трудовой стаж; фотография.
	Персональные данные работников оператора, а также родственников работника
	ФИО; паспортные данные; дата рождения; место рождения; адрес места проживания; информация об образовании; профессия; номер страхового свидетельства государственного пенсионного страхования; сведения о медицинском полисе; данные о воинском учете; данные о месте работы; должности; трудовой стаж; ИНН; сведения о рождении детей, о заключении/расторжении брака; семейное положение; сведения о родственниках работника (ФИО; степень родства дата рождения); номера телефонов [4].
Юридическое лицо	ФИО; информация о дате и месте рождения; пол субъекта; информация из документов, удостоверяющих личность (данные паспорта: серия, номер, когда и кем выдан, код подразделения); адрес места фактического проживания и регистрации; электронная почта; номера телефонов (мобильного, городского домашнего и рабочего) [5].
Физическое лицо	ФИО; информация о дате и месте рождения; информация из документов, удостоверяющих личность (серия, номер, когда и каким органом выдан, код подразделения); номер телефона; адрес; адрес электронной почты; ИНН; стаж труда; доходы; должность; звание, ученая степень; номер страхового свидетельства государственного пенсионного страхования [6].

Требования по защите и обработке персональных данных для муниципальных или государственных организации, физических и юридических лиц устанавливаются:

1. Федеральным законом «О персональных данных» от 27.07.2006 № 152-ФЗ.

2. Приказом Федеральной службы по техническому и экспортному контролю от 18.02.2013 № 21 (ред. от 23.03.2017) «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

3. Постановлением Правительства РФ от 01.11.2012 N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

4. Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

Для определения требований по защите и обработке персональных данных для государственных и муниципальных организаций существует дополнительное постановление:

Постановление Правительства РФ от 21.03.2012 N 211 (ред. от 06.09.2014) «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».

Обобщив вышеперечисленные законодательные акты, ко всем операторам ПДн предъявляются следующие основные требования:

1. Оператор ПДн обязан предоставить в свободный доступ свою политику в отношении обработки персональных данных.

2. Оператор ПДн обязан сообщить цель обработки персональных данных субъекта.

3. Обработка ПДн оператором должна иметь под собой правовое обоснование.

4. Оператор обязан сохранять конфиденциальность ПДн.

5. Оператору рекомендуется указывать сроки хранения ПДн.

6. Оператор обязан следить за актуальностью ПДн и исправлять неточности.

7. В случае неправомерной обработки ПДн оператор обязан немедленно ее прекратить.

8. При отзыве субъектом ПДн своего согласия на обработку ПДн, данные должны быть уничтожены (за исключением отдельных случаев).

9. Оператор не имеет права осуществлять обработку ПДн без согласия субъекта ПДн.

10. Оператор ПДн обязан предоставить субъекту ПДн информацию об обработке ПДн этого субъекта.

11. Оператор обязан защищать ПДн от неправомерного доступа, удаления, копирования и других неправомерных действий.

Сравнивая требования по обработке персональных данных, предъявляемые физическим и юридическим лицам с государственными и муниципальными организациями, оказалось, что требования по обработке ПДн для государственных и муниципальных предприятий являются более строгими и полными в силу дополнительного постановление Правительства РФ от 21.03.2012 N 211. Также отмечается, что выполнение операторами персональных данных предписанных требований законодательства в отношении политики обработки персональных данных, поможет оператору успешно пройти аудит политики безопасности ПДн и защитить персональные данные.

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. 1. С. 27–30.

2. О персональных данных: федер. закон от 27 июля 2006 N 152-ФЗ (последняя редакция). URL: http://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения 26.03.2018).

3. Андрианов В. И., Виткова Л. А., Сахаров Д. В. Исследование алгоритма защиты общедоступных персональных данных в информационных системах // Актуальные проблемы инфотелекоммуникаций в науке и образовании. V международная научно-техническая и научно-методическая конференция: сб. науч. ст. 2016. С. 227–231.

4. Политика в области обработки и защиты персональных данных в муниципальном казенном учреждении «Многофункциональный центр оказания государственных и муниципальных услуг» [Электронный ресурс]. URL: https://admmegion.ru/org/municipal/mku_mfc/laws/index.php?ELEMENT_ID=293745 (дата обращения 27.03.2018).

5. Политика обработки и защиты персональных данных ООО «ММС РУС» [Электронный ресурс]. URL: http://www.mitsubishi-motors.ru/pdp_policy/ (дата обращения 28.03.2018).

6. Политика в отношении обработки персональных данных в ИП Клопов [Электронный ресурс]. URL: http://interer-architects.ru/files/politika_v_otnoshenii_obrabotki_dannyh_2.pdf (дата обращения 28.03.2018).

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

УДК 004.7

МОДЕЛЬ ПРИМЕНЕНИЯ НЕЙРОННЫХ СЕТЕЙ ДЛЯ УПРАВЛЕНИЯ СЕТЯМИ SON

А. А. Бородинский, А. Б. Гольдштейн

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

В данной статье анализируется возможность применения нейронной сети для управления сетями SON. Описание функций, которые могут выполнять нейронные сети, в том числе: маршрутизация сети, распределение каналов в сетях LTE, автоматическая конфигурация оборудования в сети, восстановление сети в случае аварий. Так же будет описана предлагаемая модель, в которой возможно внедрение нейронной сети совместно с сетью SON и актуальность данного технического решения.

нейронная сеть, модель, обучение нейронной сети, конфигурация, оптимизация, восстановление, самоорганизация, управление сетями.

Введение

Современные сети, в частности LTE, предполагают автоматизацию большинства процессов, связанных с управлением сетью, маршрутизацией, а также другими аспектами организации их работы и эксплуатации. Одним из вариантов достижения этих целей является концепция SON (*Self-Organizing Networks*), которую описывает 3GPP консорциум [1]. Три основные задачи, которые возлагаются на SON это:

Самоконфигурация – включает в себя добавление и изменение конфигурации новых и уже существующих сетевых элементов.

Самооптимизация – включает в себя управление производительностью сетевых устройств в зависимости от требуемых ресурсов в данный момент.

Самовосстановление – включает в себя действия, направленные на восстановление работы SON LTE сети в случае сбоя [2].

Несмотря на некоторый застой в развитии этой концепции на другие сети, кажется интересным рассмотреть варианты расширения возможностей управления сетями, в частности, аспекты применения нейронных сетей для совершенствования работы SON сегмента.

Нейронные сети в сегменте телекома

Нейронная сеть представляет собой модель биологической нейронной сети мозга, в которой нейроны имитируются относительно простыми, часто однотипными элементами (искусственными нейронами). Нейронная сеть

представляет собой совокупность нейронов, которые составляют слои. В каждом слое нейроны между собой никак не связаны, но связаны с нейронами предыдущего и следующего слоев. Количество слоев и нейронов в них определяет точность и достоверность получаемых результатов при решении задач, т. е. чем больше слоев и нейронов на каждом слое – тем меньше ошибок и выше надежность работы сети [3].

В сфере телекоммуникаций на сегодня уже описаны некоторые задачи, которые можно решить при помощи нейронных сетей. Например, это:

1. Распределение каналов в сотовых радиосетях, в том числе решение задачи назначения частот и прогнозирования напряженности поля.

2. Территориальное планирование сотовых сетей подвижной радиосвязи, в ходе которого выбирается структура (конфигурация) сети и места размещения базовых станций, рассчитывается возможность обеспечения охвата (покрытия) требуемой зоны обслуживания с заданным качеством связи и емкость сети, требуемая для обслуживания абонентской нагрузки с заданной интенсивностью потерь (отказов в обслуживании).

3. Снижение временных затрат при выполнении задач маршрутизации в сети.

Пример применения нейронной сети для сети SON

В предлагаемой нами модели (рис. 1) нейронная сеть развертывается на устройстве, осуществляющем управление SON (NMS), которое так же подключено к LTE сети и базе данных (*Database*), на которой хранятся шаблоны сценариев действий при определенных событиях (авария на сети, добавление нового устройства и другие). С помощью этих шаблонов и будет производиться обучение нейронной сети.

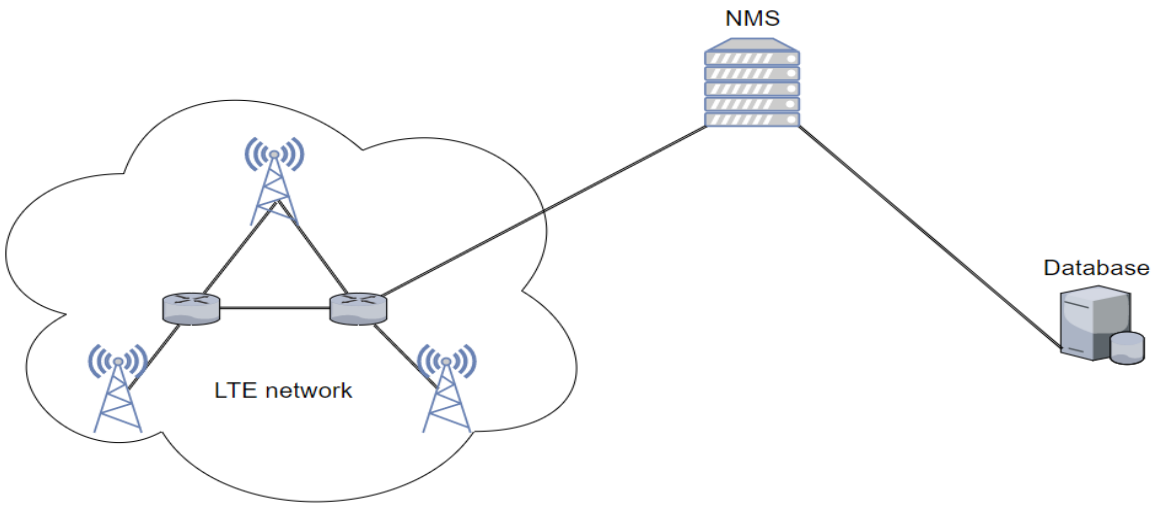


Рис. 1. Топология модели

Обучение нейронной сети возможно двумя вариантами:

1. С учителем: в виде учителя присутствует оператор, который будет анализировать решения, предлагаемые нейронной сетью, и давать нейронной сети обратную связь о том, насколько подходящим было решение. Постепенно, основываясь на ответах оператора, нейронная сеть будет выдавать более подходящие решения.

2. Без учителя: в данном случае нейронная сеть будет обучаться сама без присутствия оператора, основываясь только на данных об изменениях в SON LTE сети после последних действий. Чем больше изменений нейронная сеть совершит, тем лучше она будет понимать, как те или иные действия влияют на работу SON LTE сети.

Пройдя обучение (рис. 2), нейронная сеть сможет выполнять функции самоконфигурации, самооптимизации и самовосстановления, заложенные в SON, более эффективно.

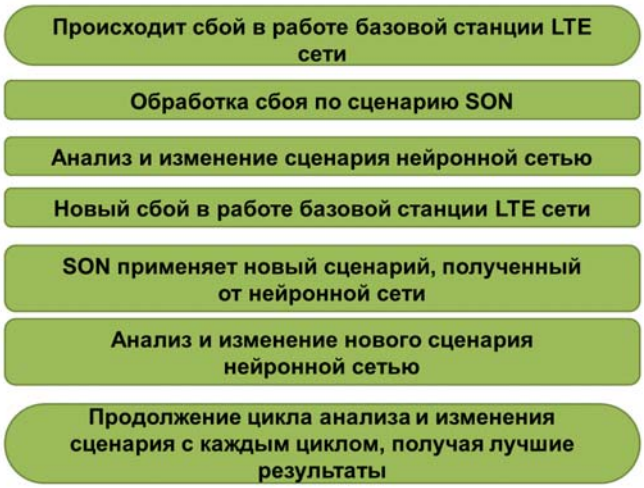


Рис. 2. Процесс обучения нейронной сети

Приведем пример возможного сценария, где реализована нейронная и SON на LTE сети совместно.

Абстрактный провайдер услуг построил новый участок сети и подключил его к своей сети. Механизмы SON запустят процессы конфигурации новых устройств и установки ПО. Спустя некоторое время на другом участке сети выходит из строя базовая станция. Стандартный сценарий SON выдает решение об увеличении мощности соседних базовых станций на 90 %. На следующем этапе подключается нейронная сеть, которая уже прошла несколько циклов обучения, описанных на рис. 2. Рекомендация нейронной сети по изменению сценария SON может быть в виде повышения мощности только на 50 %, исходя из опыта обработки предыдущих сбоев, тем самым уменьшив количество затрачиваемых ресурсов на восстановление участка сети.

Заключение

Таким образом, применение данной модели поставщиком сетевых услуг позволит: оптимизировать работу своих сетевых элементов, сократить штат работников, отвечающих за работу сети, и минимизировать потери при сбоях на участках LTE сети. Впоследствии все эти возможности могут быть

применены для управления любыми сетями, в том числе SDN, IMS, post NGN и т. д.

Список используемых источников

1. Гольдштейн А. Б., Кисляков С. В., Феноменов М. А. Управление сетями 3G: SON и явь // Мобильные коммуникации. 2015. № 3–4. С. 14–17.

2. Magdalena Nohrborg Self-Organizing Networks. URL: http://www.3gpp.org/technologies/keywords-acronyms/105-son

3. Николенко С. И., Кадурин А. А., Архангельская Е. О. Глубокое обучение. Погружение в мир нейронных сетей. СПб. : Питер, 2018. 480 с. ISBN 978-5-496-02536-2.

УДК 004.056

ПРОГРАММНЫЕ СПОСОБЫ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ ФУНКЦИОНИРОВАНИЯ СЕТЕВЫХ СИГНАТУРНЫХ СИСТЕМ ОБНАРУЖЕНИЯ АТАК

А. А. Браницкий

Санкт-Петербургский институт информатики и автоматизации Российской академии наук

Рассматриваются несколько приемов, направленных на повышение эффективности функционирования сетевых сигнатурных систем обнаружения атак. Среди предложенных подходов выделяются использование высокоскоростных драйверов захвата сетевых пакетов, балансировка сетевого трафика между несколькими процессами СОА, разработка модифицированных алгоритмов поиска шаблонных подстрок в сигнатурных правилах и т. д. Приводятся результаты экспериментальных исследований СОА.

система обнаружения атак, сигнатурный анализ, драйвер сетевой карты, балансировка сетевой нагрузки, алгоритм поиска подстрок.

Введение

С развитием информационных технологий возникают вопросы, связанные с обеспечением безопасности сетевых ресурсов. Для их решения могут применяться сетевые системы обнаружения атак (СОА), функционирование которых основано на сигнатурном анализе. Выявление вредоносной сетевой активности осуществляется при помощи механизма правил, включающих сопоставление с образцом, пороговый анализ, поиск подстрок. Целью данной работы является разработка подходов, направленных на повышение эф-

фективности функционирования (ускорение процессов обработки и фильтрации сетевых пакетов) таких систем, а также их экспериментальное исследование.

Повышение эффективности функционирования сетевых сигнатурных СОА

Выделим следующий набор программных способов повышения эффективности функционирования сетевых сигнатурных СОА:

– использование технологии PF_RING для ускорения перехвата пакетов;

– балансировка сетевой нагрузки между несколькими параллельно запущенными на одной машине копиями СОА;

– разработка параллельных модификаций алгоритмов поиска подстроки

– использование технологии XDP (*eXpress Data Path*);

– применение обработки агрегированных потоков, поступающих с нескольких netflow-сенсоров на IPFIX-коллектор;

– применение сетевых фильтров и экранов (*ipchains*, *pf*, *ipfw*, *iptables*) для блокировки аномальных соединений.

Отметим, что все из названных подходов не требуют существенной реорганизации архитектуры СОА. Эта особенность позволяет добавлять отдельные компоненты, которые встраиваются в СОА и повышают эффективность их функционирования. Для экспериментального исследования были выбраны первые три подхода.

Рассмотрим первый подход. Набор утилит PF_RING содержит в своем составе высокоскоростной аналог библиотеки libpcap с поддержкой механизма кольцевой буферизации пакетов. Память в таком кольце выделяется единожды, и при поступлении нового пакета его содержимое записывается на место самого старого элемента, находящегося внутри кольца. В пространстве пользователя непосредственный доступ к структуре захваченного на драйвере пакета осуществляется через системный вызов mmap. Кроме этого, в состав PF_RING входят следующие компоненты: модуль ядра Linux (*pf_ring.ko*) для хранения пакетов в кольцевом буфере, библиотека (*libpfring.so*) для построения пользовательских приложений, драйверы сетевых карт Intel (*e1000e*, *igb*, *ixgbe*, *i40e*, *fm10k*), а также базовые примеры сетевых приложений (*pfsend*, *pfcount*, *pfflow*, *pfbridge* и т. д.). При помощи специализированных драйверов сетевых карт Intel возможно использование режима zero-copy, который позволяет осуществлять эффективное пробрасывание пакетов в область пользовательских задач с обходом ядра (*bypassing the Linux kernel*).

Второй подход подразумевает разбиение анализируемого сетевого потока между несколькими независимыми процессами СОА. Для сохранения

механизма инспекции пакетов с хранением состояния (*stateful packet inspection*) балансировка должна выполняться таким образом, чтобы все пакеты, принадлежащие конкретной сессии, обрабатывались при помощи одного и того же процесса COA. В качестве простых правил балансировки трафика между n копиями COA можно назвать следующие: $(src\_ip + dst\_ip)\%n$, $\min(src\_ip, dst\_ip)\%n$, $f(src\_ip, dst\_ip)\%n$, где src_ip, dst_ip – IP-адреса отправителя и получателя, f – некоторая коммутативная функция. Результат применения правила представляет собой порядковый номер i-ого сетевого интерфейса, который прослушивается i-ым экземпляром COA ($0 \le i < n$). В экспериментах использовалось первое правило балансировки трафика, а именно сложение по модулю n.

В третьем подходе предлагается исследовать быстродействие алгоритмов поиска подстрок. Среди них были выбраны классический инкрементальный поиск, алгоритм Ахо-Корасик и алгоритм Бойера-Мура.

Результаты экспериментов

Для проведения первых двух экспериментов использовалась вычислительная платформа Supermicro X9DRD-iF 1.10 со следующей конфигурацией: 2 CPUs Intel(R) Xeon(R) CPU E5- 2630 v2 2.60Ghz (6 cores), 32KB L1-cache, 256KB L2-cache, 15360KB L3-cache; 8 RAMs 16384MB DDR3 1600MHz; 2 Ethernet controllers Intel I350 1Gb.

Схема проведения первого эксперимента представлена на рис. 1.

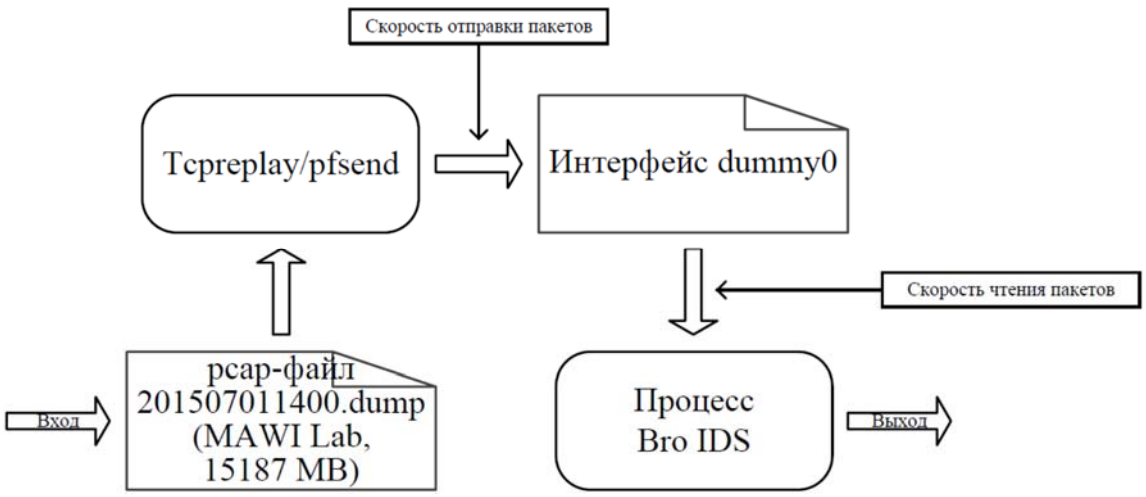


Рис. 1. Схема проведения первого эксперимента

В качестве исходного файла, хранящего образы сетевых пакетов, использовался файл 201507011400.dump из открытого набора MAWI Lab [1]. Содержимое этого файла считывалось при помощи утилит (I) tcpre-

play (без *pf_ring*) и (II) pfsend (*с pf_ring*), которые выполняли отправку пакетов на фиктивный сетевой интерфейс dummy0. Этот интерфейс прослушивался СОА Bro, которая в случае II запускалась с поддержкой модуля pf_ring [2]. Для случаев I и II на рис. 2 представлены кривые, отражающие число отброшенных пакетов в зависимости от скорости обрабатываемого трафика.

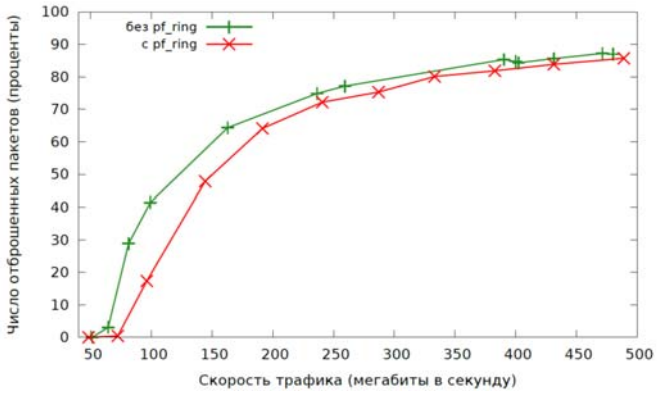


Рис. 2. Зависимость числа отброшенных пакетов от скорости трафика

Прирост производительности несущественный, поскольку при проведении эксперимента отрицательно сказывается малый размер пакетов [3] (средний размер пакета 56,54 байта, всего пакетов 219530230).

Схема проведения второго эксперимента представлена на рис. 3.

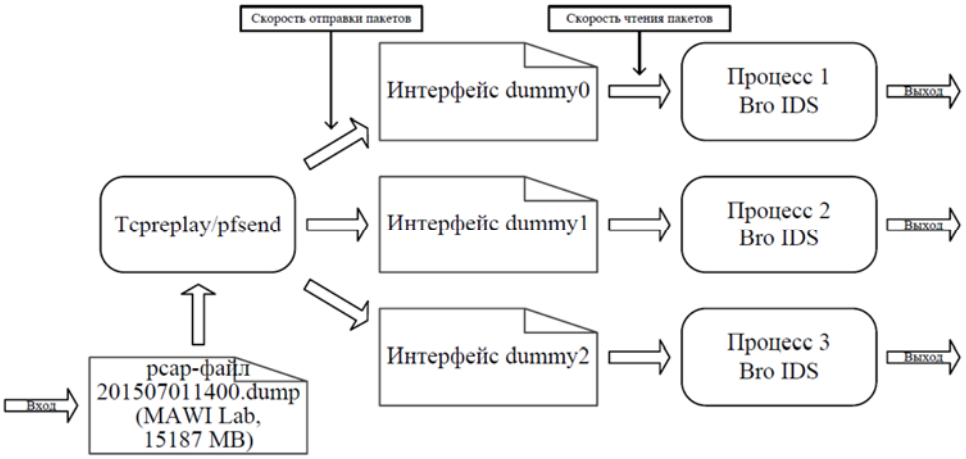
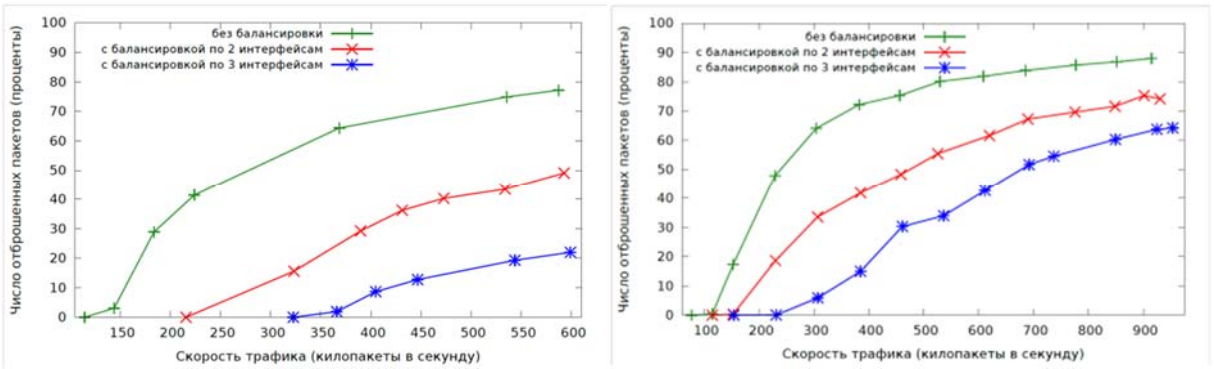


Рис. 3. Схема проведения второго эксперимента

Для этого эксперимента утилиты tcpreplay и pfsend были модифицированы таким образом, чтобы поступающий на их вход трафик распределялся по нескольким выходным интерфейсам. На рис. 4 показаны кривые, отражающие зависимость суммарного количества отброшенных пакетов от скорости трафика при балансировке по двум и трем интерфейсам как без применения pf_ring (рис. 4*а*), так и с применением pf_ring (рис. 4*б*).



а) без применения pf_ring б) с применением pf_ring

Рис. 4. Зависимость числа отброшенных пакетов от скорости трафика с балансировкой

Для рис. 4*а* число отбрасываемых пакетов на скорости около 600 Kp/s снизилось на 27–28 % при добавлении одного нового интерфейса. Для рис. 4*б* на скорости около 950 Kp/s этот показатель снизился на 10–13 %.

Схема проведения третьего эксперимента представлена на рис. 5.

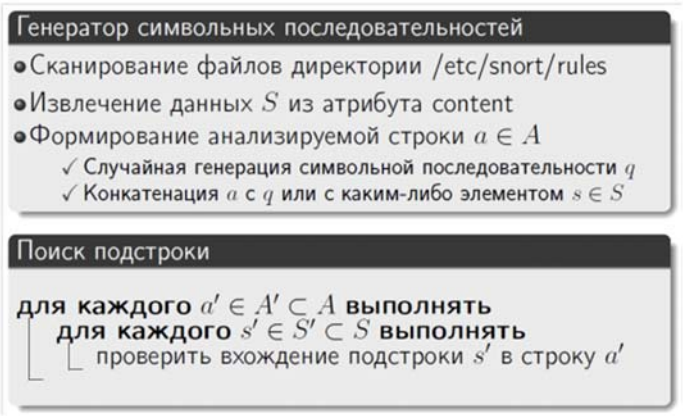


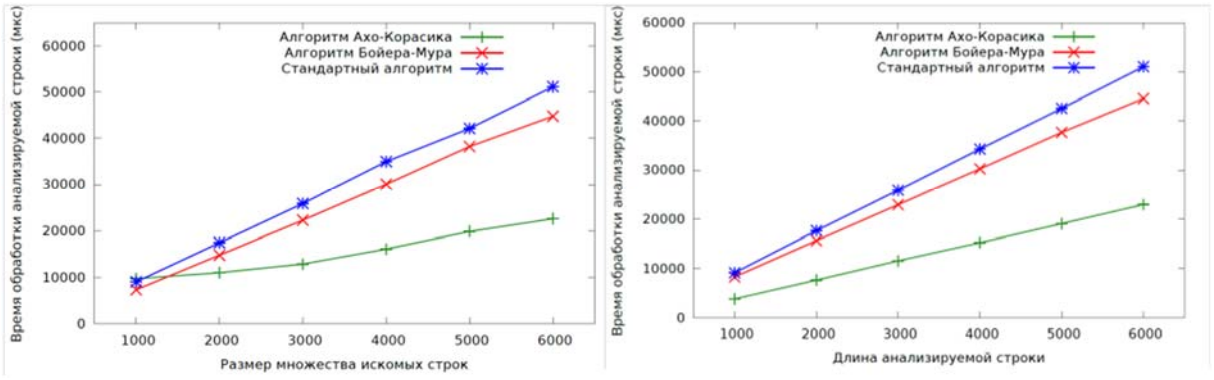
Рис. 5. Схема проведения третьего эксперимента

Для этого эксперимента использовалась машина со следующей конфигурацией: CPU Intel(R) Core(TM) i5-3210M 2.50 Ghz (2 cores); RAM 4GB DDR3 1600 MHz. На рис. 6 показаны кривые, отражающие время работы исследуемых алгоритмов в зависимости от размера множества искомых строк (рис. 6*а*) и длины анализируемой строки (рис. 6*б*).

Кроме того, были разработаны модификации алгоритмов Ахо-Корасик и Бойера-Мура, распараллеленные на уровне CPU и GPU, что позволило существенно повысить скорость анализа содержимого пакетов.

Заключение

Рассмотренные способы позволяют повысить эффективность функционирования сетевых сигнатурных СОА, что подтверждают результаты выполненных экспериментов. Дальнейшее направление – детальное исследование влияния различных параметров в предложенных подходах.



а) в зависимости от размера множества искомых строк

б) в зависимости от длины анализируемой строки

Рис. 6. Время обработки анализируемой строки для трех алгоритмов поиска подстрок

Список используемых источников

1. MAWI Lab Data set. URL: http://www.fukuda-lab.org/mawilab (дата обращения 27.03.18).

2. Bro plugin PF_RING. URL: https://github.com/ntop/bro-pf_ring (дата обращения 27.03.18).

3. Deri L. et al. Improving passive packet capture: Beyond device polling // Proceedings of the 4th International System Administration and Network Engineering Conference. 2004.

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

УДК 681.7.08

ВОПРОСЫ РЕАЛИЗАЦИИ АППАРАТНО-ПРОГРАММНОГО КОМПЛЕКСА ПРОГНОЗА ПАРАМЕТРОВ ПЕРЕДАЧИ РАЗЪЕМНОГО СОЕДИНЕНИЯ ПО РЕЗУЛЬТАТАМ ВИДЕОДИАГНОСТИКИ ТОРЦЕВОЙ ПОВЕРХНОСТИ ФЕРРУЛА ВОЛОКОННО-ОПТИЧЕСКОГО КОННЕКТОРА

А. В. Бурдин, А. М Гиниатулина, С. С. Пашин

Поволжский государственный университет телекоммуникаций и информатики

На сегодняшний день современные аппаратно-программные комплексы видеодиагностики волоконно-оптических разъемных соединений, представленные на рынке телекоммуникаций, предполагают оценивание качества коннектора исключительно по результатам проведения теста состояния поверхности феррул на уровне «PASS/FAIL» в соответствие с ратифицированным измерительным стандартом IEC 61300-3-35.

Однако прогноз максимального значения вносимых потерь на основе анализа изображения торца феррула позволил бы сделать однозначное заключение о необходимости проведения профилактических работ либо непосредственно замене коннектора как на этапах инсталляции и монтажа оконечных устройств коммутации, но и при дальнейшем мониторинге состояния кроссовых устройств в процессе технической эксплуатации линий передачи. В работе рассмотрены ключевые аспекты реализации данного аппаратно-программного комплекса, представлены результаты разработки отдельных элементов математического аппарата оценивания параметров передачи волоконно-оптического разъемного соединения по результатам анализа изображения торцевой поверхности феррула коннектора.

феррула, коннектор, вносимые потери, коэффициент отражения, снимок торца феррулы, загрязнение.

Разработка методики оценивания ключевых параметров передачи волоконно-оптических разъемных соединений непосредственно по результатам анализа фотографии торцевой поверхности феррулов коннекторов, полученных с помощью штатных полевых комплектов видеодиагностики безусловно является актуальной задачей. Данное направление представляет несомненный интерес для достаточно большого количества компаний-инсталляторов структурированных кабельных системы (СКС). В отличие от «традиционных» сетей широкополосного доступа, соединительные волоконно-оптические линии передачи (ВОЛП) подсистем СКС характеризуются малой протяженностью (буквально десятки – сотни метров). Поэтому весь комплекс приемо-сдаточных измерений, проводимый с помощью оптических рефлектометров обратного рассеяния во временной области (OTDR), обязательный для «традиционных» ВОЛП, в соответствие с РД 45.156-2000, является опциональным для ВОЛП СКС, согласно ГОСТ Р 53245-2008. По этой причине подавляющее большинство бригад предприятий, деятельность которых ориентирована в основном на инсталляцию подсистем СКС, не укомплектованы OTDR, которые, в общем случае, являются достаточно дорогостоящими средствами измерения. В данном случае, контроль качества монтажа оконечных устройств коммутации, как минимум, осуществляется с помощью оптических тестеров для проведения обязательного комплекса измерений вносимых потерь на кабельном участке, выполняемых непосредственно только по окончании всех работ по инсталляции линии. Для оперативного контроля качества разъемных соединений в патч-панелях и телекоммуникационных розетках непосредственно в процессе монтажа дополнительно используются источники видимого излучения и комплекты видеодиагностики. Первые позволяют визуально определить возможность прохождения излучения по оптическим волокнам (ОВ), вторые – оценить качество монтажа в автоматическом режиме по принципу «PASS-FAIL». Все это приводит к достаточно высоким значениям процента

«ложного» перемонтажа, когда инсталлятор при формальном не прохождении такого теста вынужден повторно монтировать коннектор или розеточный модуль и, соответственно, расходовать новый комплект коннектора, несмотря на приемлемое значение вносимых потерь. Более того, нередко бывает ситуация, когда, наоборот, коннектор проходит тест видеодиагностики и при этом результаты последующих измерений вносимых потерь на соответствующих ОВ ВОЛП, выполненных оптическим тестером, являются неудовлетворительными: устранение недостатков в этом случае требует вскрытия патч-панели или телекоммуникационной розетки, повторного монтажа коннекторов и нового цикла измерений вносимых потерь на соответствующих портах. Следует отметить, что и OTDR не решает данную задачу. Учитывая, упомянутую малую протяженность ВОЛП СКС, OTDR обеспечивает корректные измерения исключительно оптической длины волокон кабеля. В то время как тестирование портов оконечных устройств ВОЛП СКС фактически сводится к визуальному контролю ширины мертвой зоны рефлектограммы (заключение делает сам оператор), либо автоматизированной оценке качества подключения «переднего разъема» относительно установленного оператором значения коэффициента отражения также по принципу «PASS-FAIL» без определения искомых действительных значений базовых параметров передачи разъемного соединения – вносимых потерь и коэффициента отражения. Решение описанной выше проблемы подразумевает разработку аппаратно-программного комплекса прогноза параметров передачи разъемного соединения по результатам видеодиагностики торцевой поверхности феррула волоконно-оптического коннектора.

В качестве основы для аппаратно-программного комплекса была разработана методика измерения влияния площади загрязнения торцевой поверхности феррул волоконно-оптических коннекторов на параметры передачи. Включающая в себя экспериментальную измерительную схему (рис. 1) и оценку полученных результатов. Данная схема подразумевает тестирование промышленных образцов строительных длин, как одномодовых так и многомодовых волокон, оконцованых пигтейлами необходимого типа с помощью сварочного аппарата, в зависимости от конфигурации схемы. Оценка степени загрязнения торцевой поверхности феррул коннектора перед выполнением разъемного соединения проводиться с помощью комплекта видеодиагностики, с ориентацией на проведение теста чистоты феррула на уровне «PASS/FAIL» в соответствие с ратифицированным стандартом IEC 61300-3-35, который предполагает зонирование центра ферула коннектора на 3 области: «A» – сердцевина; «B» – оболочка ОВ; «C» – контактная зона феррула. После чего выполняется разъемное соединение пар ОВ, и далее с помощью оптического рефлектометра обратного рассеянии

во временной области OTDR осуществляется измерение параметров передачи – вносимых потерь и коэффициента отражения. Измерения проводиться с двух сторон [1, 2, 3, 4, 5].

В следствии чего была накоплена минимальная база снимков торцов феррул с нанесенными дефектами, а также присущие каждому снимку вносимые потери и коэффициент отражения. Для максимальной точной оценки полученных результатов и дальнейшего соединения/сравнения с математической моделью, разработан алгоритм нейросети обучающейся с помощью снимков. В качестве знаний используются снимки торцов феррул волоконно-оптических коннекторов полученные с помощью экспериментальной измерительной схемы (рис.1).

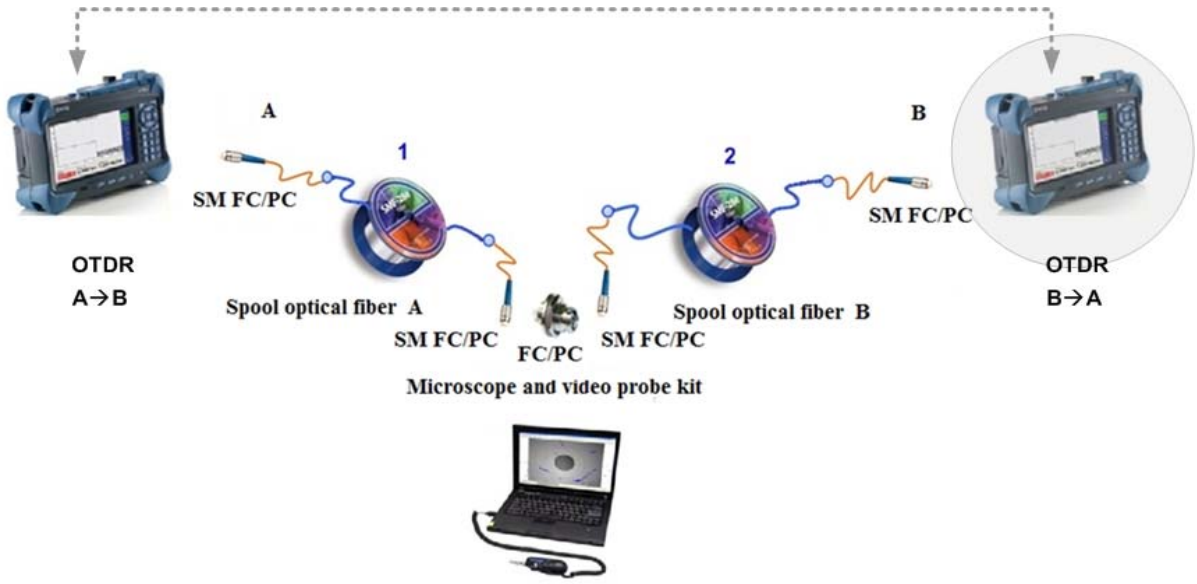


Рис. 1. Экспериментальная измерительная схема влияния площади загрязнения торцевой поверхности феррул волоконно-оптических коннекторов на параметры передачи (вносимых потерь и коэффициента отражения) пары SM ОВ

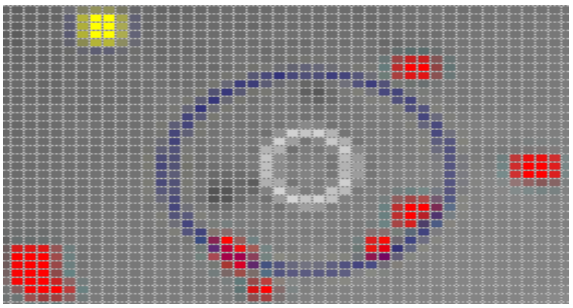


Рис. 2. Сегментирование снимка

Данные снимки заносятся в память они являются «эталоном» за счет них система нейросети будет обучаться. Главной целью нейросети является определение вносимых потерь и коэффициента отражения по полученному снимку исходя из загрязнения (повреждения) коннектора. Для того, чтобы получить заветные параметры нового снимка, необходимо определить местонахождение и площадь загрязнения. Решение этой проблемы требует, провести сегментирование снимка, что подразумевает под собой наложение координатной сетки (рис. 2).

Размер координатной сетки выбираем по пикселям. Данный размер позволяет работать с целыми клетками. Это очень важно, так как необходимо точно знать в какой из 3-х зон снимка находится загрязнение. Определение загрязненной клетки осуществляется по принципу «разных цветов». Благодаря тому, что размер координатной сетки достаточно мал и возможно работать с целыми клетками, весь снимок (вместе с загрязнением) представляем в виде большой таблицы. Каждой клетке (сегменту) присваиваем значение 0 или 1. Значение «0» проставляется, если клетка с соответствующими координатами является чистой, значение «1» присваивается, если клетка загрязнена. Таким образом, проверяется все изображение. В итоге получаем таблицу, заполненную единицами и нулями. Полученная таблица анализируется с помощью выражения для определения границ (1). Если набор из единиц окружен нулями, в том числе по диагонали, то это будет считаться обособленным загрязнением.

$$\begin{gathered} r_{i-1,j+1} - 0;\ r_{i,j+1} - 0;\ r_{i+1,j+1} - 0; \\ r_{i-1,j} - 0;\ r_{i,j} - 1;\ r_{i+1,j} - 0; \\ r_{i-1,j-1} - 0;\ r_{i,j-1} - 0;\ r_{i+1,j-1} - 0. \end{gathered} \quad (1)$$

Зная границы всех отдельных загрязнений легко находиться площадь каждого загрязнения по формуле:

$$\sum_{k=1}^{n} 1_k, \quad (2)$$

где n – количество обособленных единиц («1»); k – порядковый номер загрязнения.

Описанную выше цепочку действий также проходят и «эталонные» снимки при попадании в базу. Таким образом происходит сравнение снимков, полученных в полевых условиях с «эталонными» и выдаются вносимые потери и коэффициент отражения для необходимого снимка.

Список используемых источников

1. Пашин С. С., Жуков А. Е., Бурдин А. В. Результаты экспериментальных исследований зависимости вносимых потерь разъемных волоконно-оптических соединений от площади загрязнения торцевой поверхности феррул коннектора // XXIV росс. науч. конф. профессорско-преподавательского состава, научных сотрудников и аспирантов, Самара, 30 янва. – 3 февр. 2017 г. ИД ПГУТИ, 2017. С. 160.

2. Пашин С. С., Гиниатулина А. М., Хоркуш В. В., Жуков А. Е., Бурдин А. В. Исследование влияния площади загрязнения торцевой поверхности феррул коннектора на параметры передачи разъемного соединения оптических // Оптические технологии в телекоммуникациях: XIV международная научная конференция, Самара, 22–24 нояб. 2016 г. ИД ПГУТИ, 2016. С. 122–123.

3. Пашин С. С., Гиниатулина А. М., Хоркуш В. В. Исследование влияния площади загрязнения торцевой поверхности феррул коннектора на коэффициент отражения одно-

типных разъемных соединений оптических волокон // Прикладная электродинамика, фотоника и живые системы: международная научно-техническая конференция молодых ученых, аспирантов и студентов, Казань, 12–14 апр. 2017 г. ИД КНИТУ-КАИ, 2017. С.425–429.

4. Пашин С. С., Гиниатулина А. М., Жуков А. Е., Бурдин А. В. Исследование влияния характера и степени загрязнения торцевой поверхности феррул коннекторов на параметры передачи разъемных соединений оптических волокон // Оптические технологии в телекоммуникациях: XV международная научно-техническая конференция молодых ученых, аспирантов и студентов, Казань, 20–24 нояб. 2017 г. ИД КНИТУ-КАИ, 2017. С. 223–224.

5. Листвин А. В., Листвин В. Н. Рефлектометрия оптических волокон М. : ЛЕСА-Арт, 2005, 208 с., ил.

УДК 621.373.826

РАЗРАБОТКА ВОЛОКОННО-ОПТИЧЕСКИХ УСТРОЙСТВ УПРАВЛЕНИЯ МОДОВЫМ СОСТАВОМ ОПТИЧЕСКОГО ИЗЛУЧЕНИЯ В МАЛОМОДОВОМ РЕЖИМЕ НА БАЗЕ СВЕТОВОДОВ С НАНЕСЕННЫМИ ПРЕЦИЗИОННЫМИ МАКРОСТРУКТУРНЫМИ ДЕФЕКТАМИ

А. В. Бурдин, А. С. Евтушенко, Е. С. Соколов

Поволжский государственный университет телекоммуникаций и информатики

В работе приведены результаты экспериментальных исследований потенциальных возможностей реализации устройств управления модовым составом оптического излучения на основе волоконно-оптических элементов, представляющих собой кварцевые волоконные световоды с нанесенными каскадами прецизионных макроструктурных элементов, в том числе типа «бочка» и «перетяжка», в разных конфигурациях и последовательности.

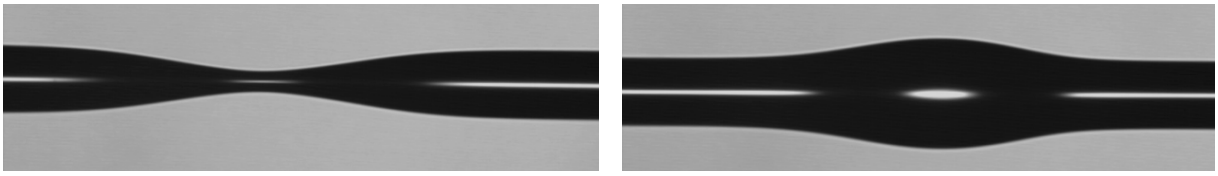
оптические волокна, прецизионный макроструктурный дефект, «бочка», «перетяжка», вносимые потери, каскад макроструктурных дефектов.

На сегодняшний день опубликовано достаточно большое количество работ, посвященных вопросам практической реализации формирования прецизионных макродефектов в структуре кварцевых волоконных световодов и практическому приложению таких волоконно-оптических элементов в различных областях волоконной оптики и фотоники. Среди подобных дефектов целесообразно выделить, так называемые, «перетяжки» («*tapers*»,

в отдельных источниках известные как «конические ответвители» – рис. 1*а*) и «бочки» («*up-tapers*», в отдельных источниках известные также как «*bubbles*» – «пузыри» – рис. 1*б*).

Такие элементы активно используются для решения задачи сращивания оптических волокон (ОВ) с разбросом технологических параметров, в частности, например, диаметров сердцевины или диаметра пятна моды [1], а также соединения ОВ неодинаковой структуры в целом [2]. Кроме того, они применяются в различных устройствах согласования источников оптического излучения с ОВ [1, 3]. Отдельный интерес представляет приложение описанных волоконно-оптических элементов в локальных сенсорах внешних воздействий измерительных систем на базе волоконно-оптических датчиков [4], интерферометрии [5] и устройствах управления модовым составом оптического излучения [1, 3, 6]. Нередко эти дефекты используются в сочетании с волоконными решетками Брэгга (ВРБ), которые могут быть записаны как в непосредственной близости от ВРБ – буквально на расстоянии в несколько диаметров световода, так и поверх предварительно сформированного дефекта [7, 8].

В общем случае, формирование прецизионных макроструктурных дефектов, в том числе упомянутых выше «перетяжек» и «бочек», с заданными геометрическими параметрами в ОВ требует применения дорогостоящего специализированного лабораторного оборудования. Вместе с тем, известен ряд публикаций – например, [8, 9] и др., в которых демонстрируется возможность реализации данных макродефектов с помощью традиционных полевых аппаратов для сварки телекоммуникационных кварцевых ОВ.



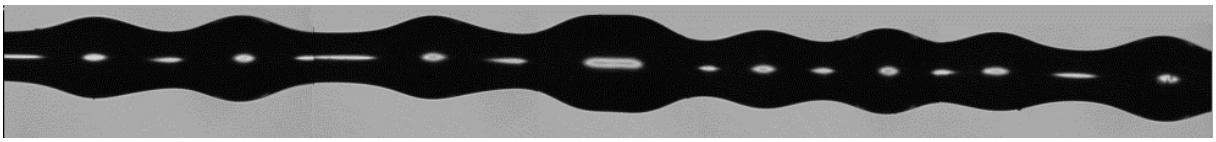
а) б)

Рис. 1. Прецизионные макродефекты, сформированные в структуре кварцевого ОВ [10, 11]: а) «перетяжка»; б) «бочка»

В свою очередь, авторами была разработана и успешно экспериментально апробирована методика формирования прецизионных макроструктурных дефектов обоих указанных типов в кварцевых телекоммуникационных ОВ с помощью комплекта полевого сварочного аппарата Ericsson FSU-975, которая подробно изложена в публикациях [10, 11]. Результаты последующих экспериментальных исследований маломодовых режимов, проведенных как для отрезков ОВ с нанесенными макродефектами по-отдельности и в сочетании с ВРБ, так и с включением в соответствующие узлы

измерительных схем на базе протяженных многомодовых ОВ, продемонстрировали потенциальные возможности управления модовым составом оптического сигнала, возбуждаемого когерентным источником излучения, при распространении в многомодовых ОВ [11, 12, 13, 14]. Это создало предпосылки для перехода к разработке новых волоконно-оптических элементов, представляющих собой отрезки ОВ с нанесенными последовательностями указанных макроструктурных дефектов заданной конфигурации. В данной работе представлены некоторые результаты экспериментальных исследований потенциальных возможностей реализации таких каскадов разной конфигурации и последовательности.

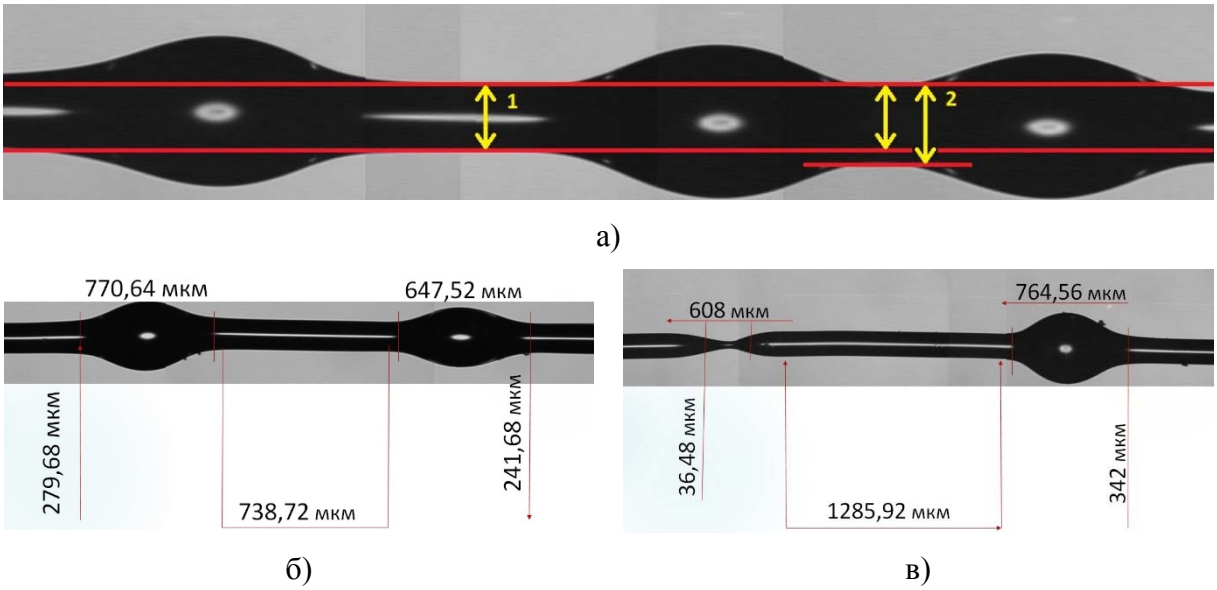
Пример пилотного каскада из 8-ми «бочек», сформированный в структуре градиентного многомодового ОВ кат. ОМ2+/ОМ3 представлен на рис. 2. Уже на первом этапе проведения экспериментальных исследований возникла задача оценивания предельно возможных расстояний между дефектами соответствующей конфигурации, в пределах которых: а) не происходит деформации предыдущего дефекта при нанесении последующего и, соответственно, б) на котором эти дефекты можно физически последовательно нанести на ОВ с применением штатного комплекта аппарата для сварки ОВ и прецизионного скалывателя. Для этой цели предварительно была проведена серия экспериментальной записи однотипных и разнотипных двухэлементных каскадов с поэтапным уменьшением интервала между ними, значение которого определялось на базе ранее разработанной методики оценивания геометрических параметров ОВ по видеоизображению в зоне обжига, выводимого на дисплей сварочного аппарата, подробно изложенной в публикациях [10, 11]. Примеры таких каскадов с нанесением макродефектов без деформации и, напротив, с деформацией структуры представлены на рис. 3*а*...*в*.



а)

б)

Рис. 2. Пилотный каскад из 8-ми «бочек», сформированный в структуре многомодовых ОВ: а) скриншот дисплея Ericsson FSU-975; б) фотография под микроскопом



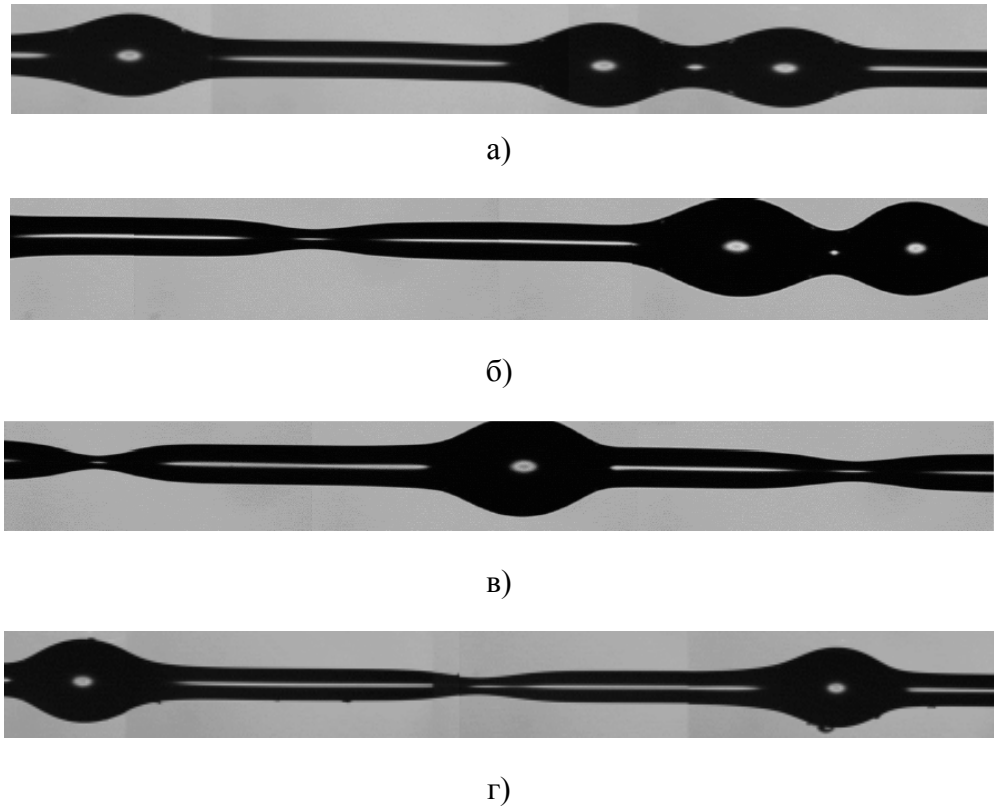
а)

б) в)

Рис. 3. К вопросу оценивания предельных расстояний между сформированными макродефектами: а) последовательно записанные дефекты типа «бочка» без нарушения геометрии соседнего образца (№ 1) и с нарушением (№ 2); б) последовательно нанесенные «бочки»; в) последовательно нанесенные «перетяжка» и «бочка»

Анализ полученных результатов показал, что для «бочек» деформация структуры дефекта при записи каскада происходит на интервалах менее 1200 мкм, в то время как для «перетяжек» минимальное допустимое расстояние составляет всего 200 мкм. Это позволило далее перейти к формированию каскадов более сложной конфигурации с увеличенным числом дефектов. Некоторые примеры таких каскадов представлены на рис. 4*а*...*в*. На данном этапе возникла задача выявления конфигурации каскада, обеспечивающего приемлемые, с точки зрения потенциальных возможностей последующего использования в измерительных схемах разного назначения, а также устройствах управления модовым составом сигнала, значения вносимых потерь в маломодовом режиме функционирования. Для этой цели сформированные образцы каскадов заданной конфигурации с помощью сварочного аппарата подключались между двумя катушками строительных длин многомодовых ОВ примерно по 400 м каждая, оконцованных пигтейлами FC/PC. Это позволило непосредственно провести измерения вносимых потерь исследуемых каскадов методом обратного рассеяния во временной области с помощью оптического рефлектометра с одномодовым оптическим модулем на длинах волн 1310 нм. Так, согласно полученным результатам, максимальные потери соответствуют конфигурации «перетяжка–бочка–бочка». Для данного трехэлементного каскада каскада значение указанного параметра достигало 7,82 дБ на указанной оптической несущей. В свою очередь, минимальные потери соответствуют конфигурации «пере-

тяжка–бочка–перетяжка» и составляют 1,06 дБ. Полученные результаты демонстрируют потенциальные возможности использования реализованных трехэлементных каскадов сложной конфигурации в устройствах управления модовым составом оптических сигналов, распространяющихся в маломодовом режиме передачи, а также в измерительных схемах разного назначения.



а) б) в) г)

Рис. 4. Примеры каскадов трехэлементных разнотипных макроструктурынх дефектов: а) три «бочки»; б) «перетяжка» – «бочка» – «бочка»; в) «перетяжка» – «бочка» – «перетяжка»; (г) «бочка» – «перетяжка» – «бочка»

Работа подготовлена при финансовой поддержке грантов РФФИ в рамках научных проектов № 16-37-6001515 мол_а_дк, № 16-37-50087 мол_нр, № 16-37-50089 мол_нр.

Список используемых источников

1. Patent WO 01/35136, IPC Classification G02B6/26. Mode adaptation for multimode optical fiber systems / D. E. Harsbarger, D. A. Nolan, C. L. Thomas, C. M. Truesdale. Corning Inc., USA. No PCT/US00/27919. publication date 17.05.2001.

2. Joannopoulos J. D., Mekis A. Tapered couplers for efficient interfacing between dielectric and photonic crystal waveguides // IEEE Journal of Lightwave Technology. 2001. vol. 19(6). P. 861–865.

3. Presby H. M., Amitay N., Scotti R., Benner A. F. Laser-to-fiber coupling via optical fiber up-tapers // IEEE Journal of Lightwave Technology. 1989. vol. 7 (2). P. 274–278.

4. Bobb L. C., Krumboltz H. D., Shankar P. M. Pressure sensor that uses bent biconically tapered single-mode fibers // Optics Letters. 1991. vol. 16 (2). P. 112–114.

5. Zhang Sh., Zhang W., Gao Sh., Geng P., Xue X. Fiber-optic bending vector sensor based on Mach–Zehnder interferometer exploiting lateral-offset and up-taper // Optics Letters. 2012. vol. 37 (21). P. 4480–4482.

6. Jung Y., Brambilla G., Richardson D. J. Efficient higher-order mode filtering in multimode optical fiber based on an optical microwire // Asia Optical Fiber Communication and Optoelectronic Exposition and Conference, Shanghai, China: OSA Technical Digest. 2008. P. SuB4-1–SuB4-3.

7. Frazao O., Falate R., Fabris L., Santos J. L., Ferreira L. A., Araújo F. M. Optical inclinometer based on a single long-period fiber grating combined with a fused taper // Optics Letters. 2006. vol. 31 (20). P. 2960–2962.

8. Tao Qi, Shilin Xiao, Jie Shi, Lilin Yi, Zhao Zhou, Meihua Bi, Weisheng Hu. Cladding-mode backward-recoupling-based displacement sensor incorporating fiber up-taper and Bragg grating // IEEE Photonics Journal. 2013. vol. 5 (4). P. 7100608-1–7100608-8.

9. Karra S., Soumya M. Preparation of tapered optical fibers to utilize the evanescent field for sensing applications // International Journal of Engineering Trends and Technology. 2013. vol. 4 (3). P. 442–446.

10. Андреев В. А., Бурдин А. В., Бурдин В. А., Василец А. А., Гаврюшин С. А., Евтушенко А. С., Казаков В. С., Морозов О. Г., Севрук Н. Л., Соколов Е. Д. Разработка методики формирования прецизионных макродефектов в структуре кварцевых волоконных световодов // Инфокоммуникационные технологии. 2017. № 1. С. 18–29.

11. Evtushenko A. S., Faskhutdinov L. M., Kafarova A. M., Kazakov V. S., Kuznetzov A. A., Minaeva A. Yu., Sevruk N. L., Nureev I. I., Vasilets A. A., Andreev V. A., Morozov O. G., Burdin V. A., Bourdine A. V. Technique for writing of fiber Bragg gratings over or near preliminary formed macro-structure defects in silica optical fibers // Proceedings of SPIE. 2017. vol. 10342. P. 103420X-1–103420X-11.

12. Evtushenko A. S., Faskhutdinov L. M., Kafarova A. M., Kazakov V. S., Kuznetzov A. A., Minaeva A. Yu., Sevruk N. L., Nureev I. I., Vasilets A. A., Andreev V. A., Morozov O. G., Burdin V. A., Bourdine A. V. Quasi-interferometric scheme improved by fiber Bragg grating written on macrostructure defect in silica multimode optical fiber operating in a few-mode regime // Proceedings of SPIE. 2017. vol. 10342. P. 103420W-1–103420W-9.

13. Бурдин А. В., Морозов О. Г., Василец А. А., Кафарова А. М., Минаева А. Ю., Севрук Н. Л. Экспериментальная апробация квази-интерферометрической схемы регистрации внешних механических воздействий на основе анализа отклика маломодового оптического сигнала // Труды учебных заведений связи. 2017. Т. 3., № 2. С. 37–50.

14. Андреев В. А., Бурдин А. В., Бурдин В. А., Евтушенко А. С., Казаков В. С., Минаева А. Ю. Экспериментальные исследования динамики отклика маломодового оптического сигнала на выходе квази-интерферометрической схемы регистрации внешних механических воздействий // Фотон-Экспресс. 2017. Т. 6, № 6. С. 225–226.

УДК 621.315

ИНТЕРФЕРЕНЦИОННАЯ МОДЕЛЬ НЕОДНОРОДНОЙ ДВУХПРОВОДНОЙ ЛИНИИ СВЯЗИ

М. С. Былина

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

В работе предложена модель процессов распространения электромагнитной энергии по неоднородной двухпроводной линии связи в частотной области, основанная на представлении попутного и обратного потоков как интерференции отдельных сигналов, отраженных от неоднородностей. Показано, что использование данного подхода позволяет существенно упростить получение временных характеристик неоднородных линий.

двухпроводная линия связи, неоднородная двухпроводная линия связи, сосредоточенная неоднородность, передаточная функция, импульсная характеристика, четырехполюсник, матрица А-параметров.

Моделью процессов распространения электромагнитной энергии по двухпроводной линии связи (ДЛС) можно считать:

в частотной области – две передаточных функции $H_+(\omega)$ и $H_-(\omega)$, позволяющие определить комплексные амплитуды напряжений $\dot{U}_l$ на выходе и $\dot{U}_0$ на входе ДЛС, в ответ на входное воздействие с комплексной амплитудой $\dot{E}$ [1, 2]:

$$H_+(\omega)=\dot{U}_l/\dot{E},\ H_-(\omega)=\dot{U}_0/\dot{E}. \qquad (1)$$

во временной области – две импульсных $g_+(t)$ и $g_-(t)$ или переходных $h_+(t)$ и $h_-(t)$ характеристики, позволяющие определить напряжения на ее входе $u_0(t)$ и выходе $u_l(t)$ в ответ на входное воздействие $e(t)$ ($e'(t)$ – производная от $e(t)$) [1, 2]:

$$\begin{aligned} u_0(t)&=\int_{-\infty}^{t} e(t_1)g_-(t-t_1)dt_1=\int_{-\infty}^{t} e'(t_1)h_-(t-t_1)dt_1 \\ u_l(t)&=\int_{-\infty}^{t} e(t_1)g_+(t-t_1)dt_1=\int_{-\infty}^{t} e'(t_1)h_+(t-t_1)dt_1 \end{aligned}, \qquad (2)$$

Под неоднородной ДЛС будем понимать линию, эквивалентная схема (рис.) которой включает N последовательно соединенных однородных участков с разными, в общем случае, параметрами, между которыми

могут включаться сосредоточенные неоднородности, эквивалентные схемы которых представляют собой четырехполюсники с сосредоточенными параметрами, характеризующиеся известными А-матрицами [3].

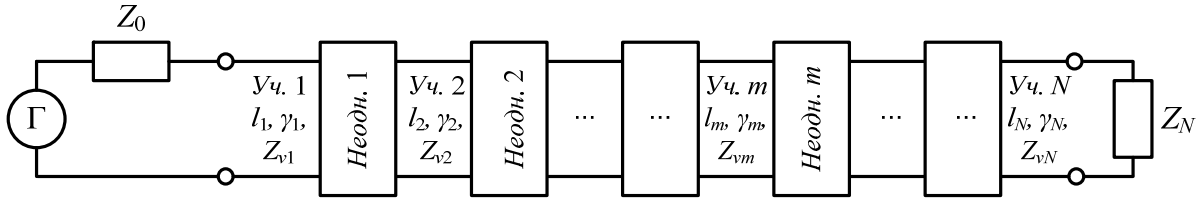


Рисунок. Эквивалентная схема неоднородной ДЛС

Однородные участки также можно представить четырехполюсниками, имеющими распределенные параметры, и характеризовать А-матрицами. Для m-го участка длиной l_m с волновым сопротивлением Z_{vm} и постоянной распространения γ_m А-матрица имеет вид:

$$\mathbf{A}_{line}^{(m)} = \begin{pmatrix} ch(\gamma_m l_m) & Z_{vm} sh(\gamma_m l_m) \\ sh(\gamma_m l_m)/Z_{vm} & ch(\gamma_m l_m) \end{pmatrix}, \tag{3}$$

где $sh(x)$ и $ch(x)$ – гиперболические синус и косинус.

Обозначая через $\mathbf{A}^{(m)}$ матрицу А-параметров, характеризующую m-тую сосредоточенную неоднородность, запишем выражение для А-матрицы неоднородной ДЛС:

$$\mathbf{A} = \begin{pmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{pmatrix} = \left(\prod_{m=1}^{N-1} \mathbf{A}_{line}^{(m)} \mathbf{A}^{(m)} \right) \mathbf{A}_{line}^{(N)}. \tag{4}$$

Учитывая, что для входного сопротивления четырехполюсника, нагруженного на сопротивление Z_N, справедливо [3]:

$$Z_{in} = (A_{11} \cdot Z_N + A_{12})/(A_{21} \cdot Z_N + A_{22}), \tag{5}$$

для $H_+(\omega)$ и $H_-(\omega)$ можно получить выражения:

$$H_- = (A_{12} + A_{11} Z_N)/(A_{11} Z_N + A_{12} + A_{21} Z_0 Z_N + A_{22} Z_0), \tag{6}$$

$$H_+ = Z_N/(A_{11} Z_N + A_{12} + A_{21} Z_0 Z_N + A_{22} Z_0) \tag{7}$$

Отметим, что теория распространения электромагнитной энергии по неоднородной ДЛС во временной области практически не представлена в известной литературе. Одной из причин являются значительные трудности, получения $g_{\pm}(t)$ или $h_{\pm}(t)$ из (6), (7) с использованием обратных преобразований Фурье или Лапласа.

Аналитическое выражение для импульсной или переходной характеристики даже для однородной согласованной ДЛС можно получить только при

упрощающих предположениях [2]. Поэтому строгое решение задачи возможно только численными методами. Однако трудоемкость таких вычислений с увеличением длины ДЛС и сложности ее структуры возрастает практически экспоненциально.

Рассмотрим методику, позволяющую упростить получение временных характеристик неоднородной ДЛС.

Известно, что в неоднородной ДЛС возникают попутный и обратный потоки, представляющие собой совокупности сигналов, отраженных от неоднородностей и распространяющихся по ДЛС в прямом (от источника к нагрузке) и обратном (от нагрузки к источнику) направлении соответственно. Каждый отраженный сигнал, входящий в состав попутного и обратного потоков можно характеризовать кратностью отражения (числом отражений, которые он испытал до регистрации). Очевидно, что с увеличением кратности отражения сигналы уменьшаются по амплитуде (их вклад в попутный и обратный поток уменьшается) и сильнее задерживаются во времени. Поэтому при анализе ДЛС можно ограничиться только теми отражениями, которые попадают в рассматриваемый временной интервал и не являются пренебрежимо малыми.

Отметим, что m-тую неоднородность в схеме (1) можно характеризовать коэффициентами отражения $R_{m\pm}$ и пропускания $K_{m\pm}$, определяемыми следующим образом:

$$R_{m\pm} = \dot{U}_{m ref\pm} \big/ \dot{U}_{m inc\pm}, \quad K_{m\pm} = \dot{U}_{m tra\pm} \big/ \dot{U}_{m inc\pm}, \tag{8}$$

где $\dot{U}_{m inc}$, $\dot{U}_{m ref}$, $\dot{U}_{m tra}$ – комплексные амплитуды напряжений в падающей, отраженной и прошедшей волнах. Знак «+» относится к волне, распространяющейся в прямом направлении, а знак «–» – в обратном. Коэффициенты $R_{m\pm}$ и $K_{m\pm}$ можно связать с коэффициентами известной из теории четырехполюсников матрицы рассеяния или S-матрицы:

$$R_{m+} = S_{11}^{(m)}, \quad K_{m+}\sqrt{\frac{Z_{vm}}{Z_{v(m+1)}}} = S_{21}^{(m)}, \quad R_{m-} = S_{22}^{(m)}, \quad K_{m-}\sqrt{\frac{Z_{v(m+1)}}{Z_{vm}}} = S_{12}^{(m)}. \tag{9}$$

Используя известные выражения для связи коэффициентов S-матрицы и A-матрицы, можно получить соотношения:

$$A_{11}^{(m)} = \left(R_{m+} - R_{m-} - R_{m+}R_{m-} + K_{m+}K_{m-} + 1\right)/\left(2K_{m+}\right),$$

$$A_{12}^{(m)} = Z_{v(m+1)}\left(R_{m+} + R_{m-} + R_{m+}R_{m-} - K_{m+}K_{m-} + 1\right)/\left(2K_{m+}\right),$$

$$A_{21}^{(m)} = \left(-R_{m+} - R_{m-} + R_{m+}R_{m-} - K_{m+}K_{m-} + 1\right)/\left(2Z_{vm}K_{m+}\right),$$

$$A_{22}^{(m)} = Z_{v(m+1)}\left(-R_{m+} + R_{m-} - R_{m+}R_{m-} + K_{m+}K_{m-} + 1\right)/\left(2Z_{vm}K_{m+}\right). \quad (10)$$

Используя соотношения (10), можно выразить (4)–(7) через $R_{m\pm}$ и $K_{m\pm}$.

Рассмотрим ДЛС, содержащей два однородных участка и единственную сосредоточенную неоднородность. Из (4)–(10) получаем:

$$H_+ = K_0\left(1 + R_l\right)K_+H_1H_2P, \quad (11)$$

$$H_- = K_0\left(1 + R_+H_1^2 - R_-R_lH_2^2 + R_l\left(K_+K_- - R_+R_-\right)H_1^2H_2^2\right)P, \quad (12)$$

$$P = \left[1 - R_lR_0\left(K_+K_- - R_+R_-\right)H_1^2H_2^2 - R_+R_0H_1^2 - R_-R_lH_2^2\right]^{-1} \quad (13)$$

$$H_{12} = exp\left(-\gamma_{12}l_{12}\right), \quad K_0 = \frac{Z_{v1}}{Z_0 + Z_{v1}}, \quad R_0 = \frac{Z_0 - Z_{v1}}{Z_0 + Z_{v1}}, \quad R_l = \frac{Z_l - Z_{v2}}{Z_l + Z_{v2}}, \quad (14)$$

где $R_\pm$ и $K_\pm$ – коэффициенты отражения и пропускания неоднородности, H_1 и H_2 – передаточные функции однородных участков ДЛС, K_0 – коэффициент передачи от генератора к ДЛС, R_0 и R_l – коэффициенты отражения от входа и выхода ДЛС, Z_0 – внутреннее сопротивление генератора, Z_l – сопротивление нагрузки.

В (11) и (12) входит множитель P, который можно представить в виде суммы членов бесконечно убывающей геометрической прогрессии:

$$P = \sum_{n=0}^{\infty}\left[R_lR_0\left(K_+K_- - R_+R_-\right)H_1^2H_2^2 + R_+R_0H_1^2 + R_-R_lH_2^2\right]^n. \quad (15)$$

Подставим (15) в (11) и (12) и запишем в явном виде несколько первых членов сумм:

$$H_+ = \underbrace{K_0K_+H_1H_2}_{\text{ïðÿìîé ïîòîê}} + \underbrace{K_0K_+R_lH_1H_2}_{\text{îäíîêð. ïîò. îò ê-îíöà ÄËÑ}} + \underbrace{K_0K_+R_lR_-H_1H_2^3}_{\text{äâóêð. ïîòàæ.: ê-îíåö ÄËÑ -> íåîäí.}} +$$

$$+ \underbrace{K_0K_+^2K_-R_lR_0H_1^3H_2^3}_{\text{äâóêð. ïîòàæ.: ê-îíåö ÄËÑ -> íà÷-àëî ÄËÑ}} + \underbrace{K_0K_+R_+R_0H_1^3H_2}_{\text{äâóêð. ïîòàæ.: íåîäí. -> íà÷-àëî ÄËÑ}} + \underbrace{K_0K_+R_l^2R_-H_1H_2^3}_{\text{òðåõêð.ïîòàæ.: ê-îíåö ÄËÑ -> íåîäí. -> ê-îíåö ÄËÑ}} +$$

$$+ \underbrace{K_0K_+^2K_-R_l^2R_0H_1^3H_2^3}_{\text{òðåõêð.ïîòàæ.: ê-îíåö ÄËÑ -> íà÷-àëî ÄËÑ -> ê-îíåö ÄËÑ}} + \underbrace{K_0K_+R_+R_0R_lH_1^3H_2}_{\text{òðåõêð.ïîòàæ.: íåîäí. -> íà÷-àëî ÄËÑ -> ê-îíåö ÄËÑ}} + \ldots \quad (16)$$

$$H_- = \underbrace{K_0}_{\text{ïð. ïîòîê}} + \underbrace{K_0R_+H_1^2}_{\text{îäíîêð. ïîò. îò íåîäí.}} + \underbrace{K_0K_+K_-R_lH_1^2H_2^2}_{\text{îäíîêð. ïîò. îò ê-îíöà ÄËÑ}} + \underbrace{K_0R_+R_0H_1^2}_{\text{äâóêð. ïîò.: íåîäí. ->íà÷-àëî ÄËÑ}} +$$

$$+\underbrace{K_0K_+K_-R_0R_lH_1^2H_2^2}_{\text{äâóêð. îòð.: êîíåö ÄËÑ -> íà÷àëî ÄËÑ}}+\underbrace{K_0R_+^2R_0H_1^4}_{\text{òðåõêð. îòð.: íåîáõ. -> íà÷àëî ÄËÑ -> íåîáõ.}}+\underbrace{K_0K_+^2K_-^2R_0R_l^2H_1^4H_2^4}_{\text{òðåõêð. îòð.: êîíåö ÄËÑ -> íà÷àëî ÄËÑ -> êîíåö ÄËÑ}}+$$

$$+\underbrace{K_0K_+K_-R_-R_l^2H_1^2H_2^4}_{\text{òðåõêð. îòð.: êîíåö ÄËÑ -> íåîáõ. -> êîíåö ÄËÑ}}+\underbrace{K_0K_+K_-R_+R_0R_lH_1^4H_2^2}_{\text{òðåõêð. îòð.: êîíåö ÄËÑ -> íà÷àëî ÄËÑ -> íåîáõ.}}+\ldots \quad (17)$$

Из (16) и (17) видно, что результирующие волны напряжения на входе и выходе ДЛС представляют собой интерференцию волны прямого потока и бесконечного числа переотраженных волн, поэтому данную модель ДЛС будем называть интерференционной.

Очевидно, что каждый член суммы в (16) и (17), начиная со 2-го, представляет собой передаточную функцию, позволяющую рассчитать один из отраженных сигналов, входящих в состав попутного или обратного потоков. Интерференционной моделью, аналогичной (16) и (17), может быть представлена любая неоднородной ДЛС (рис.) с произвольным числом неоднородностей.

Использование интерференционной модели неоднородной ДЛС для расчета ее временных характеристик позволяет существенно упростить их получение, так как появляется возможность в выражениях, аналогичных (16) и (17), ограничиться конечным числом первых членов сумм.

Список использованных источников

1. Былина М. С., Глаголев С. Ф. Рефлектометрия кабелей связи. СПб: СПбГУТ, 2015. 228 с.

2. Андреев В. А. Временные характеристики кабельных линий связи. М. : Радио и связь, 1986. 104 с.

3. Гупта К., Гардж Р., Чадха Р. Машинное проектирование СВЧ устройств: пер. с англ. / Под ред. В. Г. Шейкмана. М. : Радио и связь, 1987. 432 с.

УДК 621.375.8

ОПТИЧЕСКИЕ УСИЛИТЕЛИ НА ОСНОВЕ КОМБИНАЦИОННОГО (РАМАНОВСКОГО) РАССЕЯНИЯ СВЕТА

М. С. Былина, М. Н. Халилов

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

В работе рассмотрены принцип действия, классификация и параметры рамановских оптических усилителей. Представлена математическая модель процессов усиления оптических сигналов в рамановском ОУ. Приведены результаты моделирования рамановских ОУ, которые сопоставлены с представленными в литературе результатами, полученными другими исследователями.

рамановское усиление, оптический усилитель, коэффициент усиления, попутная накачка, встречная накачка.

Рамановские оптические усилители (ОУ) используются в волоконно-оптических системах передачи для усиления ослабленных оптических сигналов. Работа рамановского ОУ основана на явлении вынужденного комбинационного рассеяния в оптическом волокне (ОВ) [1, 2, 3]. Схема рамановского ОУ представлена на рис. 1. Ее основными элементами являются лазер накачки, мультиплексор спектрального уплотнения WDM, объединяющий излучение сигнала и накачки, и оптическое волокно (ОВ).

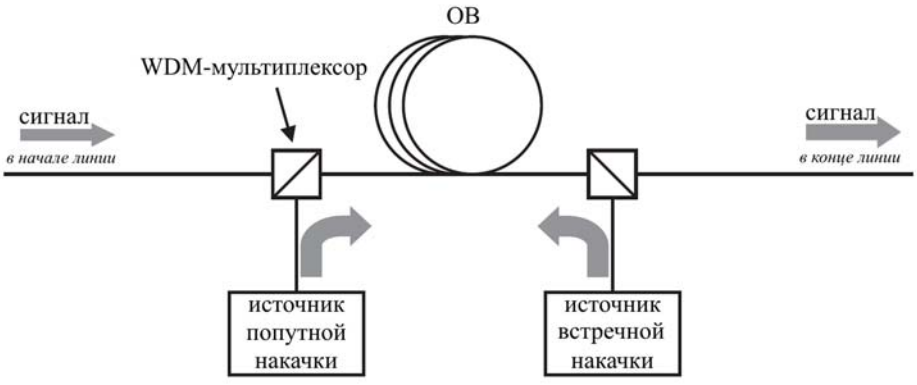


Рис. 1. Схема рамановского ОУ

Различают распределенные рамановские ОУ, в которых нелинейное взаимодействие сигнала и накачки происходит в обычном телекоммуникационном ОВ, и дискретные рамановские ОУ, в которых используется специальное ОВ. В зависимости от направления распространения излучения

накачки в ОВ и числа ее источников различают схемы с попутной, встречной и двунаправленной накачкой.

ОВ, в котором происходит взаимодействие сигнала и накачки, характеризуется длиной L, коэффициентом рамановского усиления g_r (м/Вт), коэффициентом затухания α_s (1/м) на частоте сигнала ν_s (Гц), а также коэффициентом затухания α_p на частоте накачки ν_p. Для одного источника попутной или встречной накачки процесс усиления описывается системой дифференциальных уравнений, характеризующих изменение мощностей сигнала P_S и накачки P_P (Вт) при прохождении расстояния dz (м) в ОВ [2, 3]:

$$\frac{dP_s}{dz} = \frac{g_r}{S_p} P_p P_s - \alpha_s P_s, \tag{1}$$

$$\pm \frac{dP_p}{dz} = -\frac{\nu_p}{\nu_s} \frac{g_r}{S_s} P_p \left(P_s + P_n\right) - \alpha_p P_p, \tag{2}$$

$$P_n(z) = \left(2h\nu_s F_n \cdot \Delta\nu + P_{n0}\right) \cdot \frac{P_s(z)}{P_s(0)}, \tag{3}$$

где S_s и S_p – эффективные площади поперечного сечения сердцевины ОВ для излучения сигнала и излучения накачки (м^2), P_{n0} – мощность шумов предыдущих каскадов. В выражении (2) знак «+» соответствует накачке в попутном направлении, «–» – во встречном.

Система уравнений (1)–(3) имеет аналитическое решение только, если пренебречь истощением накачки. Это решение имеет вид [2, 3]

$$P_s(L) = P_s(0)\exp\left(\pm \frac{g_r P_{p0}}{S_p} L_{eff} - \alpha_s L\right) \tag{4}$$

$$P_p(L) = P_p(0)\exp\left(\pm \alpha_p L\right) \tag{5}$$

где $P_S(0)$ и $P_P(0)$ –значения мощностей сигнала и накачки в начале ОВ;

$$L_{eff} = \frac{1 - \exp\left(\mp \alpha_p L\right)}{\alpha_p} \tag{6}$$

– эффективная длина активной среды, в которой происходит оптическое усиление.

Однако, решение (4)–(5) может в ряде случаев давать большую погрешность, поэтому оно может использоваться только для предварительной оценки параметров ОУ. Точное решение (1)–(3) может быть получено только численным методом. В данной работе для решения (1)–(3) использовалась моделирующая программа [3].

Было проведено моделирование рамановского распределенного ОУ с попутной и встречной накачкой, работающего на стандартном одномодовом ОВ. Расчеты проводились при следующих параметрах: длина волны сигнала 1,55 мкм; длина волны накачки 1,45 мкм; шум-фактор 6 дБ, коэффициент усиления среды на длине волны 1 мкм 10^{-13} м/Вт; ширина полосы пропускания оптического фильтра 0,2 нм; диаметр модового поля на длине 1550 нм 10,4 мкм^2; длина ОВ 100 км.

Некоторые результаты моделирования представлены на рис. 2–6. Из рисунков видно, что:

– для работы рамановского ОУ необходимы относительно большие мощности накачки – порядка сотен мВт.

– увеличение мощности накачки приводит к увеличению коэффициента усиления.

– эффективное усиление сигнала происходит на начальном участке ОВ, длина которого может быть приближенно оценена по выражению (6).

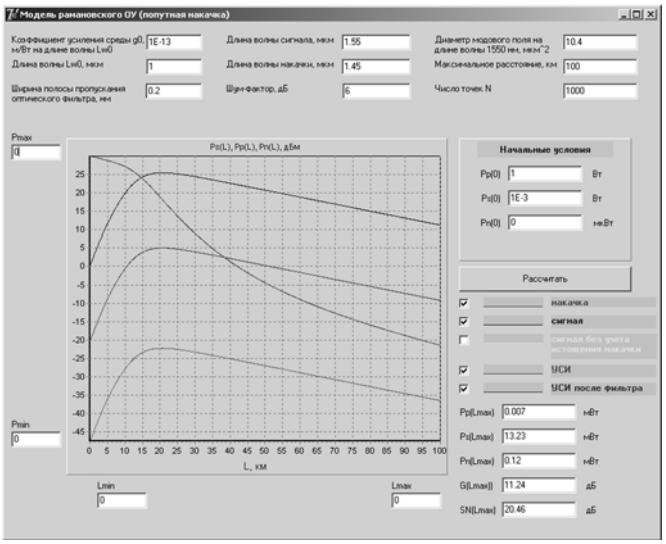


Рис. 2. Окно программы моделирования

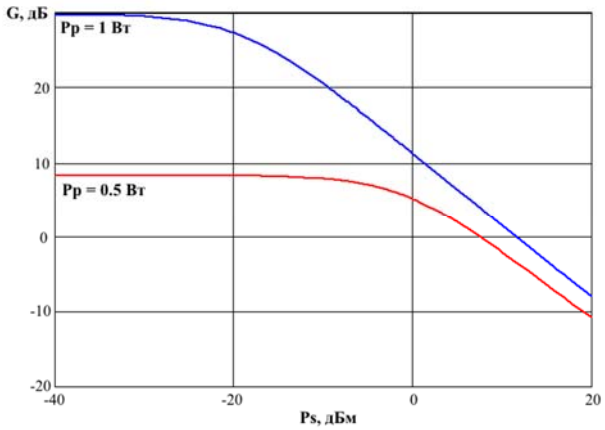


Рис. 3. Зависимости коэффициентов усиления от уровня входного сигнала при попутной накачке

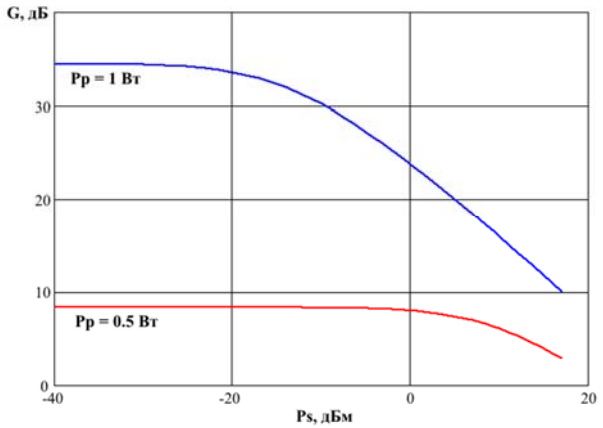


Рис. 4. Зависимости коэффициентов усиления от уровня входного сигнала при встречной накачке

– наибольший коэффициент усиления G может быть получен при работе ОУ в режиме усиления слабого сигнала. При увеличении уровня входного сигнала коэффициент усиления уменьшается – ОУ входит в режим насыщения.

– мощность насыщения увеличивается с увеличением мощности накачки.

– при использовании схемы со встречной накачкой при тех же мощностях накачки, что и при схеме с попутной накачкой, коэффициент усиления больше.

Установлено, что мощность насыщения зависит от мощности накачки (рис. 5–6). Результаты расчёта значения мощности насыщения при разных мощностях накачки для попутной и встречной накачки с помощью программы представлены в таблице.

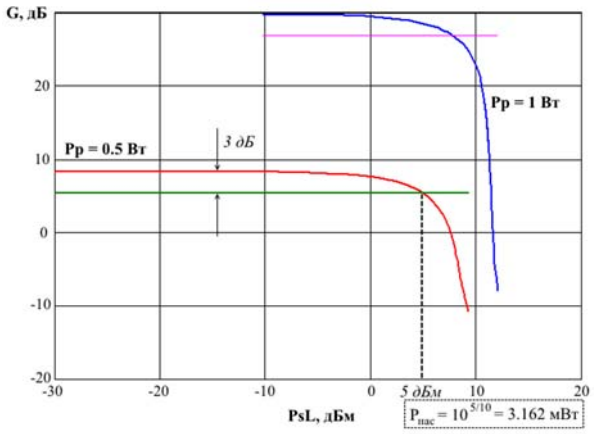


Рис. 5. Зависимости коэффициента усиления от уровня выходного сигнала при попутной накачке

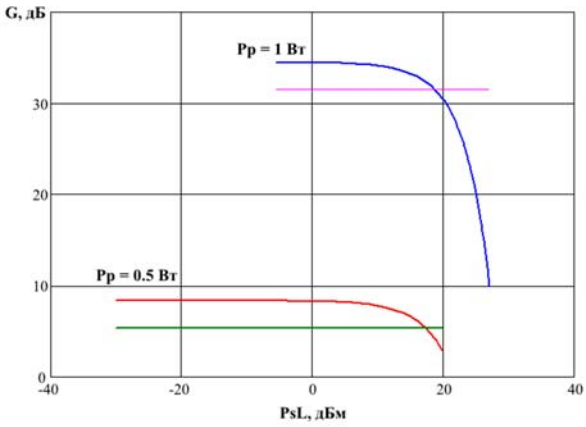


Рис. 6. Зависимости коэффициента усиления от уровня выходного сигнала при встречной накачке

ТАБЛИЦА. Мощности насыщения усилителей разных схем накачки

Мощность накачки P_P, Вт	0,5	1,0
Мощность насыщения при попутной накачке $P_{нас(п)}$, мВт	3,162	5,888
Мощность насыщения при встречной накачке $P_{нас(в)}$, Вт	0,054	0,074

Полученные результаты хорошо согласуются с параметрами рамановских ОУ, приведенными в [1, 2, 3].

Список используемых источников

1. Андреев В. А., Дашков М. В. Рамановские усилители на волоконно-оптических линиях передачи: монография. М. : ИРИАС, 2008. 219 с.

2. Headley C., Agrawal G. P. Raman Amplification in Fiber Optical Communication Systems. Academis Press, 2005.

3. Былина М. С., Глаголев С. Ф. Использование оптических усилителей в линейных трактах ВОЛС // Фотон-Экспресс. 2007. № 7 (63). С. 22–23.

УДК 004.032.32

УЛУЧШЕНИЕ МЕТРОЛОГИЧЕСКИХ ХАРАКТЕРИСТИК КВАНТОВОГО СТАНДАРТА ЧАСТОТЫ НА АТОМАХ ЦЕЗИЯ-133

А. П. Валов[1], Н. М. Гребенникова[2], В. В. Давыдов[1], А. А. Петров[2]

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

Концепция развития современных телекоммуникационных систем, систем передачи информации, спутниковой навигационной системы, метрологической службы исходит из необходимости в постоянной модернизации используемых в настоящее время квантовых стандартов частоты. В работе представлено одно из направлений модернизации КСЧ, а именно, разработка цифрового синтезатора частоты с целью улучшения метрологических характеристик КСЧ. Проведенные исследования работы КСЧ показали эффективность применения новой разработки.

квантовый стандарт частоты, система передачи данных, синхронизация, время, стабильность частоты.

В современном мире в условиях быстрого развития мировой науки, технологий и средств передачи информации невозможно обойтись без измерения времени с высокой точностью. Сложно представить без этого существование навигационных приборов или систем измерения времени, радиоэлектронной аппаратуры и телекоммуникационного оборудования, компьютерных и сотовых сетей. Многочисленное оборудование, которое используется в этих сферах деятельности, имеет различные допуски по точности, устойчивости, формату данных, а потому взаимное их использование может быть сильно затруднено из-за этой разницы.

Научно – техническому прогрессу и интегрированной мировой экономике требуется постоянная передача и обобщение результатов измерений с высокой скоростью, полученных в различных местах и часовых поясах в общую систему данных и наоборот. Для обеспечения синхронизации приемно-передающих устройств и моментов измерений необходимы высокоточные опорные генераторы. Наибольшей точностью и надежностью среди источников опорных колебаний, используемых для измерения времени обладают квантовые стандарты частоты.

Используемые в настоящее время квантовые стандарты частоты (КСЧ) находят широкое применение в науке и технике, спутниковых, навигационных, телекоммуникационных и информационных системах [1, 2, 3, 4, 5].

С ростом скорости и объемов передачи информации к работе КСЧ, в первую, очередь стали предъявлять все более жесткие требования по точности и надежности.

Учитывая высокую значимость высокоточных атомных часов и обширную область их применения, модернизация действующих и разработка новых квантовых устройств формирования частоты является одной из актуальных задач.

Для КСЧ характерно то, что модернизации может подвергаться не вся конструкция, а отдельные его функциональные узлы или блоки [3]. Так, в данной работе представлена модернизация отдельного функционального блока – синтезатора частоты (СЧ) с целью увеличения его функциональных возможностей и улучшения характеристик его выходного сигнала, что в совокупности дает возможность улучшить метрологические характеристики самого КСЧ.

Стандарты частоты на атомах цезия ^{133}Cs занимают особое место среди всех КСЧ, поскольку эталон времени, одна секунда, базируется на микроволновом переходе в атоме ^{133}Cs. Работа КСЧ на атомах ^{133}Cs основана на принципе подстройки частоты высокостабильного кварцевого генератора по частоте квантового перехода атомов цезия ^{133}Cs в атомно-лучевой трубке [1, 2, 5].

Основная функция СЧ в работе КСЧ на атомах ^{133}Cs это формирование сигнала с частотой 12,6317727 МГц, необходимого для формирования СВЧ – частоты часового перехода атомов цезия. Кроме этого, СЧ формирует низкочастотные сигналы, использующиеся в работе системы автоматической подстройки частоты (АПЧ) КСЧ.

Исходя из этого, к синтезаторам частоты предъявляются высокие требования по характеристикам выходных сигналов.

Важно, чтобы синтезатор частоты обеспечивал высокую точность выходной частоты, имел высокое подавление боковых амплитудных составляющих в спектре сигнала с частотой 12,6317727 МГц, низкую зависимость изменения частоты и амплитуды выходного сигнала от температуры, возможность перестройки частоты выходного сигнала в широкой полосе частот с малым шагом перестройки частоты, высокую скорость перестройки выходной частоты, возможность выбора различных частот модуляции выходного сигнала, имел возможность применения в различных моделях КСЧ, а также был реализован на отечественной электронной компонентной базе.

Учитывая все эти требования, необходимые для улучшения метрологических характеристик КСЧ, нами была разработана новая конструкция СЧ.

Новая конструкция цифрового синтезатора частоты была разработана на основе метода прямого цифрового синтеза (DDS – *Direct Digital Synthesis*). Более подробно принцип работы DDS рассмотрен в [6].

Учитывая требования, предъявляемые к СЧ в составе КСЧ, стандартный метод прямого цифрового синтеза был адаптирован под эти особенности.

В разработанной схеме СЧ, при частоте тактирования цифровых микросхем F_{CLK} = 15 МГц и разрядности аккумулятора фазы 40, шаг перестройки частоты ΔF_{out} составил 1,36. 10^{-5} Гц [7].

Другой характерной особенностью разработанного СЧ является очень высокая скорость перехода на другую частоту. Время перестройки разработанного СЧ складывается из времени перестройки цифровой части системы и времени запаздывания ФНЧ. Время перестройки цифровой части составляет три периода тактовой частоты. Запаздывание в ФНЧ обратно пропорционально полосе пропускания и при частоте среза $f_{ср}=\frac{F_{clk}}{4}$ составляет приблизительно четыре периода тактовой частоты. Общее время перестройки составляет семь периодов тактовой частоты. При F_{CLK} = 15 МГц время перестройки составит τ = 0,47 мкс. Более того, все перестройки по частоте происходят без разрыва фазы выходного сигнала.

Для обеспечения требований по подавлению боковых амплитудных составляющих в полосе частот до 600 кГц, во-первых, был реализован алгоритм, позволяющий использовать симметричность функции sin(x) и уменьшить шаг изменения отсчетов амплитуды функции sin(x) в 4 раза, а во-вторых, был использован 10-разрядный цифро-аналоговый преобразователь.

Реализация метода прямого цифрового синтеза, с учетом формирования сигналов с различными частотами модуляции, необходимых для работы системы АПЧ КСЧ, была осуществлена на базовом матричном кристалле (БМК). Необходимо отметить, что в разработанной конструкции синтезатора использована только отечественная электронная компонентная база. Структурная схема СЧ приведена на рис.

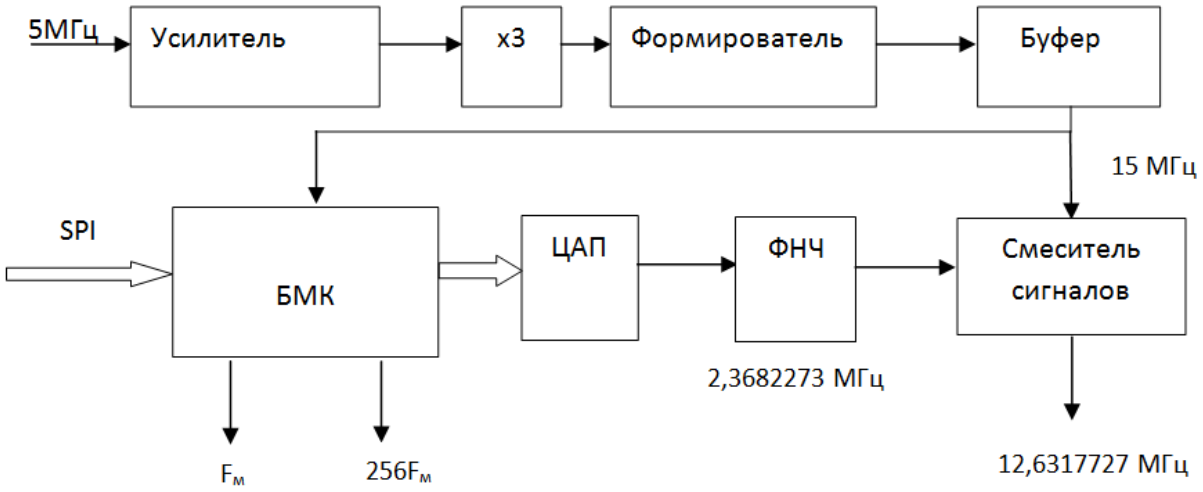


Рисунок. Структурная схема СЧ

Кроме этого новая конструкция синтезатора частоты позволяет устранить один из некоторых факторов, влияющих на долговременную стабильность частоты.

Центральный резонанс атома цезия-133, возникающий из-за эффекта Зеемана испытывает квадратичный сдвиг частоты. Для значения магнитного поля, равного $B = 6 \cdot 10^{-6}$ Тл, частотный сдвиг составляет 1,5388 Гц [8].

Нужно отметить, что частотный сдвиг испытывает не только центральный резонанс, но и все остальные 6 переходов $(3, m_f) \leftrightarrow (4, m_f)$, для которых $\Delta m_f = 0$. Эти сдвиги влияют на точность выходного сигнала стандарта частоты и непосредственно на его метрологические характеристики.

Подстройка величины магнитного поля осуществляется по соседнему переходу $|F = 3, m_f = 1> \leftrightarrow |F = 4, m_f = 1>$ методом, аналогичным подстройке частоты к основному максимуму. В ранее используемой конструкции СЧ применялся кварцевый фильтр с достаточно узкой полосой пропускания. В результате этого было невозможно сформировать частоту соседнего перехода. Но сейчас, поочередно замыкая кольца автоподстройки на центральном и соседнем переходе, системой автоподстройки мы подстраиваем и частоту кварцевого генератора к частоте атомного перехода и поддерживаем заданное значение магнитного поля внутри АЛТ постоянным.

В результате работы данной системы стабилизации исключаются эффекты, связанные с изменениями магнитного поля (например, долговременный дрейф источника тока, температурная зависимость, влияние внешнего магнитного поля и т. д.), что приводит к улучшению долговременной стабильности частоты выходного сигнала КСЧ, а также уменьшению температурного коэффициента частоты (ТКЧ) и дрейфа частоты КСЧ.

Полученные результаты исследований работы СЧ показали целесообразность применения метода прямого цифрового синтеза при разработке новой конструкции СЧ и применения СЧ в составе КСЧ.

По результатам проведенных испытаний СЧ зафиксировано уменьшение шага перестройки частоты на два порядка, расширение диапазона выходных частот до 300 кГц, улучшение спектральных характеристик выходного сигнала в полосе регистрации 6 кГц на 18 дБ.

По результатам проведенных испытаний КСЧ зафиксировано значительное (в 2,9 раза) улучшение ТКЧ КСЧ по сравнению с ТКЧ КСЧ с СЧ предыдущей конструкции. Значение вариации Аллана при времени наблюдения 1 сутки улучшено на 15 %.

Список используемых источников

1. Дудкин В. И., Пахомов Л. Н. Квантовая электроника. СПб. : Изд-во Политехнического ун-та, 2012. 387 с.

2. Риле Ф. Стандарты частоты. Принципы и применения. М. : Физматлит, 2009. 511 с.

3. Петров А. А., Давыдов В. В., Шабанов В. Е., Залетов Д. В. Цифровой синтезатор частоты для квантового стандарта частоты на атомах цезия -133 // НТВ СПбГПУ. Информатика. Телекоммуникации. Управление, НТВ-ИТУ. 2013. № 186. С. 45–52.

4. Davydov V. V., Karseev A. Yu., Nepomnyashchay H. K, Petrov A. A., Velichko E. N. Fiber – Optic Super – High – Frequency Signal Transmision System for Sea – Based Radar Station. // Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). 2014. Vol. 8638 LNCS. P. 694–702.

5. Одуан К., Гино Б. Измерение времени. Основы GPS. М. : Техносфера, 2002. 400 с.

6. Ридико Л. И. DDS: прямой синтез частоты // Компоненты и технологии. 2001. № 7.

7. Петров А. А., Давыдов В. В. Цифровой синтезатор частоты для атомных часов на парах ^{133}Cs. // Радиотехника и электроника. 2017. Т. 62. №. 3. С. 300–306.

8. Petrov A. A., Vologdin V. A., Davydov V. V., Zalyotov D. V. Dependence of microwave – excitation signal parameters on frequency stability caesium atomic clock // Journal of Physics: Conference Series. 2015. Vol 643. No 1. P. 012087.

УДК 004.056.52

ФУНКЦИОНАЛЬНО-ДИСКРЕЦИОННАЯ МОДЕЛЬ УПРАВЛЕНИЯ ДОСТУПОМ. ЗАЩИТА ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА АВТОМАТИЗИРОВАННЫХ РАБОЧИХ МЕСТ ДОЛЖНОСТНЫХ ЛИЦ

Ю. А. Валюшкина, М. О. Лепешкин, П. А. Новиков

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

В автоматизированных системах применяются различные модели управления доступом. Например, дискреционная, мандатная, ролевая, модель целостности и другие. Все эти модели основаны на взаимодействии между собой одного субъекта и одного объекта. Для эффективной работы с какой-либо системой, возникает необходимость создания моделей. В современных системах остро стоит проблематика обеспечения безопасности и устойчивого функционирования. Поэтому для её решения, рассматривается объединение двух основных понятий как информационная безопасность и функциональная безопасность, с помощью которых можно описать безопасное функционирование в реальном масштабе времени.

дискреционная модель, автоматизированные системы, информационная безопасность, функциональная безопасность.

Для обеспечения функциональной безопасности предлагается разработать функциональную модель безопасности разграничения доступа на основе моделей безопасности, которая вместо традиционной двойки <*S*, *O*> рассматривает тройку <*S*, *O*, *F*>, где *S* – Субъект; *O* – Объект; *F* – множество функций АС. Задачей третьей сущности – множества функций, является описание набора задач, которые может выполнить тот или иной человек-исполнитель, обладающий достаточными правами для получения доступа к определенной информации и работе с ними. Таким образом, данная модель направлена на предотвращение как внешних, так и внутренних угроз [1, 2].

Из выше описанного для обеспечения безопасности актуальна разработка модели разграничения доступа с учетом особенностей функциональности АС: динамичность целей, функций, задач и ресурсов, адаптивность к внешним и внутренним дестабилизирующим факторам, необходимостью формального надзора за правильностью действий в критических ситуациях.

При переходе от ИБ к ФБ возникают трудности, вызванные тем, что субъектно-объектный подход, на котором строятся системы, обеспечивающие ИБ, имеют примитивный аппарат взаимосвязи субъекта и объекта (рис. 1).

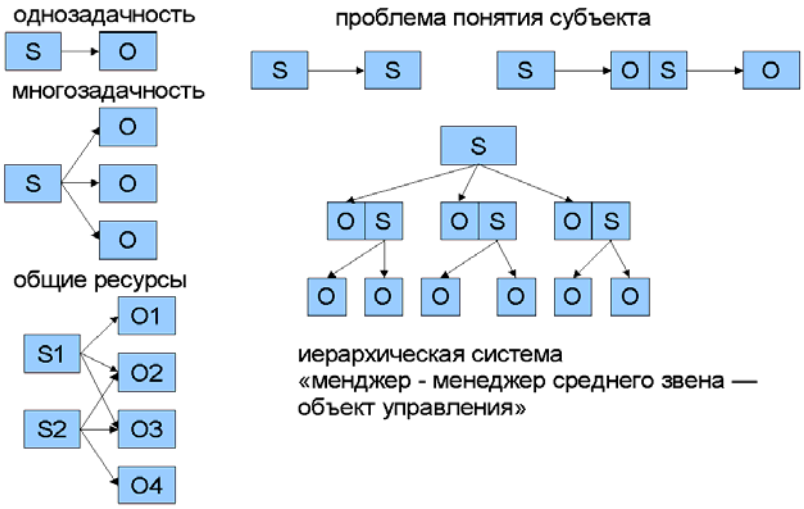


Рис. 1. Композиции субъект-объект и проблема понятия субъекта, где S – субъект, O – объект

Для решения данной проблемы рассматривается среда-ресурс с выделением центрального элемента (рис. 2).

Такой подход облегчает процесс функционирования, пользования общими ресурсами, осуществление удаленного доступа через посредника и обеспечивает большую защиту от НСД [3, 4].

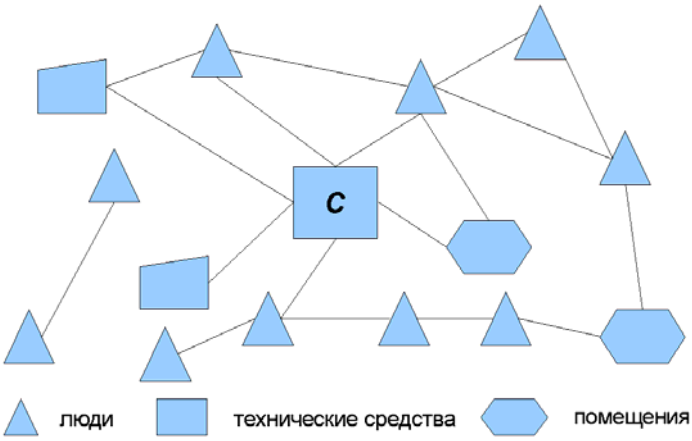


Рис. 2. Условное обозначение сложной системы, состоящей из объектов-систем нескольких видов. *C* – «центральный» экосистемы

В качестве основной модели, которая актуальна в современное время и используется практически во всех АС, выступает дискреционная модель управления доступом. Её недостатком является то, что при одновременном доступе нескольких субъектов к ресурсам одного объекта, возникает вероятность НСД. Таким образом, если субъект S_1 получает доступ к объекту O_2, и в то же время субъект S_2 получает доступ к объекту O_2, то субъект S_2 получает доступ к ресурсам субъекта S_1, чего происходить не должно (рис. 3).

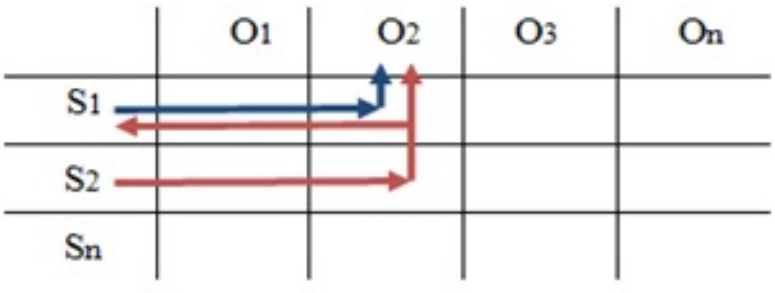


Рис. 3. Недостаток дискреционной модели доступа

Рассмотрим пример, в котором происходит утечка права. Пусть в начальном состоянии (рис. 4) в системе имеются три субъекта: *o*, *s* и *t*, *s* обладает правом записи по отношению к *t*, а *t* некоторым правом *a* (которое может представлять собой либо *r*, либо *w*) по отношению к *o*. Покажем, как субъект *s* может получить право доступа *a* по отношению к субъекту *o* [5].

1. Система находится в начальном состоянии.

2. Субъект *s* создаёт новый субъект *x*, по отношению к которому автоматически получает права чтения и записи.

3. Субъект *s* передаёт субъекту *t* права чтения и записи по отношению к *x*.

4. Субъект *t* передаёт субъекту *x* право доступа *a* по отношению к *o*.
5. Субъект *s* получает от субъекта *x* право доступа а по отношению к *o*.

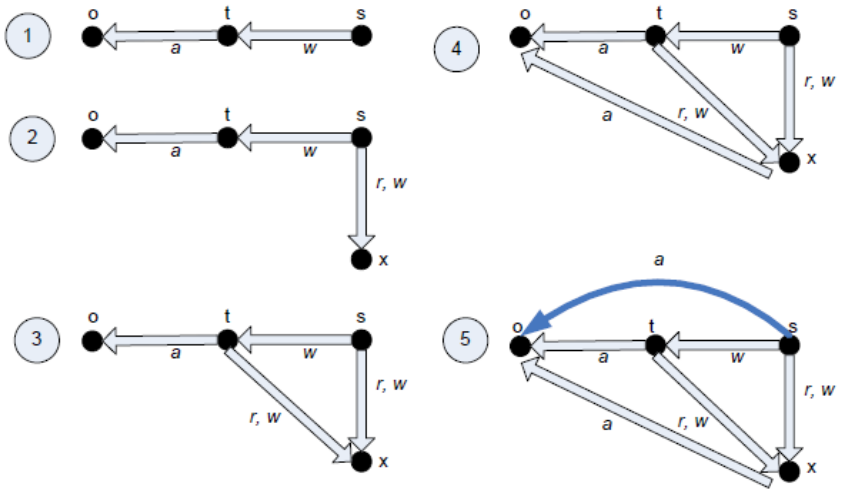


Рис. 4 Утечка права *a*

Данная проблема утечки прав и имеет название «Троянский конь», которая представляет собой вирусную программу, способную нарушить политику безопасности всех моделей разграничения доступа, основанных на матрице доступа. Модель Харрисона-Руззо-Ульмана способна лишь частично повлиять на решение данной проблемы.

Критерий безопасности в модели Харисона-Руззо-Уильмана формулируется следующим образом: для заданной системы начальное состояние $Q_0 = (S_0, O_0, M_0)$ является безопасным относительно права г, если не существует применимой к Q_0 последовательности команд, в результате которой право г будет занесено в ячейку матрицы M, в которой оно отсутствовало в состоянии Q_0.

Смысл данного критерия состоит в том, что для безопасной конфигурации системы субъект никогда не получит право доступа г к объекту, если он не имел его изначально.

Для решения данной проблемы рассматривается функционально-дискреционная модель управления доступом. Так как функция представляет собой ряд задач, то для каждого субъекта составляется определенное правило, которое является основой для организации разграничения и осуществления доступа (рис. 5).

Для создания дискреционной модели описываются шесть элементарных операций: добавление субъекту S права R по отношению к объекту O, удаление у субъекта S права R по отношению к объекту O, создание нового субъекта S, изменения в состоянии системы, удаление существующего субъекта S, создание нового объекта O, удаление существующего объекта

О. При описании ФДМ основой являются те же операции, но добавляется значение функции F, которое включает в себя ряд задач (a_1, a_2,…, a_n) [6, 7].

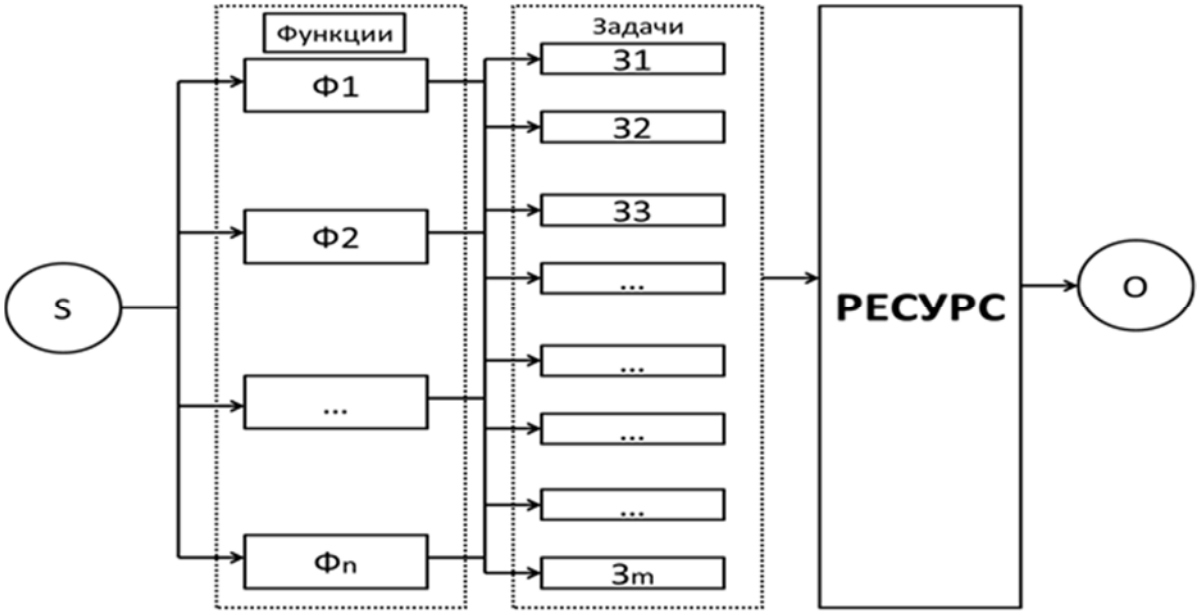


Рис. 5. Схема функционально-дискреционной модели управления доступом

Результатом описания функционально-дискреционной модели доступа является устранение недостатков дискреционной модели и обеспечение автоматизированных рабочих мест должностных лиц защитой от несанкционированного доступа.

Список используемых источников

1. Цирлов В. Л. Основы информационной безопасности автоматизированных систем. Ростов-на-Дону : Феникс, 2008. 173 с. ISBN ISBN 978-5-222-13164-0.

2. Шестухина В.И. Теоретические основы компьютерной безопасности. Ростов-на-Дону : ДВГУПС, 2008. 212 с.

3. Корсунский А. С., Лепешкин О. М. Подход к формализации автоматизированной информационной системы для оценки функциональной безопасности // Вопросы радиоэлектроники. 2012. Т. 3. № 1. С. 75–82.

4. Будко Н. П., Будко П. А., Булгаков О. Ю., Васильев В. В., Давидчук В. В., Евграфов А. Е., Жук А. П., Карпов В. В., Князев В. В., Кублик Е. И., Лепешкин О. М., Лощенков И. В., Ляченков С. В., Мезенцев А. В., Павловский И. С., Пирогов М. В., Попов А. А., Потюпкин А. Ю., Прошин Д. С., Радько С. А. и др. интеллектуализация сложных систем язык схем радикалов в проблемных вопросах предпроектных исследований, оснащения, сопровождения систем и в экспериментальных задачах внедрения критических наукоемких технологий: коллективная монография // Информационно-измерительные и управляющие системы. 2009. Т. 7. № 3. С. 1–92.

5. Бударин Э. А., Васюков Д. Ю., Дементьев В. Е., Колбасова Г. С., Краснов В. А., Лепешкин О. М., Лаута О. С., Митрофанов М. В., Худайназаров Ю. К. Обеспечение защиты информации в локальных вычислительных сетях // Военная академия связи им. Маршала Советского Союза С. М. Буденного. Санкт-Петербург, 2013.

6. Лепешкин О. М., Карпов А. В., Шостак Р. К. Актуальность осуществления сетевого контроля защищенности информационных сетей // Радиолокация, навигация, связь. XXIII Международная научно-техническая конференция. В 3-х томах. 2017. С. 1198.

7. Лепешкин О. М., Фиалкин И. А. Формальная модель функционально-ролевого разграничения доступа // Радиолокация, навигация, связь. XXIII Международная научно-техническая конференция. В 3-х томах. 2017. С. 1199.

Статья представлена старшим преподавателем, доктором технических наук, полковником О. М. Лепёшкиным.

УДК 004.056.53

СКРЫТОЕ ВЛОЖЕНИЕ В БАЙТ-КОД JAVA НА ОСНОВЕ ИСПОЛЬЗОВАНИЯ МЕТОДА ПЕРЕОПРЕДЕЛЯЕМЫХ ЗНАЧЕНИЙ ПЕРЕМЕННЫХ

М. В. Верещагин, А. В. Красов

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

В статье рассмотрены вопросы защиты авторского права на программное обеспечение. В частности, рассматривается возможность и методы вложения цифрового водяного знака в исполняемые файлы Java. Для подробного рассмотрения выбран метод, основанный на переопределении значений переменных. Рассматриваются инструкции, которые можно заменить и данные, которые можно успешно вложить.

скрытие информации, стеганография в исполняемых файлах, покрывающие сообщения, байт-код Java, виртуальная машина Java.

В последнее время защита цифровой продукции от кражи стала одной из самых актуальных проблем. Незаконное копирование программного обеспечения наносит большой материальный ущерб компаниям разработчиков. Один из способов защитить разработчиков от убытков, которые могут быть нанесены кражей программных продуктов, является внедрение цифрового водяного знак [1]. Цифровой водяной знак – это идентификатор авторского права, который можно встроить в программу, указывающий на авторские права. Такой тип защиты не всегда сможет защитить программное обеспечение от кражи, однако, с помощью него можно будет доказать право собственности на программу, либо с какой «лицензии» началось незаконное копирование программы. Цифровой водяной знак скрыт от невооруженных глаз, но определяется специальными декодерами,

настроенными на его выявление. Он встраивается таким образом, чтобы его нельзя было удалить, не повредив продукт.

В данной статье рассматривается вариант вложения ЦВЗ в программу, написанную на языке программирования Java. Таким образом, покрывающим сообщением будет являться class-файл [2]. Избыточность подобного покрывающего сообщения меньше, чем в медиа-файлах, но обнаружить и изъять цифровой водяной знак становится сложнее. В такие файлы можно вложить следующие типы информации:

1. Информация об авторах.
2. Номер лицензии.
3. Информация для проверки целостности программы.

Компилятор преобразует исходный код на языке java в байт-код, который выполняется на виртуальной машине Java и не зависит от архитектуры процессора. Виртуальная машина Java реализована в качестве стековой виртуальной машины. Рассмотрим метод переопределения переменных и замены эквивалентных инструкций. Данный метод может незначительно изменять время работы программы. Виртуальная машина Java, может хранить и выполнять действия практически над всеми видами переменных. Однако, в большинстве случаев, для сокращения и оптимизации кода, она может приводить типы данных к одному. Так, в случае с целочисленными переменными, виртуальная машина Java может применять приведение к int. Благодаря этому можно считать эквивалентными инструкции, представленные в таблице.

ТАБЛИЦА. Команды для замены

61 (ladd) Сложение переменных типа long	60 (iadd) Сложение переменных типа int
63 (dadd) Сложение переменных типа double	62 (fadd) Сложение переменных типа float
65 (lsub) Вычитание переменных типа long	64 (isub) Вычитание переменных типа int
67 (dsub) Вычитание переменных типа double	66 (fsub) Вычитание переменных типа float
69 (lmul) Перемножение переменных типа long	68 (imul) Перемножение переменных типа int
6B (dmul) Перемножение переменных типа double	6A (fmul) Перемножение переменных типа float

Соответственно, вкладывать информацию можно с помощью замен одних инструкций, другими [3]. Обнаружить цифровой водяной знак можно будет имея оригинал программы без вложения. Так, например, можно зара-

нее договориться, что измененная инструкция надо считать «1», а неизменную «0». Пример байт-кода оригинала и изменённого приведён на рисунке ниже.

На рисунке изображена замена операций сложения и умножения переменных типа int на операции сложения и умножения переменных типа long.

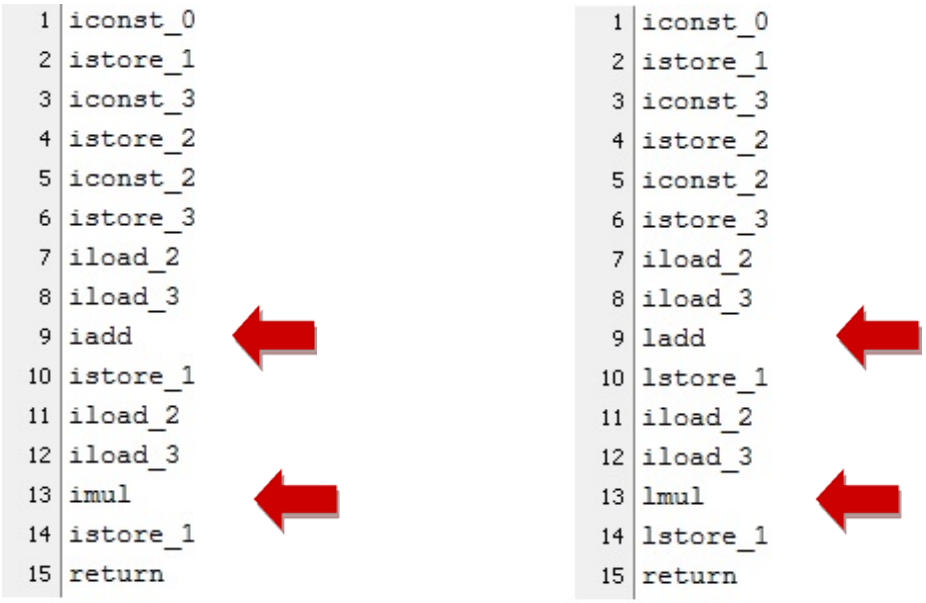


Рисунок. Пример изменения байт-кода

Данный метод позволяет произвести вложение в любую программу, написанную на языке Java достаточного количества символов для вложения информации об авторском праве и номера лицензии. Изменение размера файла либо не происходит, либо несущественно. Данный факт позволяет использовать предложенный метод почти для любой программы. Использование подобного метода позволит при помощи «номера лицензии» определять легитимность использования программного обеспечения и узнавать, от какого пользователя произошла «кража» ПО.

Список используемых источников

1. Shterenberg S. I., Krasov A. V., Ushakov I. A. Analysis of using equivalent instructions at the hidden embedding of information into the executable files // Journal of Theoretical and Applied Information Technology. 2015. Т. 80. № 1. P. 28–34.

2. Шариков П. И., Красов А. В., Штеренберг С. И. Методика создания и вложения цифрового водяного знака в исполняемые java файлы на основе замен опкодов // T-Comm: Телекоммуникации и транспорт. 2017. Т. 11. № 3. С. 66–70.

3. Шариков П. И. Методика нахождение величины наиболее выгодного контейнера в форматах исполняемых файлов // Наукоемкие технологии в космических исследованиях Земли. 2015. Т. 7. № 5. С. 58–62.

УДК 65.654.072

АНАЛИЗ МЕТРИК ДЛЯ ОЦЕНКИ ЭФФЕКТИВНОСТИ РАБОТЫ ПЕРВОЙ ЛИНИИ ТЕХНИЧЕСКОЙ ПОДДЕРЖКИ

А. Ю. Вериков, М. Ю. Скоринов

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

В статье рассматривается понятие эффективности, возможные цели контроля такой характеристики, а также метрики, позволяющие проанализировать эффективность работы первой линии технической поддержки, которая выступает единой точкой входа для клиентов. Для отбора показателей использовались открытые источники, спецификации TMForum и COPC CX Standards.

метрика, показатели, эффективность, assurance подразделение, техническая поддержка.

Эффективность – это анализ того, насколько рационально используются финансовые, трудовые, информационные ресурсы компании для достижения требуемых результатов. Оценка такой характеристики дает возможность определить рациональность расхода ресурсов компании или определить их недостаточность, узнать узкие места в бизнес-процессах, контролировать качество обслуживания клиентов с помощью измеримых показателей в динамике, выявлять возможные проблемы обслуживания и решать их, а также визуально демонстрировать сотрудникам показатели, мотивируя их на лучшую командную работу. Данная характеристика не может носить строго определенного математического значения, это не получение максимальной выручки при минимуме затраченных ресурсов, а анализ насколько качественно, оперативно было выполнено обслуживание клиентов, решение их вопросов и заявок.

В настоящее время в телекоммуникационной деятельности имеется проблема удержания абонентов, контроля лояльности конкретного абонента, ее измерения и повышения [1]. Выполнение функции контроля уровня обслуживания, эффективности работы связано напрямую с лояльностью абонентской базы, на объемы пользования услугами связи, желание приобрести новые, сумму доходов и прибыли.

Assurance подразделение в классической структуре состоит из трех линий технической поддержки, каждая из которых имеет свои особенности и инструменты работы. Первая линия – это структурная единица, цель которой идентификация клиента и его вопроса для дальнейшего логирования

и решения [2]. Для оценки работы зачастую используются метрики, характеризующие параметры звонков, так как основным каналом взаимодействия с клиентом остается телефония. Вторая и третья линии – это следующие структурные единицы, в которых происходит систематизация, анализ и решение заявок в CRM системе, а значит для их оценки необходимо формировать выгрузки обращений клиентов и строить логику оценки на их основе.

Для отбора метрик оценки первой линии можно воспользоваться стандартом Customer Operations Performance Center (COPC) и профильными инструментами, которые дает консорциум TMForum, а именно Frameworx Metrics (GB988). В данной спецификации даны названия, определения, порядок расчета для использования в различных бизнес-процессах. Документ содержит свыше 2500 показателей, которые были определены в TMForum и представляет собой набор последовательных полей и классификаций.

1. Число поступивших/принятых/пропущенных звонков.

Такой показатель является базовым операционным показателем для оценки работы ЦОВ.

В терминологии Frameworx Metrics эти показатели носят название:

– Total inbound calls (tid 400);
– Total Calls Answered On Time (tid 403);
– Total Abandoned calls (tid 401).

2. Среднее время обслуживания вызова.

Этот показатель равен отношению времени обслуживания к количеству обслуженных вызовов, а время обслуживания входящего вызова, в свою очередь, состоит из времени разговора, удержания, постобработки и паузы. Можно сказать, что время обслуживания вызова и есть результат работы сотрудника 1 линии технической поддержки. В спецификации GB988 метрика носит название Average Handle Time (tid 29) [3]. При росте необходимости проанализировать: квалификации операторов, тематику обращений абонентов, значение времени постобработки и паузы, так как возможен их рост по объективным (увеличение количества обращений) и субъективным (искусственное увеличение времени отдыха между звонками, снижение дисциплины среди операторов) причинам.

3. Уровень обслуживания.

Показатель в англоязычной литературе называется Service Level и определяется, как процент ответов в определенный интервал времени [4]. Наиболее известным примером является ситуация, когда на 80 % вызовов операторы должны отвечать в течении первых 20 секунд с начала соединения, в данном случае целевой SL = 80/20. Стандарты не предъявляют конкретных цифр к этому показателю, но разумеется низкий SL вызывает неудовлетворенность абонентов. В Frameworx Metrics наиболее подходящая

метрика носит название Total Calls Answered On Time (tid 403). Мониторинг данного показателя перекрывает необходимость контроля среднего времени ожидания ответа оператора.

4. Время ожидания звонка.

Имеют место быть временные промежутки, когда оператор готов принять вызов, но вызова/разговора еще нет. Данный показатель обратно пропорционален метрике Occupancy, которая будет описана и в среднем составляет 13–32 % общего продуктивного времени работы оператора (при нормальном уровне Occupancy 68–87 %).

Время в ожидании это резерв (буфер), который позволяет держать уровень сервиса (*Service Level*) в заданных параметрах при колебании количества пришедших звонков в один момент времени. Согласно имеющемуся описанию метрик в спецификации GB988, наиболее подходит показатель Total Headset Hours (tid 398).

5. Occupancy.

Такой показатель дает возможность оценить насколько эффективно составлены графики работы операторов, не находятся ли операторы много времени в режиме ожидания звонка (*Available time*) или наоборот, загруженность звонками выше нормы. Вычисляется он как отношение времени обслуживания вызова к сумме времени обслуживания и времени ожидания звонка [4].

Средний целевой показатель равен 68–87 %. Если измеренное значение меньше, значит на линии одновременно находится больше операторов, чем нужно, а это неэффективно потраченные финансовые ресурсы, если значение приближается к 90 % – стоит задуматься расширении штата сотрудников, так как человеческий ресурс на пределе.

6. Utilization.

Именно это метрика характеризует насколько эффективно сотрудник отработал затраченные финансовые ресурсы, сколько времени он уделял непосредственно исполнению своих обязанностей и своей зоне ответственности. Для расчета здесь необходимо знать общую продолжительность оплачиваемого времени. Если в компании не оплачивается время обеда, тренинги, вебинары, то они исключаются из расчета.

Вычисляется Utilization как отношение суммы времени обслуживания и времени ожидания звонка к оплачиваемому времени сотрудника

Рекомендуемое значение согласно стандарту COPC 86 % [4].

7. First Call Resolution.

Решение вопроса клиента во время его первого обращения в режиме разговора не только повышает удовлетворенность клиентов, но и уменьшает

количество повторных звонков, что снижает нагрузку на операторов и затраты. Для решения задачи вычисления метрики лучше после окончания разговора с оператором использовать автоинформатор с вопросом о том, что решена ли проблема пользователя, также можно использовать данные из CRM системы, осуществляя поиск обращений того же клиента с той же тематикой.

8. Время решения заявок. Конверсия. Воронка.

По результатам работы подразделения могут строить так называемые воронки. Применительно к технической поддержке на верхнем уровне можно отразить количество заявок первой линии, на нижнем – на третьей линии. Соответственно, нужно, чтобы как можно больше заявок решалось на первой линии, и как можно меньше передавалось на третью.

Ниже приведен пример отражения числа заявок (*Customer Requests* – tid 230) и времени их решения (*Hours Service Problem Handling Time, Per Service Problem Report Resolved* – tid 70) на каждой из линий технической поддержки, а также доли от общего числа заявок, которая решается на заданной линии – процент конверсии (рис.).

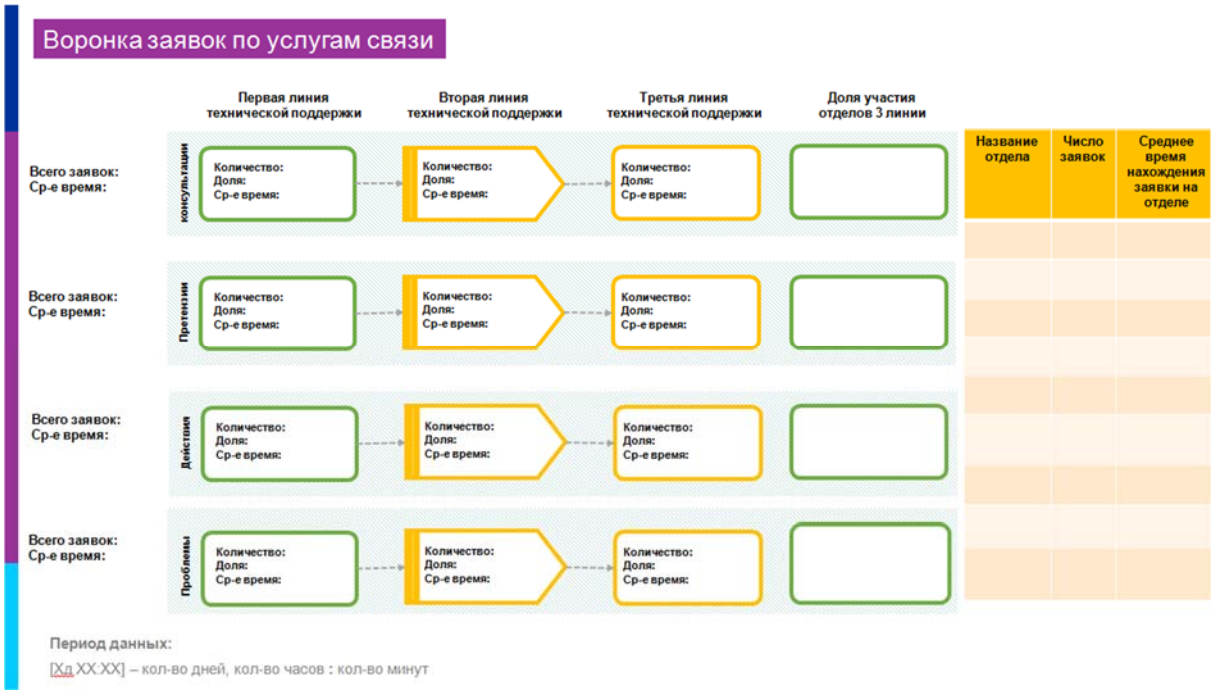


Рисунок. Воронка заявок

Список используемых источников

1. Ланкевич К. Е., Хабаев Н. С., Скоринов М. Ю. OSS комплекс как инструмент контроля лояльности клиентов оператора связи // T-Comm: Телекоммуникации и транспорт. 2016. Т. 10. № 5. С. 36–40.

2. Самолюбова А. Б. Call Center на 100 %: практическое руководство по организации Центра обслуживания вызовов. 2-е изд., перераб. и доп. М. : Альпина Паблишер, 2010.

3. Robert Bratulic, Gerard Damm, Leszek Lesiewicz, Snigdha Mitra. TM Forum Metrics Definitions Rel 16.5.0. 2016 [Электронный ресурс]. URL: https://www.tmforum.org/resources/best-practice/gb988-tm-forum-metrics-definitions-r16-5-1 (дата обращения: 20.03.2018).

4. COPC Customer Experience Standard, Rel 6.0a, Ver 1.0 [Электронный ресурс]. URL: https://www.copc.com/copc-standards/copc-cx-standards-release-6-0 (дата обращения: 20.03.2018).

Статья представлена научным руководителем, кандидатом технических наук, доцентом кафедры А. Б. Гольдштейном.

УДК 004.056.5

АУДИТ ЛОКАЛЬНО-ВЫЧИСЛИТЕЛЬНЫХ СЕТЕЙ ОРГАНОВ ГОСУДАРСТВЕННОЙ ВЛАСТИ

Л. А. Виткова, А. С. Гаврилов Е. Ю. Герлинг, А. А. Глущенко

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

Одним из важнейших этапов в управлении информационной безопасности ИТ-инфраструктуры предприятия является аудит сетей. Авторы доклада рассматривают этапы аудита локально-вычислительных сетей государственных органов и представляют возможные варианты оптимизации процесса, используя последние технические средства.

локально-вычислительные сети, аудит, топология, сервер, маршрутизатор, коммутатор, сетевое оборудование, оконечные устройства, коммутация, ПО.

Введение

Многие организации производят стыковку своих сетей с общественными сетями передачи данных (*Public Data Networks*), в частности с Internet. Часто возникает необходимость консолидации удаленных офисов с центральным, в том числе организация доступа к общим ресурсам и организация совместной работы.

Локально-вычислительная сеть (ЛВС) представляет собой комплекс оборудования, обычно находящихся в одном здании, и программного обеспечения, обеспечивающий передачу, хранение и обработку информации.

Оборудование делится на три типа:

1. Активное оборудование:
   - Повторители, концентраторы.
   - Коммутаторы, маршрутизаторы.
2. Компьютерное и периферийное оборудование:
   - Серверы.
   - Рабочие станции.
   - Принтеры.
   - Сканеры.
3. Пассивное оборудование:
   - Кабели.
   - Монтажные шкафы.
   - Коммутационные панели.
   - Информационные розетки.
   - Каналы связи.

Каналы связи делятся на:

✓ Кабельные технологии (Витая пара, коаксиальный кабель, оптоволоконный кабель).

✓ Беспроводные технологии (Радио среда, передача данных в микроволновом диапазоне, лазерная передача, инфракрасные технологии).

Локальные сети позволяют отдельным пользователям легко и быстро взаимодействовать друг с другом, и обращаться к совместно используемым ресурсам.

Варианты построения ЛВС сводятся к трем типам:

• Проводные сети.

• Беспроводные сети.

• Смешанный тип сетей.

Также немаловажное значение имеет топология локально-вычислительной сети. Топология – это физическая конфигурация сети в совокупности с ее логическими характеристиками.

Существует несколько видов топологий:

▪ Шинная топология основана на использовании кабеля, к которому подключены рабочие станции.

▪ Кольцевая топология характеризуется тем, что рабочие станции последовательно соединяются друг с другом, образуя замкнутую линию. Выход одного узла сети соединяется со входом другого.

▪ Звездообразная топология основывается на концепции центрального узла (сервера или пассивного соединителя), к которому подключаются рабочие станции сети.

▪ Древовидная топология представляет собой более развитый вариант шинной топологии. Дерево образуют путем соединения нескольких шин.

▪ Полносвязная топология является наиболее сложной и дорогой. Она характеризуется тем, что каждый узел сети связан со всеми другими рабочими станциями.

Современные компьютерные сети имеют сложную структуру. Со временем наступает момент, когда уровень информационных технологий перестает соответствовать потребностям организации. Поэтому, как и в любой системе, в ней могут появиться слабые и уязвимые места, которые могут привести к несвоевременному получению, неадекватности или неудобной организации информации, необходимой для выработки управленческих решений. В связи с этим обеспечение безопасности передаваемой, хранимой и обрабатываемой информации требует все больших усилий. В особенности, учитывая важность государственной и коммерческой информации, возможные проблемы в случае ее частичной потери или утечки – обеспечение безопасности информационно-технической инфраструктуры представляется одной из ключевых задач.

Анализ

Для оценки состояния информационной инфраструктуры организации и выработки методов приведения в соответствие этого состояния потребностям служит аудит информационной инфраструктуры.

Аудит сети - это комплекс мер по анализу, обследованию и тестированию работы всех элементов сетевой инфраструктуры компании с последующей разработкой и выдачей рекомендаций по ее модернизации [1].

Цель аудита сети – анализ уязвимостей компонентов ЛВС (таких как сервера баз данных, межсетевые экраны, маршрутизаторы, сервера приложений, терминальные, почтовые, WEB, рабочие станции) с целью устранения этих уязвимостей, оптимизации и повышения надежности.

Источники угроз делятся на 2 группы:

• Внешние, связанные с окружающей средой ИТ инфраструктуры. (Контроль входящего и исходящего Интернет трафика, защита компьютерных сетей от вирусов и хакерских атак, обеспечение безопасного удаленного доступа в компьютерные сети для сотрудников организации, борьба со спамом).

• Внутренние, возникающие непосредственно в компьютерной сети. (Риски, связанные с устройствами ввода-вывода информации, защита от сбоев и потери важных сведений, архивирование и резервное копирование важной информации, разграничение прав доступа к информации с целью повысить безопасность ИТ-инфраструктуры) [2].

Объектами аудита являются:

• Оборудование ЛВС/БЛВС.

• Логическая структура сети.

- Межуровневое взаимодействие.
- Способы подключения клиентских устройств к сети.
- Применяемые решения по обеспечению безопасности сети.
- Системы мониторинга и управления сетевой инфраструктурой.
- Подключение к внешним сетям.

Аудит ЛВС целесообразно проводить:

❖ Нет сети или отсутствует вся необходимая документация на нее.

❖ Произошел переезд в новый офис – сеть там уже проложена, но необходимо настроить ее «под себя».

❖ Перед модернизацией сети, если появилась необходимость спроектировать новую сеть;

❖ После модернизации сети, чтобы убедиться, что сеть удовлетворяет требованиям стандартов Российского законодательства;

❖ При возникновении подозрений в утечке трафика и несанкционированного доступа к ресурсам локальной сети;

❖ Для повышения стойкости сети перед возможными атаками с целью предотвращения вывода ее из строя или кражи информации;

❖ При увеличении нагрузки на сеть [3].

Основные этапы работ:

- Анализ требований.
- Разработка регламента, устанавливающего порядок и рамки проведения работ.
- Инструментальный сбор информации технической инфраструктуры организации.
- Анализ собранной информации с целью выявления технологических, эксплуатационных уязвимостей, «узких мест», а также недостатков организационно-правового обеспечения.
- Документирование и подготовка отчетной документации [4].

Инструментальный анализ предназначен для:

- Инвентаризация ресурсов сети (устройства, ОС, службы, ПО).
- Идентификация и анализ технологических уязвимостей и «узких мест» [4].
- Подготовка отчетов с описанием проблем и методов отладки.

Типы используемых для анализа средств:

- Сетевые сканеры безопасности.
- Сканеры безопасности для конечного пользователя (проверка ОС и приложений).
- Утилиты удаленного администрирования.
- Утилиты для верификации найденных уязвимостей.
- Утилиты для инвентаризации ресурсов [5].

Отчет по итогам аудита включает в себя:

- Актуальную информацию о физической и логической топологии ЛВС/БЛВС.
- Информацию о необходимых направлениях развития ЛВС/БЛВС.
- Список существующих в сети проблем.
- Набор мер по устранению обнаруженных проблем.
- Рекомендации по модернизации логической и физической топологии, а также предложения по применению дополнительного сетевого оборудования с целью достижения повышения надежности, эффективности, безопасности ЛВС/БЛВС.
- Рекомендации по подключению ЛВС/БЛВС к внешним сетям [5].

Выводы

Проведение аудита ЛВС обеспечивает следующие преимущества:

- Объективная оценка реального состояния локальной сети.
- Обнаружение уязвимых мест и рекомендации по их устранению.
- Обоснованные рекомендации по модернизации, изменению архитектуры, замене оборудования и обновлению программного обеспечения.
- Экономия финансовых средств за счет оптимизации.
- Повышение степени защиты и надежности сети.

Список используемых источников

1. Официальный сайт компании «Techsvit». URL: https://techsvir.eu/services/audit-setevogo-oborudovaniya.html.

2. Официальный сайт компании «ЭЛИАС». URL: http://elias.ru/localnet/.

3. Официальный сайт компании «IT-Professional». URL: https://it-professional.ru/audit/lan_audit.

4. Официальный сайт национального открытого университета «ИНТУИТ». URL: https://www.intuit.ru.

5. Электронный ресурс http://life-prog.ru/1_1235_instrumentalnie-sredstva-analiza-sistem-zashchiti.html.

УДК 004.056

МЕТОДЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ ПРИ ВОЗНИКНОВЕНИИ ЧРЕЗВЫЧАЙНОЙ СИТУАЦИИ

Л. А. Виткова, В. С. Гераськина, И. А. Ушаков

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

Обеспечение безопасности населения города является одной из основных задач правительства. В статье рассмотрены системы и методы оповещения населения, эффективность их использования, а также отличные способы оповещения, тенденции использования различных систем и устройств в повседневной жизни.

оповещение о чрезвычайных ситуациях, информирование, система оповещения, источник информации, информационная безопасность.

Жизнь современного общества подвержена различного вида опасности. Помимо опасностей природного и техногенного характера, стоит выделить угрозы национальной безопасности, в том числе различные теракты, пожары и многие другие. Проблема уведомления о таких глобальных происшествиях является актуальной в любое время. Ведь чем сильнее прогресс, тем больше должна быть зона распространения информации.

Оповещение и информирование населения является одной из главных составляющих и одной из основных задач органов управления всех уровней, организующих защиту в ЧС мирного и военного времени. Реагирование на любую ЧС начинается с оповещения и информирования о возникновении или угрозе возникновения какой-либо опасности.

Одними из самых основных задач единой государственной системы предупреждения и ликвидации чрезвычайных ситуаций являются:

– сбор, обработка, обмен и выдача информации в области защиты населения и территорий от чрезвычайных ситуаций;

– организация оповещения населения о чрезвычайных ситуациях и информирования населения о чрезвычайных ситуациях, в том числе экстренного оповещения населения;

– и некоторые другие.

Конституция РФ, Закон «О стратегии национальной безопасности РФ», Доктрина информационной безопасности РФ гарантируют нам защищенность в случаях ЧС, а главное своевременное и актуальное информирование о ЧС и способах защиты населения.

Рассмотрим способы экстренного информирования в современном мире.

Во многих странах до сих пор основной системой оповещения остается использование сирен и громкоговорителей, установленных повсеместно, не исключается так же радио-, спутниковое и телевещание. В Японии общенациональная система предупреждения населения работает через спутники, что позволяет властям оперативно транслировать оповещения в местных СМИ и через громкоговорители. В США помимо выше названных способов существует беспроводная система предупреждения о ЧС (*Wireless Emergency Alerts*, WEA) [1]. Это текстовые сообщения с предупреждениями о ЧС, которые отправляются уполномоченными госорганами на сотовые телефоны и мобильные девайсы. В Польше с помощью Региональной системы оповещения власти предупреждают население о грядущих катаклизмах по телевидению, на своих сайтах и через специально разработанные для всех платформ мобильные приложения. На телевидении сообщения появляются в виде надписей, содержащих краткую информацию о ЧС. Курсирующие по населенным пунктам машины с громкоговорителями тоже могут оповещать население.

Как и в большинстве развитых стан, в России применяется система оповещения через громкоговорители и сирены, телерадиовещание.

Ключевое звено в системе защиты населения – централизованное оповещение граждан по системе гражданской обороны. Электросирены находятся практически во всех населенных пунктах и располагаются на крышах самых высоких зданий.

Существует общероссийская комплексная система информирования и оповещения населения в местах массового пребывания людей (ОКСИОН), объединяющая большое количество различных функций и играющая большую роль в современном городе.

С развитием технологий и появлением мобильной связи к оповещению подключили операторов мобильной связи. МЧС заключило договор с ведущими операторами связи, а это подразумевает рассылку уведомлений как минимум о погодных катаклизмах. Однако и эта система работает не идеально.

Минком связи РФ разработало правила оповещения о ЧС, согласно которым, оповещение населения будет осуществляться по СМС, при помощи автодозвона или передачи голосового сообщения. Кроме того, пользователь может быть автоматически перенаправлен на специально созданную страницу при выходе в интернет. Но возникает вопрос о времени внедрения столь действенной системы.

Компания «Протей» разработала систему Cell Broadcast-центр, которая представляет собой центр рассылки коротких вещательных сообщений

для сетей стандарта GSM. Система обеспечивает возможность вещания информации, передаваемой внешними приложениями, всем абонентам, находящимся в определенном сегменте зоны обслуживания оператора GSM. Применение комплекса совместно с технологией SIM Toolkit открывает для абонента возможность интерактивного взаимодействия с системой через SIM-menu. Внедрение оборудования НТЦ «Протей» позволяет оператору получить удобное средство для массовой рассылки абонентам «локально-зависимой» информации.

Учитывая неоднородность слоев населения, использующих всевозможные устройства связи (различного функционала и поколения), стоит взять во внимание различные способы отправки уведомлений, разнообразие средств приема, а также его функционал.

На данном этапе существует большое количество технологий продвижения информации в массы. И сейчас мы говорим об информации в целом.

На рис. 1 приведена статистика использования различных источников получения информации в сравнении 2013 и 2017 годов в России.

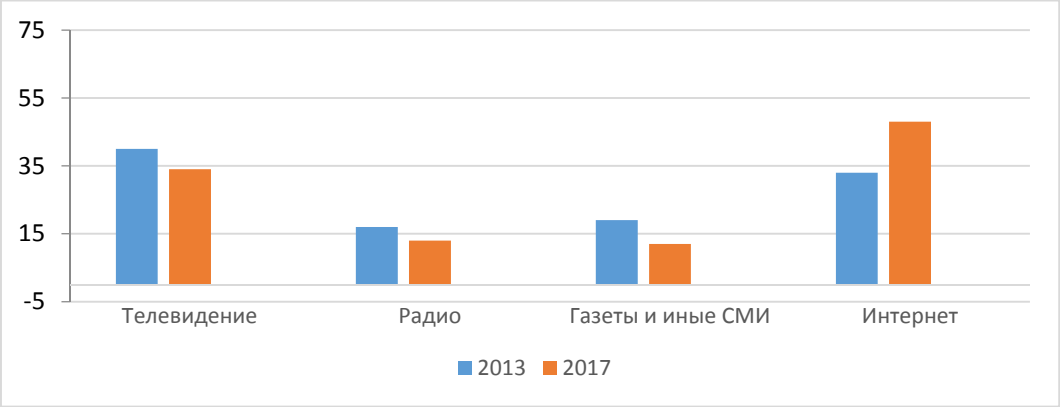


Рис. 1. Статистика использования различных источников информации

Примерно половина населения страны до сих пор большую часть информации получает посредством просмотра телевидения: этот источник пользуется наибольшим доверием среди граждан [2]. Так же предпочтение отдается радио и газетам, но стоит отметить, что доля людей, использующих эти источники сильно снижается. Однако, это касается преимущественно старшего поколения. Сейчас 40 % населения страны – это люди младше 35-ти лет. Именно эта группа людей все больше использует всемирную сеть «Интернет» для поиска и получения информации [3]. Уже с 2013 г. Интернет занимает второе место в России в списке источников информации. Учитывая тенденции развития информационного пространства сети Интернет, в 2017 г. показатели среди опрашиваемых граждан возрастают – все большее число людей пользуются именно этим каналом связи для получения информации.

Рассмотрим статистику использования определенных устройств для поиска в сети «Интернет», приведенную на рис. 2 [4].

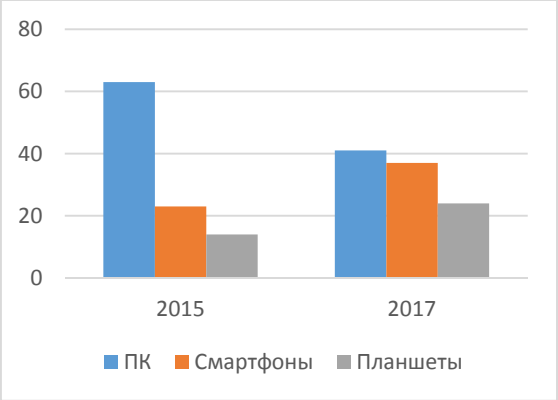


Рис. 2. Статистика использования устройств для входа в Интернет

По исследованиям 2015 г. более 60 % пользователей заходят в интернет через ПК, соответственно около 23 через смартфоны и 17 через планшеты. С учетом увеличения площади покрытия городов сетью «Интернет» можно сделать вывод, что уже к концу 2017 г. пользователей ПК становится меньше.

Как известно, на одного человека приходится хотя бы один телефон, на два – хотя бы один смартфон, а в некоторых случаях по несколько смартфонов, включая планшет на одного человека. В связи с этим и возрастает время, проводимое в сети «Интернет». Очень часто, погружаясь и интернет пространство люди абстрагируются от реальности. Достаточно посмотреть вокруг – каждый второй в наушниках или увлечен чтением с головой.

Тут стоит задуматься о том, что уже существующие способы оповещения не в полной мере охватывают население и уже имеющиеся способы оповещения не очень эффективны.

Стоить помнить, что сейчас стало возможно использование устройств без SIM-карт, осуществляя подключение к интернету по Wi-Fi. Особенно часто это практикуется в мессенджерах. Учитывая выше сказаное, необходимо сделать моментальную рассылку уведомлений или создать определенные каналы, позволяющие оповещать пользователей о ЧС.

Существует система **DPI (система глубокого анализа трафика), которая** получила широкое распространение среди операторов связи и интернет-провайдеров за счет функций блокировки запрещенных ресурсов по спискам Роскомнадзора, улучшения эффективности использования полосы пропускания, а также повышения удовлетворенности пользователя от предоставляемых услуг и QoS [5].

Данная технология помогает управлять трафиком, а значит и уведомлять абонентов. Эта Функция позволяет оператору передавать сообщения абоненту во время работы в Интернете. Пользователь вводит адрес сайта, который хочет посетить, и видит в браузере сообщение от оператора, сменяемое через несколько секунд запрашиваемой страницей.

Все это наводит на мысль о том, что «Интернет» является почти самым распространенным СМИ, но никак не адаптирован под действительно важные функции. Действительно важной задачей является внедрение различ-

ных, способов оповещения именно в сети «Интернет», помимо уже имеющихся, будь то различные системные сообщения или всплывающие окна в браузерах.

В данной статье используются данные, представленные для общего пользования различными исследовательскими компаниями, в частности ГК ФОМ.

Список используемых источников

1. Информационный источник РИА-Новости [Электронный ресурс]/ URL: https://ria.ru/spravka/20121116/910970183.html

2. Новостной источник РБК [Электронный ресурс]. URL: https://www.rbc.ru/society/18/06/2014/57041e609a794760d3d3f677

3. Информационный источник ФОМ [Электронный ресурс]. URL: http://fom.ru/SMI-i-internet/13323

4. Информационный источник GFK [Электронный ресурс]. URL: http://www.gfk.com/ru/insaity/press-release/issledovanie-gfk-tendencii-razvitija-internet-auditorii-v-rossii/

5. VASEXPERTS [Электронный ресурс]. URL: https://vasexperts.ru/blog/opoveshhenie-naseleniya-v-sluchae-chs-reshenie-dlya-operatorov-svyazi/

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

УДК 004.056

ВЫБОР ОПТИМАЛЬНОГО МЕТОДА ОЦЕНКИ ЭФФЕКТИВНОСТИ ПЕРЕХОДА К ОБЛАЧНОЙ АРХИТЕКТУРЕ

Л. А. Виткова, А. А. Глущенко, Д. В. Сахаров, М. В. Чмутов

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

По всему миру происходит развитие облачных вычислений, и все больше организаций переходят на облавные технологии. Изучение различных методов перехода к облачной архитектуре позволит выбрать наиболее эффективный и надёжный способ. Облачные технологии имеют большой потенциал, но при переходе на облачную архитектуру можно столкнутся с рядом проблем.

облачная архитектура, OpenStack, единая информационная система, оценка эффективности.

При переходе на сложные и высокопроизводительные среды компании должны понимать, какие приложения и данные переводить туда и как это сделать. Облачное перемещение – это мульти-дисциплинарный процесс, охватывающий огромное количество функции. Миграционные команды из разных департаментов должны заранее оценить задачу, чтобы обеспечить плавный переход в облако, удовлетворяющий все потребности и соответствующий правилам, без ущерба для безопасности бизнеса [1].

Понимание стратегических целей миграции в облако даст понять, как поступать компании в начале процесса. Гибкость и подвижность – общая цель перемещения в облако, поскольку для цифровой трансформации нужны более управляемые технологические платформы.

Создание гибкой среды облачных вычислений предполагает пересмотр существующего ряда приложений. Устаревшие приложения не предназначены для работы в распределенных, виртуализированных системах и публичном или частном облаке. Их адаптация или трансформация станет важной частью процесса облачной миграции.

Требования к безопасности облачных вычислений не отличаются от требований безопасности к центрам обработки данных. Однако, виртуализация ЦОД и переход к облачным средам приводят к появлению новых угроз. Доступ через Интернет к управлению вычислительной мощностью один из ключевых характеристик облачных вычислений. В большинстве традиционных ЦОД доступ инженеров к серверам контролируется на физическом уровне, в облачных средах они работают через Интернет. Разграничение контроля доступа и обеспечение прозрачности изменений на системном уровне является одним из главных критериев защиты.

Серверы облачных вычислений и локальные серверы используют одни и те же операционные системы и приложения. Для облачных систем угроза удаленного взлома или заражения вредоносным ПО высока. Риск для виртуальных систем также высок. Параллельные виртуальные машины увеличивает «атакуемую поверхность». Система обнаружения и предотвращения вторжений должна быть способна обнаруживать вредоносную активность на уровне виртуальных машин, вне зависимости от их расположения в облачной среде [2].

Когда виртуальная машина выключена, она подвергается опасности заражения. Доступа к хранилищу образов виртуальных машин через сеть достаточно. На выключенной виртуальной машине абсолютно невозможно запустить защитное программное обеспечение. В данном случаи должна быть реализована защита не только внутри каждой виртуальной машины, но и на уровне гипервизора.

Среда, имитирующая облачную архитектуру, позволит миграционной команде перенастроить и проверить приложения перед их переносом.

Это область, где облачные разработки могут весьма пригодиться, автоматизируя и ускоряя работу облачных архитектур для быстрого тестирования и развертывания.

Необходимо учесть важность приложений для вашего бизнеса и приемлемый уровень простоя, а также требования к безопасности данных этого приложения. Такие параметры повлияют на тип сервиса, на который вы будете переносить приложения. Это может быть модель «софт как услуга» (SaaS), «платформа как услуга» (PaaS) или «низкоуровневая инфраструктура как услуга» (IaaS) [3]. Также эти параметры покажут, сможет ли программное обеспечение работать в общедоступной облачной инфраструктуре, локальном частном облаке или, возможно, в гибридной модели. Объем данных, обрабатываемых приложением, также сильно зависит от миграционного плана. Если рабочая нагрузка включает большой объем данных, команды миграции должны четко понимать, как переносить их в физическое месторасположение.

Этот процесс связан с логическими и физическими проблемами. Миграционным командам предстоит определить формат и разработать под него политику миграции. Это может быть связано с миграцией всего образа сервера, изменением его конфигурации в соответствии с облачными стандартами среды или переносом существующей виртуальной технологии из частной облачной среды.

Решения по защите от угроз безопасности.

Сохранность данных шифрованием. Шифрование – один из самых эффективных способов защиты данных. Провайдер, предоставляющий доступ к данным должен шифровать информацию клиента, хранящуюся в ЦОД, а и безвозвратно удалять в случае отсутствия необходимости.

Защита данных при передаче. Зашифрованные данные при передаче должны быть доступны только после аутентификации. Данные не получится прочитать или сделать изменения, даже в случаи доступа через ненадежные узлы. Такие технологии достаточно известны, алгоритмы и надежные протоколы AES, TLS, IPsec давно используются провайдерами [4].

Аутентификации – защита паролем. Для обеспечения более высокой надежности, часто прибегают к токенам и сертификатам. Для прозрачного взаимодействия провайдера с системой идентификации при авторизации, также рекомендуется использовать LDAP (*Lightweight Directory Access Protocol*) и SAML (*Security Assertion Markup Language*).

Изоляция пользователей. Использование индивидуальной виртуальной машины и виртуальную сеть. Виртуальные сети должны быть развернуты с применением таких технологий, как VPN (*Virtual Private Network*), VLAN (*Virtual Local Area Network*) и VPLS (*Virtual Private LAN Service*). Часто провайдеры изолируют данные пользователей друг от друга за счет изменения данных кода в единой программной среде [5].

Выводы. Описанные решения по защите от угроз безопасности облачных вычислений неоднократно были применены системными интеграторами в проектах построения частных облаков. После применения данных решений количество случившихся инцидентов существенно снизилось. Правильное использование средств защиты, грамотная постановка целей миграции и качественное сопровождение и проверка действий по переходу на облачную архитектуру помогут в успешной реализации процесса миграции с должным уровнем защищенности [6].

Список используемых источников

1. OpenStack® Ocata Strengthens Core Infrastructure Services and Container Integration with 15th Release of Cloud Computing Software. URL: https://www.openstack.org/news/view/302/openstack-ocata-strengthens-coreinfrastructure-services-and-container-integration-with-15th-release-of-cloud-computing-software/ (дата обращения 22.03.2018).

2. Алейников А. А., Билятдинов К. З., Красов А. В., Кривчун Е. А., Крысанов А. В. Технические аспекты управления с использованием сети интернет: монография, СПб. : Центр научно-информационных технологий «Астерион», 2016. 305 с. ISBN 978-5-00045-408-4.

3. Открытая облачная архитектура IBM. URL: https://www.ibm.com/cloud/learn/iaas-paas-saas/ (дата обращения 22.03.2018).

4. Алейников А. А., Билятдинов К. З., Красов А. В., Левин М. В. Контроль, измерение и интеллектуальное управление трафиком: монография. СПб. : ЦНИТ Астерион, 2016. 92 с.

5. Красов А. В., Левин М. В. Возможности управления трафиком в рамках концепции SDN // Актуальные проблемы инфотелекоммуникаций в науке и образовании. IV Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 2 т. 2015. С. 350–354.

6. Виткова Л. А., Андрианов В. И. Исследование и разработка адаптивных систем информационной безопасности на основе теории бифуркации // Актуальные проблемы инфотелекоммуникаций в науке и образовании. II Международная научно-техническая и научно-методическая конференция: сб. науч. ст. 2013. С. 813–815.

УДК 004.056

ТЕХНОЛОГИЯ БЛОКЧЕЙН И ЕЁ ПРИМЕНЕНИЕ

Л. А. Виткова, В. В. Гореленко, Д. В. Сахаров, И. С. Чернобородов

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

В настоящее время технология блокчейн стала очень популярна. Актуальность вызвано её применением в криптовалютах, таких как биткоин, управлении данных и дру-

гое. Различные структуры, включая государственные, активно внедряют данную технологию для улучшения и оптимизации своих процессов. В статье были рассмотрены различные применимости с более детальным анализом в криптовалюте "Bitcoin".

блокчейн, криптовалюта, БД, биткоин, хэширование, SHA256.

Технология блокчейн (*blockchain*) стала широко известна достаточно недавно, в 2008 г., когда данный концепт представил миру Сатоши Накамото, но благодаря своим применимостям, можно причислить её к разряду самых популярных и актуальных на данный момент в сфере информационных технологий.

Блоки информации, объединённые в цепочку, представляют из себя распределенную БД (базу данных), которая хранит в себе постоянно растущий список упорядоченных записей. В каждый блок вшита метка времени и ссылка на предыдущий блок.

Главной особенностью блокчейна является возможность доверительного обмена без наблюдения или посредничества третьей стороны, сильно сокращая или даже устраняя риск контрагента.

Безопасность реализовывается посредством применения криптографии, при этом сохраняя прозрачность и проверяемость всех операций. Различные криптографические техники гарантируют неизменность журнала транзакций блокчейна, решают задачу аутентификации и контролируют доступ к сети и данным в блокчейне в целом [1].

Блок транзакций применяется в криптовалюте Биткоин (*Bitcoin*). В данной криптовалюте используется система с закрытыми и открытыми ключами, представляющих из себя последовательность бит. Благодаря закрытому ключу, участники обмена могут создавать свои уникальные цифровые подписи, при этом различающиеся в зависимости от сообщений. Для подтверждения подписи используется открытый ключ. Открытый ключ реально вычислить на основе закрытого ключа, а вот обратное преобразование требует невозможного на практике объема вычислений.

В биткойне используется стандарт эллиптической криптографии ECDSA вместе с эллиптической кривой secp256k1. В ней закрытый ключ имеет длину 32 байта, открытый – 33 байта, а подпись – около 70 байт [2].

При переводе данной валюты между пользователями формируется транзакция, где записывается, откуда следует взять данные криптоединицы, а точнее происходит отсылка к предыдущей транзакции, и открытый ключ того, кому они будут отправлены.

Затем отправитель подписывает транзакцию, используя свой секретный ключ. Любой узел в биткойн-сети может проверить, что транзакция подписана определенным открытым ключом (аутентификация), с которым

до выполнения транзакции были ассоциированы данные криптоединицы (авторизация). Если эти условия выполнены, то переведенный биткойны начинает ассоциироваться с открытым ключом получателя.

В блокчейне информация об аутентификации содержится в каждой транзакции, что позволяет полностью защитить систему от попыток обойти данный процесс.

Хеш-функции в блокчейнах гарантируют необратимость всей цепочки транзакций. Дело в том, что каждый новый блок транзакций ссылается на хеш предыдущего блока в реестре. Хеш самого блока зависит от всех транзакций в блоке, но вместо того, чтобы последовательно передавать транзакции хеш-функции, они собираются в одно хеш-значение при помощи двоичного дерева с хешами (дерево Меркла). Таким образом, хеши используются как замена указателям в обычных структурах данных: связанных списках и двоичных деревьях [3].

За счет использования хешей общее состояние блокчейна – все когда-либо выполненные транзакции и их последовательность – можно выразить одним-единственным числом: хешем самого нового блока. Поэтому свойство неизменности хеша одного блока гарантирует неизменность всего блокчейна.

Для биткоина был выбран алгоритм SHA256 с длиной дайджеста сообщения в 256 бит, однако в иных криптовалютах применяются и другие хеш-функции.

Помимо криптовалюты технология блокчейн может использоваться для хранения любого вида цифровой информации.

С блокчейном тесно связан механизм умных-контрактов. Это компьютерный протокол, который на основе математических алгоритмов самостоятельно проводит сделки с полным контролем за их выполнением.

Механизм «умных контрактов» (*smart contract*) состоит из применения фрагмента кода, запрограммированного таким образом, что он начнет выполнятся только тогда, когда обе договаривающиеся стороны вводят свои ключи, тем самым соглашаясь на заключение контракта. Вся программная логика смарт-контракта записывается и находится в блоке, который является программным контейнером, который объединяет все сообщения, относящиеся к конкретному смарт-контракту. Сообщения могут выполнять роль входов и выходов программного кода смарт-контракта и приводить к каким-либо действиям в реальном или цифровом мире за пределами блока блокчейн [4]. Применимости обширны: различного рода сделки в сфере поставок продукции, выплаты, оборот документов, оплата услуг ЖКХ и другое.

По мимо этого блокчейн используется для подтверждения и сохранения авторства художников такими ресурсами как Ascribe и Bitproof.

Существует платформы управления идентификацией на базе блокчейн, услуги которых направлены на решение проблемы кражи личных сведений клиентов.

Начинают применяться и платформы для интернета вещей, нацеленные на улучшение потребительского опыта.

В Российской федерации данная технология рассматривается как возможный инструмент в государственном управлении. Потенциал применимости в здравоохранении, голосовании, учете и документообороте выводит перспективы развития данной технологии в нашей стране на высокий уровень.

Список используемых источников

1. Мелани Свон. Блокчейн: Схема новой экономики: пер. с англ. М. : Олимп-Бизнес, 2017. 240 с.

2. Андреас Антопопулос. Овладение Биткоином: пер. с англ. М. : Олимп-Бизнес, 2017. 293 с.

3. Коржик В., Яковлев В. Основы криптографии: учебное пособие. СПб. : Интермедия, 2016. 295 с. ISBN 978-5-89160-097-3.

4. Савельев А. И. Договорное право 2.0. «умные» контракты как начало конца классического договорного права // Вестник гражданского права. 2016. N 3. С. 32–60.

УДК 004.056.5

ВОПРОСЫ ФОРМИРОВАНИЯ БЕЗОПАСНОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ НА ОСНОВЕ ТЕХНОЛОГИИ ДЕЦЕНТРАЛИЗОВАННЫХ СЕТЕЙ

Л. А. Виткова, Е. И. Денисов, Д. В. Сахаров, И. А. Ушаков

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

В статье рассматриваются вопросы формирования безопасной информационной системы на основе технологии децентрализованных сетей, включая анализ публичной и частной модели сети, решение вопросов уязвимости элементов информационной системы, основанной по принципу одноранговой сети, подходы к реализации проблемы посредством существующих концептов блокчейн, сравнительный анализ распространенных реализаций формирования блокчейн-цепей на основе распространенных на рынке решений. В ходе работы были выявлены недостатки и преимущества различных реализаций, выявлены необходимые качества информационных систем на основе децентрализованных сетей.

информационная безопасность, децентрализованные сети, одноранговые сети, блокчейн.

Распределенный реестр, построенный на децентрализованной сети, это база данных, которая может быть распределена по сети разнообразных сайтов, в разных географических зонах или организациях. Любые изменения в базе данных отражаются во всех копиях в течение короткого промежутка времени, который условно можно назвать «мгновенно». Информация, содержащаяся в реестре, может быть финансовыми, юридическими, физическими или электронными данными. Безопасность и достоверность хранимых в реестре активов достигается криптографическими методами, которые разграничивают права доступа участников сети.

Таким образом, возможно построить децентрализованную базу данных, с требованием доступности и модифицируемости всеми участвующими в сети узлами. Также, она должна быть согласованной, то есть все узлы видят абсолютно одинаковую версию базы, доступной – узлы могут производить запись и чтение из нее в любой момент времени, и устойчивой к разделению.

В случае, если один узел становится неработоспособным, это никак не отражается на базе данных. В большей мере таким высоким запросам отвечает распределённая база данных на основе технологии блокчейн.

Блокчейн предоставляет возможность безопасно обрабатывать и/или распространять данные между лицами через недовереную сеть. В качестве данных может быть в том числе и информация, требующая наличия третьей доверенной стороны.

Блокчейн опирается на следующие три понятия: одноранговые сети, распределенный консенсус, основой которого является решение математической задачи и асимметричная криптография [1].

В свою очередь, в распределённых сетях выделяют ранг публичных блокчейнов. В такой сети нет единого центра, который бы управлял процессами и на который абсолютно точно проводились бы атаки злоумышленников, чем достигается общая устойчивость сети к атакам. Однако, отсутствие координационного центра лишает возможности вносить изменения в сеть, решать проблемы, требующие непосредственного вмешательства человека в процесс. Поэтому наряду с публичными существуют и приватные блокчейны.

Приватные блокчейны – это блокчейны, создание блоков в которых централизовано, а все права на проведение операций принадлежат одной организации. Большинство узлов сети может только читать информацию – проводить аудит, а управлением базами и другими приложениями занимаются только доверенные узлы.

При этом приватные блокчейны имеют определенные преимущества. Во-первых, это низкая стоимость транзакций – групп последовательных операций с базой данных, которые представляет собой логическую единицу работы с данными. Это достигается тем, что проверка их валидности проводится доверенными и высокопроизводительными узлами вместо десятков тысяч пользовательских устройств, как в случае с общедоступными сетями.

Для того, чтобы добавить блок в цепочку блокчейн, узлу необходимо решить определенные вычислительные задачи, которые существенно усложняют возможность контроля со стороны одного узла. Такой концепт получил название "Proof of Work", что буквально означает «доказательство работы». Он предполагает, что некоторый узел способен проверить, что узел, который добавляет новый блок в блокчейн, действительно выполнил расчеты.

Процесс, посредством которого в сети достигается консенсус специально создан так, чтобы занимать некоторое время для того, чтобы создание нового разветвления, называемого также «развилка» или «форк», стало невыгодным с позиции затрат вычислительной мощности атакующего.

Выгоды, предлагаемые приватным блокчейном – это сравнительно быстрое подтверждение транзакций в сети и коммуникации, возможность исправлять ошибки и снимать подтвержденные транзакции, а также способность ограничивать доступ, тем самым уменьшать вероятность атаки извне.

Доказательство работы (ДР) является уязвимой частью в системе блокчейн перед атакой «двойного расходования», при которой пользователь осуществляет попытку повторной передачи одной и той же информации в децентрализованных системах информации.

ДР стало импульсом к возникновению специализированного оборудования. Это стало следствием того, что ресурсы, затрачиваемые на хеширование блоков блокчейна, очень велики и превышают мощности даже самых крупных суперкомпьютеров [2].

Используя задержки в сетевом соединении между дочерними узлами, атака вызывает «двойное расходование» в блокчейне, работающем на алгоритме ДР. В этой ситуации у атакующего появляется возможность использовать протокол GHOST (англ. "*Greedy Heaviest-Observed Sub-Tree*") и полностью заблокировать от остальных узлов одну из веток блокчейн. Ресурсы, необходимые для того, чтобы успешно провести вышеописанную балансатаку – иметь в расположении как минимум 20 минут и как минимум 5 % хеша сети [3].

В процессе работы, узлы обмениваются, так называемыми, «токенами» (определенными значениями, связанными с транзакционными выходами и входами), которые создают блокчейн-баланс узла получателя. Это послужило идеей использовать «стейк» (“*stake*” или доля) – то есть некоторое значение, зафиксированное на транзакционных выходах, которое

является ресурсом, который в свою очередь определяет право узла на генерирование следующего блока. Основой подхода "proof of stake" («доказательство доли», ДД) служит тот факт, что узлы также вычисляют хеш данных в поисках наименьшего определенного значения, но распределение степени сложности в конкретном случае происходит пропорционально и находится в соответствии с балансом этого узла или в соответствии с числом монет (токенов) на счету.

Операторы формируют блоки по очереди через заданные временные интервалы. Порядок создания блоков или фиксирован, или перемешивается после полного цикла – некоторого количества обработанных блоков. По сути, ДР переводит доверие к блокчейну из субъективного (доверие к системе эквивалентно доверию к контролирующей его организации) к объективному (доверие к системе вытекает из математических законов и гарантированно высокой экономической стоимости атаки на систему, которая не зависит от личности атакующего) [4].

Если некоторые узлы неактивны или периодически активны, необходимо, чтобы сеть оставалась структурированной для работы, что нужно для достижения консенсуса относительно произведенных подтверждённых транзакций и для верификации новых без нерабочих узлов. В дополнение к этому, она должна быть способна быстро вернуть узлы на необходимую скорость в случае их повторного подключения [5].

Для нарушения работы информационной системы (ИС) атакующий также может воспользоваться уязвимостью Nothing-at-Stake или пустой стек, чтобы построить свой вариант развилки цепи блокчейн. Кроме того, атакующий может заручится поддержкой других узлов, поскольку они также не осуществляют расходование ресурсов. Посредством форка атакующий может блокировать определенные транзакции и производить атаки «двойного расходования» [6].

Проблема пустого стека проявляет себя на всех векторах возможных атак на ДД-системы. Условно, атаки можно разделить на следующие две категории: дальние и ближние. В ситуации с ближними атаками осуществляется замена большинства созданных последних блоков, а при дальней атаке атакующий пытается заменить всю сформированную историю сети. Цель – дойти до базового первого блока или генезис-блока.

В случае ближней атаки, атакующий пытается вычислить ответвление большинства последних блоков и начинает с того блока, который им предшествует. Основной целью таких действий является построение цепочки блоков длиннее существующей цепи на данный момент.

В случае дальней атаки, атакующий пытается заменить всю историю транзакций. Поскольку вычислительные усилия для ДД-систем меньше, в теории он может начать со старого блока и расположить транзакции таким

образом, что будет в состоянии создать более длинный, чем существующий, блокчейн.

Резюмируя вышеописанное, необходимо описать преимущества, которыми достигаются построение ИС на технологии блокчейн.

Блокчейн не только хранит конечное состояние, но и хранит все предыдущие состояния. Каждый может проверить правильность конечного состояния, пересчитывая факты с самого начала.

К фактам в блокчейне однозначно можно относится с доверием, так как они технически подтверждаются консенсусом, даже если в сети находятся злоумышленники.

Помещение данных в блокчейн достаточно медленная операция, поскольку она требует достижения распределенного консенсуса.

В целом, вне зависимости от классификации, отличаются блокчейны уровнем доступа к реестру с информацией и кругом допустимых участников: активных участников – тех, кто имеет право одобрять транзакции и, таким образом, изменять состояние реестра и для пассивных – тех, кто может просто просматривать реестр и отслеживать изменения в нем.

Степень структурированности хранилища должна быть способна сохранять внутреннюю структуру содержащихся в ней данных, с целью предоставления возможности приложениям связывать записи между собой [7].

Важно, чтобы БД позволяла осуществлять удаление данных. По причине постоянного роста объема данных и постепенного устаревания информации.

Необходимо также определить требования к хранилищу данных, которое будет непосредственно обеспечивать блокчейн-систему. Распределённость необходима по причине того, что вся инфраструктура блокчейна распределенная, следовательно, хранилище данных также не может быть сконцентрировано в каком-либо центре.

Требование публичности также является следствием того, что блокчейн подразумевает расширение вычислительных мощностей общей сети за счет свободного присоединения всех желающих добавить свое оборудование в сеть. Поддержку этого необходимо реализовать и в базе данных. Необходима гибкая система масштабирования БД

В то время, как риски разработки финансового рынка или другой инфраструктуры на публичном блокчейне могут поставить нового пользователя перед выбором, частные блокчейны предлагают уровень контроля как над поведением участника, так и над процессом подтверждения транзакции. Использование системы, основанной на блокчейне, является признаком прозрачности и удобства такой системы, что подкрепляется принципом безопасности системы. Заинтересованные организации оставляют за собой решение, где лучше расположить системы – на более безопасной частной сети

или в общедоступном Интернете. Своё применение находят оба вида блокчейнов: где требуется быстрота транзакции, возможность её отменить, и централизованный контроль за её подтверждением, лучше подойдут приватные блокчейны; там, где важнее широкая вовлеченность масс, прозрачность и подтверждение третьими сторонами, будут использоваться публичные блокчейны.

Список используемых источников

1. Равал С. Децентрализованные приложения. Технология Blockchain в действии, СПб. : Питер, 2017. 240 с.: ил. ISBN 978-5-496-02988-9.
2. Форк А. Bitcoin. Больше чем деньги. Тверь : Тверская областная типография, 2014. 280 с. ISBN: 978-5-87049-836-2
3. Natoli C. Gramoli V. The Blockchain Anomaly. University of Sydney, 2016.
4. Дешевых Е.А., Конюхов В.М., Крылов К.Ю., Ушаков И.А. Исследование методов защиты от инсайдерских атак // Актуальные проблемы инфотелекоммуникаций в науке и образовании. IV Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 2 т. 2015. С. 310–313.
5. Никитин В. Н., Юркин Д. В. Влияние механизмов защиты на пропускную способность каналов с ошибками // Защита информации. Инсайд. 2009. № 3 (27). С. 46–51.
6. Атака double-spending в системе Bitcoin [Электронный ресурс]. URL: https://bits.media/double-spending/
7. Головчинер М. Н. Базы данных: лекции. Томск, 2009. 129 с.

УДК 004.056

ОБЗОР АКТУАЛЬНЫХ УГРОЗ И МЕТОДОВ ЗАЩИТЫ В СФЕРЕ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ

Л. А. Виткова, А. И. Иванов

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

Виртуальная инфраструктура – отличный инструмент для быстрого и гибкого масштабирования ИТ-систем, воплощения экспериментальных разработок и экономии в целом. При грамотном подходе она позволяет экономить время и инвестировать его в корневые задачи. Но, также стоит учесть, что переход в облако влечёт множество рисков для конфиденциальной информации, хранимой в информационной системе. Перед миграцией необходимо взвесить все достоинства и недостатки, возможные потери в случае нарушения периметра безопасности и разработать наиболее эффективные методы защиты.

облачные технологии, угрозы, информационная безопасность, методы защиты.

Облачные технологии обеспечивают повсеместную доступность данных посредством сети Интернет, это приводит к тому, что информация ограниченного доступа хранится и обрабатывается в разных точках разных инфраструктур. Необходимость в беспрерывном доступе к данным из любой точки земли, гибкой инфраструктуре, позволяющей организовать рабочий процесс удалённо, и прогресс в сфере телекоммуникаций и распределенных вычислений привели к достаточно серьезному изменению ландшафта вычислительных технологий. Почти все современные ЦОД базируются на гибридной инфраструктуре, которая состоит из виртуальных, физических и облачных развертываний, которые могут быть размещены как локально, так и удалённо.

Хранение информации конфиденциального характера в ЦОД, нуждается в особом подходе к организации защищенности системы. Защита должна состоять из средств защиты сети, обеспечения отказоустойчивости, физической защиты и защиты от вредоносного ПО. Внедрение облачных технологий в информационные системы, где производится обработка информации ограниченного доступа накладывает определенные законодательные обязательства в сфере обеспечения защиты информации [1].

Немаловажную роль играет защита системы контроля и управления облаком, неконтролируемые виртуальные машины и процессы могут представлять опасность для облака. Для этого требуется грамотно выстроить систему защиты, основываясь на модели управления рисками облачных инфраструктур.

Физическая безопасность должна быть основана на организации контроля доступа к серверам. Для обеспечения сетевой безопасности необходимо составить модель угроз, которая будет базироваться на разграничении сетей межсетевым экраном, системе предотвращения вторжений и других инструментах. Более того, в некоторых случаях необходимо обеспечение сертифицированного шифрования на этапе передачи информации от клиента к серверу.

Возникновение новых угроз неизбежно, потому что доступ к управлению облачным сервисом осуществляется через Интернет, в отличие от традиционных ЦОД. Для минимизации угроз на уровне системы необходимо разграничить контроль доступа, а также обеспечить прозрачность изменений [2].

Динамичность виртуальных машин может стать дополнительной проблемой при организации безопасности. Создание, остановка и перезапуск виртуальных машин производятся за короткое время. Виртуальные машины могут быть клонированы, перемещены между физическими серверами. Как следствие, возникает высокая изменчивость, которая создаёт дополнительные трудности в планировании системы защиты. Особое внимание сле-

дует уделить уязвимостям операционной системы и приложений, распространение которых невозможно проконтролировать. На состояние защищенности облачной системы не должно влиять её местоположение или её состояние.

Локальные и облачные серверы основаны на использовании практически идентичных операционных систем, и приложений. Облачные системы подвержены удалённому взлому и заражениям. Не следует забывать и о рисках для виртуальных систем. Вредоносная активность должна обнаруживаться системами предотвращения вторжений на уровне виртуальных машин, вне зависимости от их расположения в облачной среде.

Для защиты виртуальных машин необходимо обеспечить защиту на уровне гипервизора, так как выключенная виртуальная машина не может противостоять вирусной атаке. Основным путём атак является сеть, для заражения виртуальной машины достаточно сетевого доступа к хранилищу образов.

Использование облачных вычислений приводит к сглаживанию или полному исчезновению границ сети, что негативно отражается на уровне общей защиты. Как следствие, защита наименее защищенной части сети определяет общий уровень защищенности. Для устранения такого явления необходимо периметр сетевой безопасности сдвинуть до границ виртуальной машины. Следует отметить, что корпоративный межсетевой экран никак не влияет на серверы, размещенные в облаке [3].

Исходя из представленных угроз можно выделить несколько векторов защиты.

Шифрование – один из самых эффективных способов зашиты информации. Провайдер облачных услуг должен обеспечивать шифрование хранимой информации.

Разграничение пользователей – рекомендуется использовать собственные виртуальные машины и различные виртуальные сети, применение технологий VPN, VLAN и т. д. для развертывания виртуальных сетей.

Аутентификация – для повышения уровня защиты рекомендуется использование токенов и сертификатов.

Защищенный канал передачи – нужен для обеспечения неизменности данных при передаче через слабозащищенные узлы и защиты их от чтения злоумышленником, можно использовать различные алгоритмы шифрования.

В заключение следует отметить, что, несмотря на то что переход к облачной инфраструктуре несёт в себе определенные риски для обрабатываемой информации, эти риски не превышают тех, которые возникают при хостинге услуг внутри организации. Основным фактором, на который стоит обратить внимание - возникновение нового поля для атак, так как каналом

передачи данных будет сеть Интернет, и клиентские станции, которые могут быть так же подвержены заражению [4].

Список используемых источников

1. Риз Д. Облачные вычисления: пер. с англ. СПб. : БХВ-Петербург, 2011. 288 с.
2. Рекомендации по выбору и использованию облачных услуг [Электронный ресурс]. URL: https://www.intuit.ru/studies/courses/12160/1166/lecture/19345 (дата обращения 25.01.2018).
3. Маньшин Г. Г., Артамонов В. А., Артамонова Е. В. Парадигма безопасности облачных вычислений. [Электронный ресурс]. URL: http://itzashita.ru/oblachnyie-vyichisleniya/paradigma-bezopasnosti-oblachnyih-vyichisleniy.html (дата обращения 25.01.2018).
4. Облачные вычисления, «дырявые» облака и способы защиты данных [Электронный ресурс]. URL: http://4by4.ru/ru/analytics/oblachnye-vychisleniya-dyryavye-oblaka-i-sposoby-zashchity-dannyh (дата обращения: 25.01.2018).

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

УДК 004.056

СРАВНЕНИЕ МЕХАНИЗМОВ ПРОВЕРКИ СТАТУСА ЦИФРОВОГО СЕРТИФИКАТА X.509 В УЦ НА БАЗЕ ОС «ASTRA LINUX»

Л. А. Виткова, А. С. Исаков, М. М. Ковцур

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

Операционные системы семейства Windows широко используются для организации аккредитованных Удостоверяющих центров в Российской Федерации. Однако, одной из современных тенденций является импортозамещение, как в части аппаратного, так и программного обеспечения. Так, одной из актуальных задач для Министерства Обороны РФ является полный переход на ОС LINUX и на аппаратное обеспечение отечественной разработки. Однако, развертывание Удостоверяющих центров на базе операционных систем Linux Российского производства и существующие особенности взаимодействия УЦ описаны недостаточно в современной литературе. В данной статье описаны механизмы проверки статуса сертификата: Certificate Revocation List и Online Certificate Status Protocol, а также представлена реализация на базе УЦ на ОС Astra Linux.

инфраструктура открытых ключей, удостоверяющий центр, сертификат, CRL, OCSP.

Основной вопрос, связанный с использованием средств электронной цифровой подписи, к которым предъявляются требования по высокой отказоустойчивости, заключается в повышенных мерах обеспечения информационной безопасности при доверии к службам доверенной третьей стороны международного информационного обмена.

Как известно, все операционные системы отечественного производства семейства Astra Linux базируются на открытых кодах ОС типа Linux и прошли оценку соответствия согласно федеральному законодательству Российской Федерации. Поэтому наиболее актуален вопрос сравнения механизмов проверки статуса сертификата открытого ключа (МПСС) на базе удостоверяющих центров (УЦ) развёрнутого в среде именно Astra Linux.

Для реализации этой задачи необходимо дать характеристику существующим механизмам проверки статуса сертификата открытого ключа (МПСС) (рис. 1) [1, 2], определить критерии сравнения МПСС, развернуть УЦ с поддержкой МПСС, проверить функциональность развёрнутого УЦ в части работы МПСС.

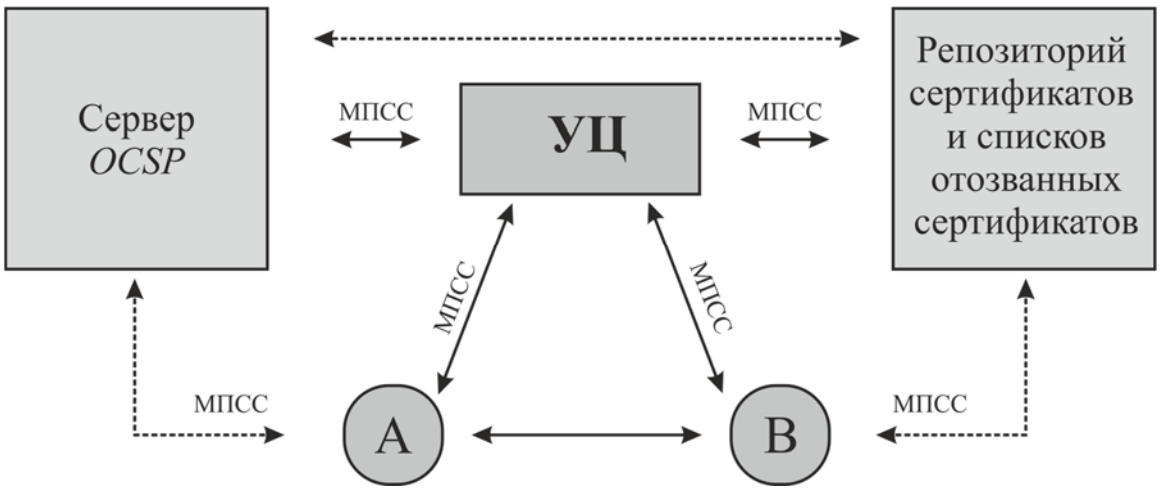


Рис. 1. Механизмы проверки статуса сертификата открытого ключа

В рамках данной статьи рассматриваются следующие МПСС:

CRL – Certificate Revocation List, представляет собой список, содержащий метку времени и идентифицирующий отозванные сертификаты, который подписывается УЦ или издателем CRL, а также помещается в открытый репозиторий для публичного доступа. При взаимодействии между собой – пользователи сначала обращаются в УЦ, а в дальнейшем напрямую к репозиторию, для получения информации о состоянии сертификата открытого ключа виде CRL с информацией о каждом отозванном сертификате (рис. 1).

OCSP – Online Certificate Status Protocol обслуживает пользователей в режиме реального времени и занимается проверкой статуса аннулирования цифрового сертификата. OCSP может использоваться для удовлетворе-

ния некоторых эксплуатационных требований предоставления более своевременной информации об отзыве, чем это возможно в CRL, а также может использоваться для получения дополнительной информации о состоянии сертификата открытого ключа. Пользователь OCSP, делает запрос о статусе сертификата открытого ключа серверу OCSP и, до прихода ответа, приостанавливает обработку соответствующих сертификатов, пока OCSP сервер не даст ответ (рис. 2).

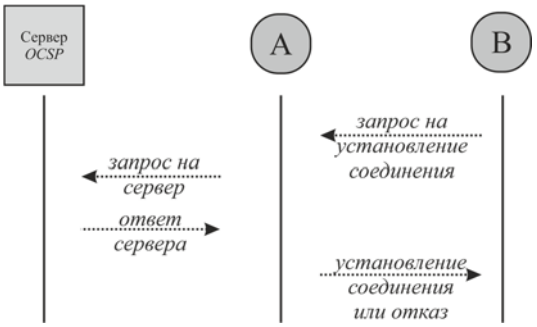


Рис. 2. Механизм работы МПСС OCSP

Для того чтобы сравнить между собой данные МПСС, введём следующие критерии:

– оперативность получения статуса сертификата;

– предоставление дополнительной информации о состоянии сертификата – подробное описание состояния сертификата на момент запроса;

– возможность получения информации о промежуточных УЦ – получение информации обо всёх объектах тракта сертификации;

– зависимость работоспособности МПСС от расширения TLS – возможность вкладывать дополнительную информацию для более информативного и полного вида тракта сертификатов с использованием дополнительных расширений;

– зависимость от доступности репозитория – необходимость для работы МПСС выполнить запросы к репозиторию для проверки статуса сертификатов открытых ключей.

Исходя из таблицы следует, что с ростом инфраструктуры PKI рекомендуется использовать OCSP, а в малых и средних инфраструктурах целесообразно придерживаться CRL (рис. 3).

ТАБЛИЦА. Сравнение МПСС CRL и OCSP

	CRL	OCSP
Оперативность получения статуса сертификата	Низкое	Высокое
Предоставление дополнительной информации о состоянии сертификата	Низкое	Высокое
Информация о промежуточных УЦ	Имеется	Опционально
Зависимость работоспособности расширения TLS	Отсутствует	Опционально
Зависимость от доступности репозитория	Имеется	Отсутствует

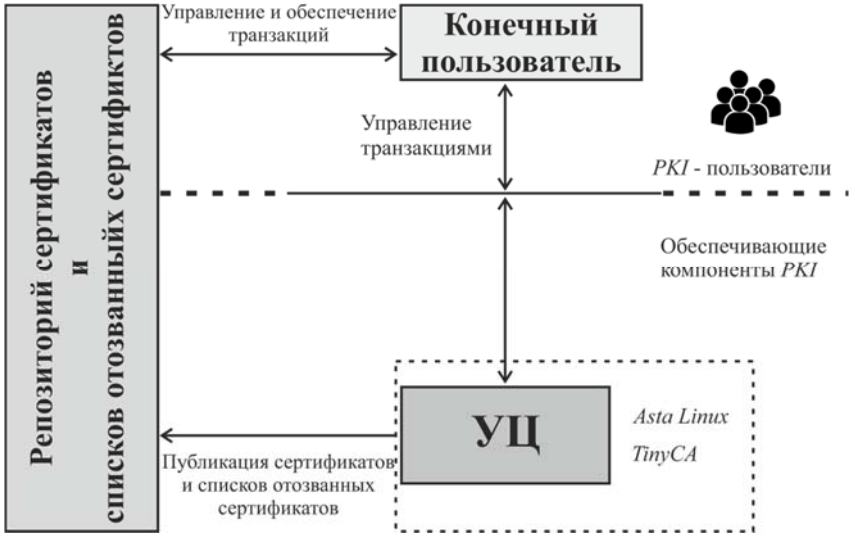


Рис. 3. Инфраструктура открытых ключей на базе ОС Astra Linux

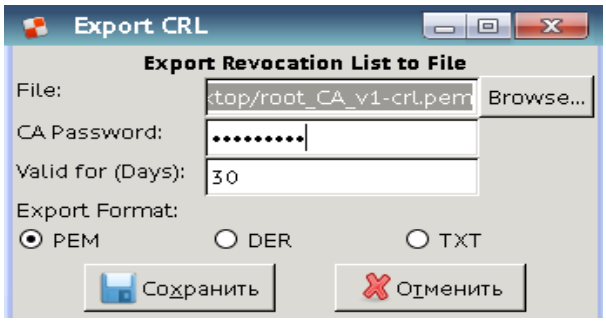


Рис. 4. Экспорт CRL в TinyCA

Далее представлен пример развёртывания CRL. Для создания CRL сертификата открытого ключа используется развёрнутый УЦ на ПО TinyCA. В ПО на графическом интерфейсе необходимо выбрать икону экспорта CRL, далее выбрать каталог и формат файла для экспорта (рис. 4). После выпуска CRL сертификат импортируется в хранилище сертификатов – репозиторий.

Как видно из рис. 5, выпущенный сертификат CRL сформирован путем подписания на секретном ключе УЦ TinyCA, который содержит информацию об отозванных сертификатах, в соответствии с требованиями стандарта X.509 [3].

```
Certificate Revocation List (CRL):
        Version 2 (0x1)
    Signature Algorithm: sha1WithRSAEncryption
        Issuer: /C=RU/ST=SPb/L=SPb/O=SUT/OU=ZSS/CN=CA
        Last Update: May 19 16:12:09 2017 GMT
        Next Update: Jun 18 16:12:09 2017 GMT
Revoked Certificates:
    Serial Number: 01
        Revocation Date: May 19 16:10:37 2017 GMT
        CRL entry extensions:
            X509v3 CRL Reason Code:
                Key Compromise
    Signature Algorithm: sha1WithRSAEncryption
         2f:bd:3d:0d:ae:20:a3:7a:7a:68:4f:2c:35:4f:24:37:ea:d8:
         d3:3f:7a:dc:1f:c0:2e:ee:58:03:a4:60:ed:a7:5f:5f:f3:ef:
```

Рис. 5. Демонстрация подписанного сертификата CRL УЦ на базе TinyCA

В заключение стоит отметить, что TinyCA позволяет выпускать сертификаты и списки отозванных сертификатов, соответствующие стандарту X.509, открытые ключи, ЭЦП, обрабатывать запросы на сертификаты, формировать базы открытых ключей и списки отозванных сертификатов механизмом CRL.

Список используемых источников

1. RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.
2. RFC 2560: X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP.
3. Recommendation ITU-T X.509 | ISO/IEC 9594-8 defines frameworks for public-key certificates and attribute certificates.

УДК 004.056

ИСПОЛЬЗОВАНИЕ BIG DATA В ПРОЦЕССАХ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИОННОЙ СФЕРЫ

Л. А. Виткова, Р. А. Мустафаев, Д. В. Сахаров, И. И. Хомин

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

Влияние информации на развитие общества велико. В случае ее отсутствия, человечество оставалось бы в стадии первобытного строя. Коммуникацию считают необходимым параметром жизнедеятельности человека и фундаментальной основой существования общества в целом. Процесс обмена информацией вышел за узкие рамки межличностного общения и перешел в разряд массовой связи со всем миром. В эпоху информационных технологий, особенно после бума социальных сетей, по каждому пользователю интернета стало накапливаться значительное количество информации, что в конечном счете дало развитие направлению Big Data. Большие Данные, на сегодняшний момент, являются одним из ключевых драйверов развития информационных технологий.

Big Data, безопасность информационной среды, диагностика и мониторинг, сети.

Мы живем в эпоху информационных технологий. Трудно оценить какое количество информации хранится на сотнях тысяч серверов по всему миру и тем более создаваемой ежедневно. Появление в мире первых соци-

альных сетей, изменило отношение к интернет ресурсам, их созданию и изменению. Резкий рост количества участников социальных сетей, таких как Facebook, Вконтакте, Twitter, Google+, а также других блогов и веб порталов, стал результатом генерации огромного количества данных ежечасно. Для лучшего представления о том откуда берется всё-таки это бескрайнее море данных приведу пару примеров:

1. На начало 2018 г. в крупнейшей социальной сети Вконтакте среднесуточная аудитория составляет более 80 миллионов посетителей, а всего зарегистрировано на начало 2018 г. приблизительно 430 миллионов пользователей.

2. Один из популярных ресурсов для получения информации «Русская Википедия» хранит в себе по состоянию на февраль 2018 г. практически 1,5 миллиона статей различной тематики, а ее старший брат «Английская Википедия» уже перешагнул за 5,5 миллиона статей.

3. Ежедневно сайт Instagram.com посещают около 900 тысяч пользователей, которые выкладывают приблизительно 2 миллиона фотографий и историй.

С каждым днём появляется всё больше и больше информации и информационных ресурсов. Этому хорошо способствует развитие научно-технического прогресса и средств связи. Информация, которая становится доступной, должна быть как-то «оптимизирована», для этого существует множество способов и подходов и каждый из них необходим для решения своего «узкого» спектра задач. Исходя из этого мы приходим к тому что должны использовать системы обработки данных Big Data или по-простому «Больших Данных».

Big Data представляет собой группу технологий и методов, при помощи которых мы можем обрабатывать огромное количество сведений – как структурированных, так и неструктурированных для получения качественно новых знаний об информационном мире, который нас окружает. Для получения полноценного восприятия, что же все такое Большие Данные мы разберем самые важные направления и задачи, которые они решают. Концепция «Больших Данных» предусматривает решение задач в трех главных направлениях:

1. Хранение и управление массивами информации исчисляемых в сотнях терабайт или петабайт, которые обычные реляционные базы данных не позволяют эффективно использовать.

2. Организация неупорядоченных наборов сведений, состоящих из различных документов, изображений, аудио, видео и других типов файлов.

3. Обработка имеющегося массива информации, с целью формирования способов работы с неструктурированной информацией и составлению аналитических отчетов, а также внедрения(составления) прогностических моделей.

В нашем случае, обеспечение безопасности информационной сферы, нам интересен как раз-таки 3 аспект. Ведь в нашей жизни технологии заняли такую большую долю, что прогнозирование поведения людей либо же сбор статистики уже не доставляет больших проблем. Для анализа поведения используются различные системы мониторинга инфокоммуникационного пространства. Мониторинг являет собой получение и структурирование первичных данных. Как раз для этого используются, так называемые, Большие Данные (*Big Data*): сообщения, межпользовательские связи, ссылки на внешние ресурсы – все это собирается для дальнейшего анализа. Возможности конкретной системы определяются размером полученной информации и режимом ее обработки. Анализ подразумевает несколько этапов обработки первичных данных:

1. Вычисление базовых показателей, которые позволяют отвечать на простые количественные запросы типа «сколько сообщений написал пользователь?».

2. Выявления статистических и структурных закономерностей в данных дает понимание природы исследуемой сети. Например, типы распределений, к которым относятся обслуживания тех или иных систем.

В нашем контексте мы рассматриваем Big Data как набор инструментов для обеспечения безопасности информационной сферы нас интересуют возможные задачи, решение которых может понадобиться органам государственной власти. Например, поиск информация, содержащей контент, запрещенный по законодательству (экстремистская деятельность, детская порнография, информация об изготовлении или получении наркотиков, психотропных веществ и их прекурсоров, подталкивание на совершение суицида и прочие ресурсы, нарушающие Российское или международное законодательства). Поэтому государственным органам нужно контролировать этот поток информации. Для этого нам необходимо обработать и проанализировать большое количество данных, а также составить аналитические отчеты.

На сегодняшний день сфера Big Data активно задействована в зарубежных компаниях. Такие компании, как Nasdaq, Coca Cola, Netflix, Starbucks, Facebook, VISA, Google, Master Card, IBM, Bank of America, HSBC и AT&T уже используют ресурсы Больших Данных. Сферы применения данной технологии обработки информации разнообразны и варьируются в зависимости от отрасли и задач, которые ставятся для выполнения. Одни из самых явных примеров можно привести без труда:

1. HSBC использует технологии Больших Данных для предотвращения мошеннических операций с пластиковыми картами. С помощью технологии Big Data компания увеличила эффективность службы безопасности в 3 раза, распознавание мошеннических инцидентов – в 10 раз. Экономический эффект от внедрения данных технологий превысил 10 млн долл. США.

2. Антифрод компании VISA позволяет в автоматическом режиме вычислить операции сомнительного характера. По оценкам самой компании, система на данный момент помогает предотвратить мошеннические платежи на сумму 2 млрд долларов США ежегодно.

На сегодняшний день в России данное направление развито недостаточно хорошо. Причиной является недостаточная популяризация за счет трудности внедрения, затрат в финансовом плане, а также нехватка специалистов в данной сфере. Но даже несмотря на это рынок развивается. Вот несколько примеров:

1. Компания Яндекс задействовала Big Data в своих интересах. Она создала международное подразделения Yandex Data Factory, на анализе которой построено большинство таких продуктов «Яндекса» как – поиск, предсказание пробок, машинный перевод, распознавание образов и речи, фильтрация спама, рекламный таргетинг. С тех пор отечественный IT-гигант делал проекты для таких знаменитых нефтяных компаний как Роснефть и норвежской Statoil.

2. Сбербанк сейчас использует Big Data для расчета управления рисками, борьбы с мошеннической деятельностью, сегментации и оценки кредитоспособности клиентов, управления персоналом, прогнозирования загруженности в отделениях, для расчета бонусной системы своих сотрудников и других задач.

3. Газпромбанк применяет Big Data для скоринга, противодействия мошенникам, оперативного получения отчетности, персонализации предложений, доскоринговой проверки репутации потенциальных заемщиков, предоставления информации регуляторам и других задач.

Сегодня существует множество реализаций данного подхода [1, 2, 3, 4]. Самые популярные это Apache Spark [5] и Hadoop. Одним из самых популярных решений в отрасли «Больших Данных» является модель распределённых вычислений MapReduce [6, 7], предложенная компанией Google для обработки больших объёмов данных на компьютерных кластерах.

Схема данных вычисленный выглядит следующим образом (рис.).

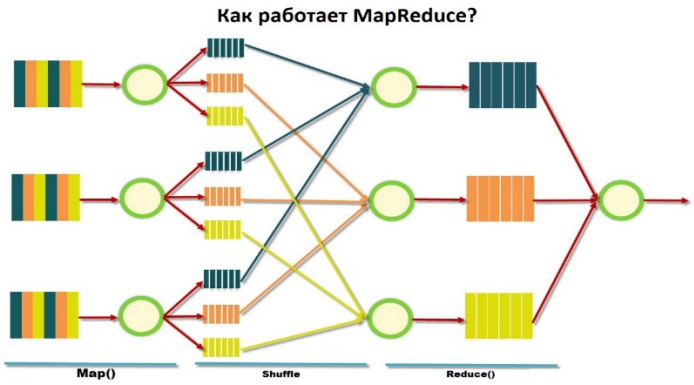


Рисунок. Схема вычислений MapReduce

MapReduce предполагает, что данные организованы в виде некоторых записей. Обработка данных происходит в 3 стадии:

1. Стадия Map. На этой стадии данные пред обрабатываются при помощи функции map(), которую задает пользователь. Работа этой стадии заключается в предобработке и фильтрации данных. Пользовательская функция применяется к каждой входной записи. Функция map() примененная к одной входной записи и выдаёт множество пар ключ-значение. Множество – т. е. может выдать только одну запись, может не выдать ничего, а может выдать несколько пар ключ-значение. Что будет находится в ключе и в значении – решать пользователю, но ключ – очень важная вещь, т. к. данные с одним ключом в будущем попадут в один экземпляр функции reduce.

2. Стадия Shuffle. Проходит незаметно для пользователя. В этой стадии вывод функции map «разбирается по корзинам» – каждая корзина соответствует одному ключу вывода стадии map.

3. Стадия Reduce. Каждая «корзина» со значениями, сформированная на стадии shuffle, попадает на вход функции reduce(). Функция reduce задаётся пользователем и вычисляет финальный результат для отдельной «корзины». Множество всех значений, возвращённых функцией reduce(), является финальным результатом MapReduce-задачи.

Анализ Больших Данных в процессах обеспечения безопасности информационной сферы будет способствовать эффективному сбору данных и полномасштабной оценке состояния всей инфраструктуры. Пока же процесс обнаружения источников брешей и оценка последствий их появления с изучением огромных объемов данных самого разного характера может растянуться на несколько месяцев. Тем самым данное направление имеет огромный потенциал развития как информационной сфере, так и в других областях науки.

Список используемых источников

1. Страница проекта Apache Hadoop [Электронный ресурс]. URL: http://hadoop.apache.org/ (дата обращения 25.03.2018).

2. Страница проекта Cloudera CDH Apache Hadoop [Электронный ресурс]. URL: http://www.cloudera.com/content/cloudera/en/products-and-services/cdh.html (дата обращения 28.03.2018).

3. Страница проекта Infinispan [Электронный ресурс]. URL: http://infinispan.org/ (дата обращения 26.03.2018).

4. Страница проекта Basho Riak [Электронный ресурс]. URL: http://basho.com/riak/ (дата обращения 25.03.2018).

5. Страница проекта Apache Spark [Электронный ресурс]. URL: http://spark.apache.org/ (дата обращения 27.03.2018).

6. Chowdhury M., Zaharia M., Stoica I. Performance and Scalability of Broadcast in Spark, 2010.

7. Gu Lei, Huan Li. Memory or Time: Performance Evaluation for Iterative Operation on Hadoop and Spark // High Performance Computing and Communications & 2013 IEEE International Conference on Embedded and Ubiquitous Computing (HPCC_EUC), 2013 IEEE 10th International Conference on. IEEE, 2013.

УДК 004.056

ПРОБЛЕМЫ БЕЗОПАСНОСТИ ИНФОРМАЦИОННОЙ СФЕРЫ В УСЛОВИЯХ ИНФОРМАЦИОННОГО ПРОТИВОБОРСТВА

Л. А. Виткова[1], А. А. Проноза[2], Д. В. Сахаров[1], А. А. Чечулин[1]

[1]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
[2]Санкт-Петербургского института информатики и автоматизации Российской академии наук

Сегодня информационно-психологическая борьба сама по себе очень агрессивная, и эта борьба зачастую порождает локальные вооруженные конфликты и войны, цветные революции. Высокий уровень доверия социальным сетям позволяет противнику моделировать и создавать внутренние социальные конфликты, путем использования дезинформации, а также дает возможность противнику управлять массовым сознанием и мнением, влиять на деструктивные социальные процессы внутри общества.

информационно-психологическая борьба, социальные сети, информационное противоборство, информационная безопасность, BigData.

Развитие информационных технологий и появление глобальной сети Интернет, социальных сетей, средств массовых коммуникаций подводит научное сообщество к кардинальному пересмотру имевшихся представлений о способах ведения войны и мире. Не только в научных кругах, но и в средствах массовой информации обсуждается аспект, касающийся национальной безопасности, а именно информационно-психологическая безопасность и информационные войны. В стратегиях ведущих стран мира в число сфер ведения боевых действий помимо земли, моря, воздуха и космоса вошло информационное пространство.

Наибольшая острота этой проблемы проявляется при попытках распознавания целевых информационных воздействий (атак) на субъекты (индивидуальных или коллективных, например, на человека, семью, группу или организацию) и оказания противодействия таким атакам. Однако вопросы многоуровневого управления информационно-психологической безопасностью государства в условиях противодействия различным видам целевых информационно воздействий в условиях необходимости обработки

больших объемов гетерогенных данных в настоящее время в мире исследованы в недостаточной степени [1, 2].

Основными недостатками существующих систем управления информационным полем государства являются:

1) отсутствие комплексного и детального анализа угроз безопасности информационной сферы в условиях информационного противоборства в социальных сетях;

2) недостаточная полнота и адекватность существующих моделей оценки воздействия нарушителя на информационную сферу государства через социальные сети;

3) отсутствие полного формализованного представления процесса автоматизированной оценки обстановки в информационной сфере социальных сетей;

4) отсутствие адекватной формализации ситуационных параметров и процессов прогнозирования, обнаружения и оценки угроз вредоносного воздействия в информационном пространстве социальных сетей;

5) ориентация на мониторинг и блокировку каналов распространения вредоносной информации, а не на противодействие самому нарушителю;

6) недостаточная полнота и адекватность существующих моделей информационного противоборства для социальных сетей.

Этим обусловливается высокая актуальность тематики исследования.

Одной из основных задач на решение которой направлен предлагаемый подход является противодействие воздействию на информационное поле государства со стороны политических экстремистских организаций, реализующих свою внутреннюю программу действий с целью создания беспорядков и условий для проведения террористических акций. Такое информационное воздействие обычно осуществляется за счет распространения информации, направленной на формирование в сознании установок и (или) стереотипов поведения для к совершения каких-либо действий или к воздержанию от их совершения.

Стоит отметить, что террористические и преступные группировки также берут на вооружение средства информационного воздействия, создают медийные агентства и пишут стратегии, направленные на расширение сферы влияния и вовлечение новых адептов через Интернет. Так, например, известно, что ИГИЛ (запрещенная организация на территории Российской Федерации) среди иных террористических группировок выделяется не только своей военной и экономической мощью, но и весьма умелым ведением пропаганды с использованием средств массовой информации и социальных сетей [3, 4].

Именно поэтому, одной из составляющих обеспечения безопасности государства представляется мониторинг, анализ и активное управление безопасностью в информационном пространстве социальных сетей. Прежде

всего, процессы управления и контроля в информационном пространстве сводятся к непрерывному контролю параметров состояния защищаемой аудитории, ее оценке вовлеченности в информационные потоки, в прогнозировании и в своевременном определении (выявлении) фактов нарушений законодательства и предпосылок нарушения безопасности.

Несмотря на то, что законодательная база, как и механизм блокировки доменных имен и указателей страниц достигли определенных результатов (в частности, создан реестр запрещенных ресурсов Роскомнадзора, ведется мониторинг информационного пространства зарегистрированных СМИ и существуют отдельные коммерческие системы) для информационно-психологической безопасности государства научно-технические вопросы управления безопасностью остаются нерешенными.

Стоит отметить, что большинство научных работ университетов и научно-исследовательских институтов в области интеллектуального анализа данных остаются в плоскости пассивного наблюдения за обменом информации в социальных сетях или же выходят за рамки виртуальных сетей в другие области знаний, включая медицину, маркетинг и т. п. В то же время мировые исследовательские центры и коммерческие компании не предлагают конструктивного решения по повышению уровня защищенности информационного пространства государства. Во время кризисов социальные сети эффективно используются для манипуляции общественным сознанием, управлением реакцией на события.

Прежде всего, сегодня не существует построенных моделей нарушителя, методик определения актуальных угроз в информационном пространстве, нет определений логических границ информационного пространства. А блокировка ресурсов направлена на ресурсы и информационные объекты, а не на источник распространения информации, то есть противоборство сегодня ведется с информацией, а не с нарушителями. Во многом это объясняется тем, что большинство систем мониторинга являются коммерческими и создавались для управления и мониторинга торговыми марками. Поэтому, данные, полученные при помощи действующих методов и приложений, не позволяют разработать эффективную стратегию противоборства.

Предлагаемый авторами подход к управлению информационным пространством базируется на методе многоуровневого управления информационно-психологической безопасностью государства и на апостериорной защиты агента от вредоносного (информационного) воздействия, осуществляемой при допущении, что нарушитель уже оказал воздействие (или может оказывать воздействие) на субъект для достижения собственной цели. Одновременно с этим в основу подхода положены модели влияния в социальных сетях, информационного конфликта и информационного противоборства [5, 6].

Представленная в работе авторов проблема является достаточно актуальной и не имеющей полного решения в настоящее время. Решение этой проблемы должно быть связано с разработкой нового комплекса методов, методик и моделей. Разработанные комплексы будут относиться к новым фундаментальным, передовым и быстро развивающимся областям научного знания, таким как интеллектуальный анализ данных, технологии Больших данных (*Big Data*) и Грид-вычисления (*Grid computing*), обработка высокосвязных информационных объектов, и др. Этим определяется высокая научная значимость решения этой проблемы. В целом совокупность моделей, методов, методик и программных приложений позволят обосновать и разработать новую информационную технологию мониторинга и противодействия вредоносному влиянию в информационном пространстве социальных сетей. Следует отметить, что вопросы прототипирования предлагаемых решений в различных условиях функционирования, а также их всесторонней экспериментальной оценки занимают значительную часть в исследовании. Для одновременной обработки информационных объектов авторы предлагают использовать элементы технологий, предназначенных для работы с Большими данными [7, 8].

Кроме того, результаты исследования могут быть использованы для построения единого ситуационного центра мониторинга социальных сетей, что также подтверждает актуальность решаемой проблемы.

Конкретной задачей в рамках проблемы, на решение которой можеть быть направлено исследование, является разработка научно-методического обеспечения, включающего комплекс методов, методик, моделей, алгоритмов и программных прототипов, для реализации компонентов системы мониторинга и противодействия вредоносному влиянию в информационном пространстве социальных сетей.

В комплекс могут включаться взаимосвязанные методы и методики мониторинга, анализа и распознавания информационного вброса со стороны нарушителя. Алгоритмы обнаружения ретрансляторов, каналов распространения источника, уточнения характеристик вредоносных информационных объектов, оценки нарушений законодательства в информационном пространстве, оценки атакуемой аудитории и выработки рекомендаций по возможным контрмерам. Разработка новых методов и методик распознавание позволит защитить атакуемую аудиторию, в том числе оказать противодействие идеологическому экстремизму в информационном пространстве социальных сетей.

Резюмируя вышесказанное, авторы делают выводы о том, что в настоящее время средства, реализующие технологии Больших данных, предоставляют возможность дальнейшего совершенствования аналитической обработки информации безопасности путем корреляции, консолидации

и контекстуализации разнообразных источников данных для более длительных периодов времени. В частности, авторы предполагают использовать алгоритмы разбиения графов, как например алгоритм Кернингана-Лина и Balanced Label Propagation [9]. Многоуровневая оптимизация позволит работать с более крупными частями графа путем стягивания ребер в вершины. Разбиение вершин на группы позволит производить первоначальные вычисления на каждом вычислительном узле, и предоставит возможность избежать существенной деградации производительности системы. Одновременно с этим построение графов взаимосвязей объектов в социальных сетях позволит вычислять ретрансляторы, источники, что в дальнейшем итоге и даст возможность для блокировки нарушителя. Анализ вектора атаки, объекта воздействия и целевой аудитории, с которой работает нарушитель, позволяет выработать эффективные контрмеры [10].

Список используемых источников

1. Губанов Д. А., Новиков Д. А., Чхартишвили А. Г. Социальные сети: модели информационного влияния, управления и противоборства. М.: Изд-во физ.-мат. лит-ры, 2010. 228 с.

2. Губанов Д. А., Новиков Д. А., Чхартишвили А. Г. Модели репутации и информационного управления в социальных сетях // Математическая теория игр и ее приложения. Управление большими системами. 2009. № 26.1.

3. Dong Y., Ding Z., Mart´ınez L., and Herrera F. Managing consensus based on leadership in opinion dynamics // Information Sciences, 397:187–205, 2017.

4. Ferrara E. Manipulation and abuse on social media. ACM SIGWEB Newsletter, (Spring):4, 2015.

5. Цыганов В. В., Бухарин С. Н. Информационные войны в бизнесе и политике : теория и методология. М. : Академический Проект, 2007. 336 с.

6. Расторгуев С. П., Литвиненко М. В. Информационные операции в сети Интернет / Под общ. ред. А. Б. Михайловского. М. : АНО ЦСОиП, 2014. 128 с.

7. Igor Kotenko, Andrey Chechulin, Dmitry Komashinsky. Categorisation of web pages for protection against inappropriate content in the internet. International Journal of Internet Protocol Technology (IJIPT), Vol. 10, No. 1, 2017. P. 61–71.

8. Котенко И. В., Кушнеревич А. Г., Саенко И. Б., Чечулин А. А. Подход к созданию программной системы распределенной параллельной обработки больших массивов данных о событиях безопасности в компьютерной сети // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VI Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. 2017. С. 286–291.

9. Formal Concept Analysis of Social Networks / Ed. by R. Missaoui, S. Kuznetsov, S. Obiedkov. Springer, 2017.

10. Работа выполнена при поддержке гранта РНФ №18-11-00302 в СПИИРАН.

УДК 004.3, 621.391

ВАРИАНТЫ АППАРАТНОЙ РЕАЛИЗАЦИИ МАЖОРИТАРНОГО ДЕКОДЕРА КОДОВ МАКСИМАЛЬНОЙ ДЛИНЫ НА ОСНОВЕ ДВОЙСТВЕННОГО БАЗИСА

С. С. Владимиров

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

В работе рассмотрены особенности построения аппаратных схем мажоритарного декодера помехоустойчивых кодов максимальной длины на основе двойственного базиса. Проведена оценка быстродействия аппаратной реализации декодера по числу тактов, требуемых для декодирования одной кодовой комбинации, с учетом вариантов реализации. Выполнен анализ построения аппаратной реализации декодера для различных вариантов электрической схемы с использованием системы моделирования цифровых электрических схем Logisim. Приведено сравнение с аппаратными декодерами кода максимальной длины, основанными на другом принципе декодирования.

код максимальной длины, мажоритарное декодирование, декодирование по минимальному расстоянию, двойственный базис, аппаратный декодер, Logisim.

В современных системах передачи данных для обнаружения и исправления ошибок, возникающих при передаче информации по зашумленным каналам связи, широко применяются различные методы помехоустойчивого кодирования. Одним из вариантов применения этих методов является использование кодов, основанных на псевдослучайных последовательностях, в качестве синхропоследовательностей в системах цикловой и кадровой синхронизации. В таких системах широко используются циклические эквидистантные коды максимальной длины, основанные на псевдослучайных М-последовательностях [1].

Использование кодовых слов помехоустойчивого кода максимальной длины в качестве синхропоследовательностей позволяет обеспечить одновременную синхронизацию и идентификацию кадров [1, 2]. В такой системе поток кадров данных определяется по виду синхрослова. Таким образом, в случае (n, k)-кода максимальной длины можно одновременно различать 2^k потоков кадров, идентифицируя, например, отправителя или получателя на стадии начала приема кадра.

Для декодирования кода максимальной длины используются различные алгоритмы декодирования, среди которых можно выделить способы мажоритарного декодирования (декодирования по максимуму правдоподобия). В статье рассмотрим два способа мажоритарного декодирования:

1. Декодирование по минимальному расстоянию.
2. Декодирование на основе двойственного базиса.

Декодирование по минимальному расстоянию

В декодере по минимальному состоянию принятое кодовое слово (n, k)-кода сравнивается со всеми возможными 2^k кодовыми словами и результатом декодирования считается слово, имеющее наименьшее расстояние Хемминга относительно принятой кодовой комбинации, т. е. отличающееся от него в наименьшем числе разрядов. Этот способ декодирования оптимален в том смысле, что он обеспечивает минимальную вероятность ошибочного декодирования кодового слова в двоичном симметричном канале [3]. Для этого метода существует простой, но вычислительно неэффективный декодер, основанный на поэлементном суммировании по модулю два принятого кодового слова с каждым кодовым словом из ансамбля кодовых слов и последующим вычислением веса каждой суммы. Сумма с минимальным весом будет соответствовать результату декодирования. На практике удобно использовать суммирование по модулю два с инверсией результата, вычисляя не количество ошибок, а количество совпадений. В этом случае результатом декодирования будет кодовое слово с максимальным числом совпадающих бит. Схема такого декодера представлена на рис. 1. Этот декодер состоит из трех основных блоков: входного регистра для записи принятой комбинации, блока сравнения с ансамблем кодовых слов, блока поиска значения с максимальным весом.

Рис. 1. Блок-схема декодера по минимальному расстоянию

Блок поиска значения с максимальным весом решает две задачи, характерные для алгоритмов мажоритарного декодирования:

1. Выделение значения с максимальным весом, которое считается результатом декодирования.

2. Принятие решения о невозможности выделения результата, в случае наличия двух и более значений с одинаковым весом, равным максимальному — так называемый «отказ от декодирования».

Работа схемы декодера была проверена в симуляторе электронных схем Logisim. Декодер принимает решение сразу после приема всей кодовой комбинации с учетом задержки на срабатывание блока сравнения и блока поиска. Если задержкой пренебречь, то можно считать, что для декодирования кодового слова (n, k)-кода требуется n тактов задающего генератора.

Декодирование на основе двойственного базиса

В этом варианте декодирования производится вычисление начальной фазы кодового слова (n, k)-кода максимальной длины по n k-элементным участкам этого кодового слова, замкнутого в кольцо [1, 4, 5]. Вычисленная начальная фаза в дальнейшем позволяет восстановить всё кодовое слово [4]. В случае систем с одновременной синхронизацией и идентификацией именно начальная фаза играет роль идентификатора [1, 2]. При декодировании безошибочной кодовой комбинации по каждому k-элементному участку будет вычислен один и тот же результат – начальная фаза кодового слова. В том случае, если в кодовом слове в результате передачи по каналу связи некоторые символы поражаются ошибкой, то k-элементные участки, содержащие эти символы, дадут вычисленное значение, отличное от искомой начальной фазы. Таким образом, в принятой на вход декодера кодовой комбинации по каждому k-элементному участку рассчитывается значение начальной фазы. Результатом декодирования считается то значение, которое получено наибольшее число раз [4, 5].

На рис. 2 приведена общая структурная схема мажоритарного декодера на основе двойственного базиса. Этот декодер состоит из следующих основных блоков: входной регистр, блок вычисления начальной фазы, блок накопления значений, блок поиска значения с максимальным весом.

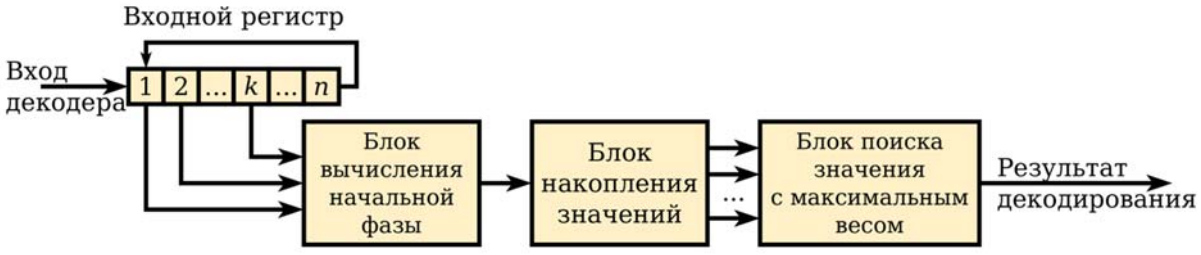


Рис. 2. Блок-схема мажоритарного декодера на основе двойственного базиса

Работа схемы этого декодера также была проверена в симуляторе электронных схем Logisim. В отличие от декодера по минимальному расстоянию декодер на основе двойственного базиса начинает вычисление начальной

фазы сразу по приему первых k элементов кодового слова. С учетом замыкания кодового слова в кольцо, последняя k-элементная комбинация рассчитывается через $k-1$ такт после приема всей кодовой комбинации (если не использовать параллельную схему с дублированием блока вычисления начальной фазы, которая значительно усложняет декодер). Однако, поскольку суммарный вес результатов вычисления в данном алгоритме не превышает n, для однозначного выделения результата требуется, чтобы он имел вес не менее $\lfloor n/2 + 1 \rfloor$. Таким образом, в случае безошибочной комбинации она будет однозначно выделена через $\lfloor n/2 + k \rfloor$ тактов. Например, в случае кода максимальной длины (15, 4) для однозначного выделения начальной фазы кодового слова потребуется принять 11 элементов этого кодового слова. Таким образом, результат декодирования может быть получен еще до окончания приема всей кодовой комбинации.

Варианты реализации блока накопления значений

На рис. 3 представлены два варианта реализации блока накопления значений.

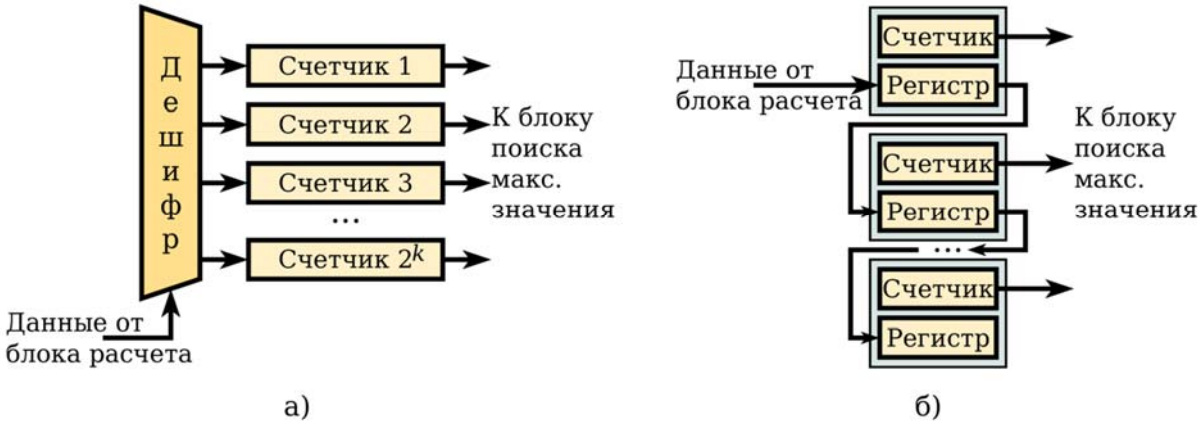


Рис. 3. Варианты реализации блока накопления значений:
а) на основе счетчиков и дешифратора; б) на основе регистров и счетчиков

В первом варианте (рис. 3*а*) каждому возможному значению начальной фазы соответствует счетчик, который при начале обработки кодового слова содержит нулевое значение. При вычислении начальной фазы по каждой k-элементной комбинации наращивается значение соответствующего полученному значению счетчика. Счетчики подключаются к выходу схемы вычисления начальной фазы через дешифратор. Для (n, k)-кода такая схема будет содержать 2^k счетчиков и дешифратор с соответствующим количеством выходов.

Во втором варианте (рис. 3*б*) используется сочетание счетчика и регистра хранения результата вычислений. Полученный по первой k-элементной комбинации результат записывается в первый регистр, и наращивается

соответствующий ему счетчик. Следующее значение сравнивается с предыдущим. В случае равенства производится наращивание значения первого счетчика. В противном случае значение записывается во второй регистр и увеличивается значение второго счетчика. Дальнейшие расчеты и сохранение результатов производятся по аналогии. Поскольку при обработке кодовых слов, содержащих ошибки, обычно возникает ограниченное количество результатов меньшее 2^k, можно получить выигрыш в сложности блока поиска значения с максимальным весом. При построении такого варианта блока накопления необходимо провести предварительное исследование, чтобы определить необходимое количество регистров и счетчиков.

Заключение

Проведенные исследования показали, что мажоритарный декодер на основе двойственного базиса может превосходить по быстродействию декодер по минимальному расстоянию. Он способен однозначно выделить начальную фазу кодового слова до окончания приема всей кодовой комбинации, что является значительным преимуществом при реализации системы с одновременной синхронизацией и идентификацией кадров.

Список используемых источников

1. Когновицкий О. С. Цикловое (кадровое) фазирование совмещенное с выделением адреса получателя на основе двойственного базиса // Информационные технологии и телекоммуникации. 2015. № 3 (11). С. 76–83.

2. Патент на изобретение № 2621181, РФ. Способ цикловой синхронизации с динамической адресацией получателя / О.С. Когновицкий, С.С. Владимиров, Д.С. Кукунин, Д.Я. Лапшов. № 2016121944.

3. Прокис Дж. Цифровая связь; пер. с англ. / Под ред. Д. Д. Кловского. М. : Радио и связь. 2000. 800 с.

4. Когновицкий О. С. Двойственный базис и его применение в телекоммуникациях. СПб. : Линк, 2009. 424 с. ISBN 978-5-98595-020-5.

5. Когновицкий О. С., Владимиров С. С. Расширенный мажоритарный метод декодирования комбинаций эквидистантного циклического кода // Телекоммуникации. 2013. № S7. С. 42–48.

УДК 621.396

МАЛОЕ МНОЖЕСТВО ПОСЛЕДОВАТЕЛЬНОСТЕЙ КАСАМИ И ИХ ДЕКОДИРОВАНИЕ НА ОСНОВЕ ДВОЙСТВЕННОГО БАЗИСА

С. С. Владимиров, О. С. Когновицкий

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

В статье проведен анализ метода обработки и декодирования составных последовательностей малого семейства Касами на основе двойственного базиса. Показаны преимущества данного метода по сравнению с другими известными методами. Определены вероятностные характеристики рассмотренного метода декодирования для моделей каналов ДСК и АБГШ.

последовательности Касами, малое множество последовательностей Касами, двойственный базис, вероятность ошибки.

Во многих радиотехнических системах связи применяются специальные псевдослучайные рекуррентные последовательности (ПСП), которые используются для расширения спектра прямой последовательностью, адресации в многоадресатных системах, скремблирования потоков цифровых данных, синхронизации приемо-передатчика, измерения дальности до объекта. Одним из широко используемых видов рекуррентных ПСП являются последовательности Касами.

В процессе декодирования последовательности в большинстве случаев необходимо после её обнаружения определить фазу ПСП. Для этого используют структурные свойства применяемых ПСП, в частности свойство рекуррентности. В качестве критериев оценки эффективности методов обнаружения и обработки рекуррентных ПСП чаще всего используют вероятности правильного и неправильного декодирования, временные задержки анализа, а также сложность аппаратно-программной реализации.

Наиболее простыми методами обнаружения и обработки рекуррентных последовательностей являются метод приема по безошибочному участку рекуррентной последовательности [1] и метод последовательной оценки Уорда [2]. Но эти методы неприменимы в случае асинхронно-адресных систем, где каждому адресату соответствует своя начальная фаза последовательности. С целью повышения надежности декодирования ПСП часто применяют корреляционные методы обработки [3]. В случае многоадресатной передачи они могут быть применены только в строго синхронной сети.

При этом последовательности должны обладать хорошими ортогональными или квазиортогональными свойствами.

Таким образом, является актуальной задача разработки новых, более эффективных, методов обнаружения и декодирования рекуррентных, главным образом составных, ПСП, в том числе и последовательностей малого семейства Касами [4, 5]. В статье даётся анализ метода декодирования последовательностей малого семейства Касами на основе двойственного базиса над расширенным полем Галуа GF(2^n) [6].

Свойства и формирование последовательностей Касами

Последовательность {$К_м$} малого семейства Касами является составной ПСП с периодом $N_1 = 2^n - 1$, построенной над полем GF(2^n), где степень n должна быть четным числом. Она представляет собой поэлементную сумму по модулю 2 двух последовательностей максимальной длины, одна из которых $\{u\}$ является $М_1$-последовательностью, порождаемой примитивным многочленом $h_1(x)$ степени n, а другая $\{v\}$ – $М_2$-последовательностью, порождаемой неприводимым многочленом $h_2(x)$ степени $n/2$ [4, 5]. Сами последовательности $\{u\}$ и $\{v\}$ формируются как функции-след двумя генераторами с обратными связями по модулям $h_1(x)$ и $h_2(x)$ соответственно [6].

Выберем в качестве исходных данных поле GF(2^6) ($n = 6$) с первообразным элементом ε и примитивный многочлен $h_1(x) = 1 + x + x^6$ с сопряжёнными корнями ε, ε^2, ε^4, ε^8, ε^{16}, ε^{32}. Поле GF(2^6) образовано многочленом $h_1(x)$, а его элементы ε^i представляют собой вычеты по двойному модулю относительно левого степенного базиса:

$$\varepsilon^i = a_0 + a_1\varepsilon + a_2\varepsilon^2 + a_3\varepsilon^3 + a_4\varepsilon^4 + a_5\varepsilon^5; \operatorname{mod d}(2, h_1(x)).$$

Согласно этим исходным данным, $М_1$-последовательности $\{u\}$ с периодом $N_1 = 2^6 - 1 = 63$ соответствует характеристический многочлен $h_1(x)$, а последовательности $\{v\}$ – многочлен $h_2(x)$ степени $n/2 = 3$, корнями которого будут корни многочлена $h_1(x)$ в степени $q = 2^3 + 1 = 9$, т. е. $\mu = \varepsilon^9$, $\mu = (\varepsilon^2)^9 = \varepsilon^{18}$, $\mu^4 = (\varepsilon^4)^9 = \varepsilon^{36}$. Порядок N_2 корней многочлена $h_2(x)$ равен:

$$N_2 = \frac{N_1}{\text{НОД}(9, N_1)} = \frac{63}{\text{НОД}(9, 63)} = 7.$$

Согласно формулам Виета полином $h_2(x)$ равен $h_2(x) = x^3 + x^2 + 1$.

В таблице 1 для примера приведена каноническая последовательность Касами $\{s\}$, образованная как сумма по модулю 2 канонической $М_1$-последовательности $\{u\}$ с начальной фазой $c = 1$, и канонической $М_2$-последовательности $\{v\}$ с начальной фазой $d = 1$. При этом в одном периоде $М_1$-последовательности $\{u\}$ содержится 9 периодов последовательности $\{v\}$.

ТАБЛИЦА 1. Каноническая составная последовательность $\{s\}$ малого семейства Касами

$\{s\}$	s_0	s_1	s_2	s_3	s_4	s_5	s_6	s_7	s_8	s_9	s_{10}	s_{11}	s_{12}	s_{13}	s_{14}	s_{15}	s_{16}	s_{17}	s_{18}	s_{19}	s_{20}
	1	1	1	0	1	1	0	1	1	1	1	0	0	0	1	0	1	1	1	0	1
$\{s\}$	s_{21}	s_{22}	s_{23}	s_{24}	s_{25}	s_{26}	s_{27}	s_{28}	s_{29}	s_{30}	s_{31}	s_{32}	s_{33}	s_{34}	s_{35}	s_{36}	s_{37}	s_{38}	s_{39}	s_{40}	s_{41}
	0	0	0	0	0	0	0	1	0	0	1	1	0	1	1	1	0	0	0	1	0
$\{s\}$	s_{42}	s_{43}	s_{44}	s_{45}	s_{46}	s_{47}	s_{48}	s_{49}	s_{50}	s_{51}	s_{52}	s_{53}	s_{54}	s_{55}	s_{56}	s_{57}	s_{58}	s_{59}	s_{60}	s_{61}	s_{62}
	0	0	0	0	0	1	0	1	0	0	0	0	0	1	1	0	0	1	0	1	1

Рассматриваемой составной последовательности $\{s\}$ малого семейства Касами соответствует характеристический многочлен:

$$P(x) = h_1(x) \cdot h_2(x) = (1 + x + x^6)(1 + x^2 + x^3) = 1 + x + x^2 + x^4 + x^6 + x^8 + x^9.$$

Для декодирования последовательности $\{s\}$ малого семейства Касами, т. е. определения начальных фаз c и d последовательностей $\{u\}$ и $\{v\}$ соответственно, с использованием двойственного базиса и с учетом корней многочленов $h_1(x)$ и $h_2(x)$ найдем по методике, изложенной в [6], коэффициенты двойственного базиса α_i – для $h_1(x)$ и β_i – для $h_2(x)$, $i = 1, 2, 3, \ldots, 9$ (табл. 2).

ТАБЛИЦА 2. Коэффициенты двойственного базиса

α_i для $h_1(x)$	α_1	α_2	α_3	α_4	α_5	α_6	α_7	α_8	α_9
	ε^{14}	ε^{19}	ε^{38}	ε^{37}	ε	1	ε^{22}	ε^{21}	ε^{15}
β_i для $h_2(x)$	β_1	β_2	β_3	β_4	β_5	β_6	β_7	β_8	β_9
	μ	μ^5	μ^3	μ^2	0	0	μ	1	μ^2

Декодирование последовательности Касами в синхронной системе

Процедура декодирования ПСП малого семейства Касами на основе двойственного базиса аналогична декодированию последовательностей Голда и ЛРД-последовательностей, рассмотренному в [6]. Целью декодирования является определение начальной фазы такой последовательности, составленной из начальных фаз последовательностей $\{u\}$ и $\{v\}$.

В синхронной системе известны начала принимаемых последовательностей $\{s\}$, т. е. при выделении безошибочного участка $(s_i, s_{i+1}, s_{i+2}, s_{i+3}, s_{i+4}, s_{i+5}, s_{i+6}, s_{i+7}, s_{i+8})$ декодеру известно значение индекса i, определяющему месторасположение символа s_i от начала последовательности $\{s\}$. Таким образом, зная значение индекса i и коэффициенты двойствен-

ного базиса, по принятому безошибочному m-элементному участку, в соответствии с методикой [6], будут определены начальные фазы c и d последовательностей $\{u\}$ и $\{v\}$.

Пусть первый 9-элементный участок последовательности $\{s\}$ из табл. 1 принят без ошибок, т. е. $(s_0, s_1, s_2, s_3, s_4, s_5, s_6, s_7, s_8) = (111011011)$. Тогда начальные фазы будут равны:

$$c = \alpha_1 + \alpha_2 + \alpha_3 + \alpha_5 + \alpha_6 + \alpha_8 + \alpha_9 = \varepsilon^{14} + \varepsilon^{19} + \varepsilon^{38} + \varepsilon + 1 + \varepsilon^{21} + \varepsilon^{15} = 1 \bmod h_1(x);$$

$$d = \beta_1 + \beta_2 + \beta_3 + \beta_5 + \beta_6 + \beta_8 + \beta_9 = \mu + \mu^5 + \mu^3 + 0 + 0 + 1 + \mu^2 = 1 \bmod h_2(x).$$

Таким образом, составные последовательности $\{u\}$ и $\{v\}$ являются каноническими с начальными фазами $c = 1$ и $d = 1$. Из этого можно сделать очевидный вывод, что фазы составных последовательностей могут быть определены по одному безошибочному m-элементному участку последовательности $\{s\}$, тогда как простые методы обработки по «зачетному» участку и метод Уорда не позволяют это сделать.

Для повышения надежности декодирования последовательностей Касами $\{s\}$ метод на основы двойственного базиса позволяет применить мажоритарный принцип обработки различных m-элементных участков, в том числе и перекрывающихся. Пусть в последовательности из табл. 1 выделен m-элементный участок (s_{24}, s_{25}, s_{26}, s_{27}, s_{28}, s_{29}, s_{30}, s_{31}, s_{32}), равный (000010011), в котором $i = 24$. По этому, также безошибочному, участку вычислим начальные фазы последовательностей $\{u\}$ и $\{v\}$:

$$c = \varepsilon^{-24}(\alpha_5 + \alpha_8 + \alpha_9) = \varepsilon^{-24}(\varepsilon + \varepsilon^{21} + \varepsilon^{15}) = 1 \bmod h_1(x);$$

$$d = \mu^{-24}(\beta_5 + \beta_8 + \beta_9) = \mu^{-3}(0 + 1 + \mu^2) = 1 \bmod h_2(x).$$

То есть, получен тот же результат, что и подтверждает возможность мажоритарного декодирования в канале с ошибками по большинству одинаковых значений c и d.

Вероятностные характеристики декодера последовательностей Касами на основе двойственного базиса при синхронном декодировании

Для оценки вероятностных характеристик синхронного декодирования по методу двойственного базиса было проведено моделирование по методу Монте-Карло в системе математических вычислений GNU/Octave. Моделирование проводилось для модели двоично-симметричного канала (ДСК) и модели канала АБГШ совместно с двоичной фазовой манипуляцией. Схема модели системы передачи приведена на рис. 1.

При моделировании было передано по 20000 последовательностей Касами на каждое значение битовой ошибки в канале ДСК и каждое значение

отношения сигнал/шум с канале АБГШ. В результате были получены оценочные значения (т. н. «доли») вероятностей правильного декодирования РПД, неправильного декодирования РНД и отказа в декодировании РОД. Под отказом в декодировании понимается ситуация, при которой в результате мажоритарного декодирования не представляется возможным однозначно определить значение начальной фазы.

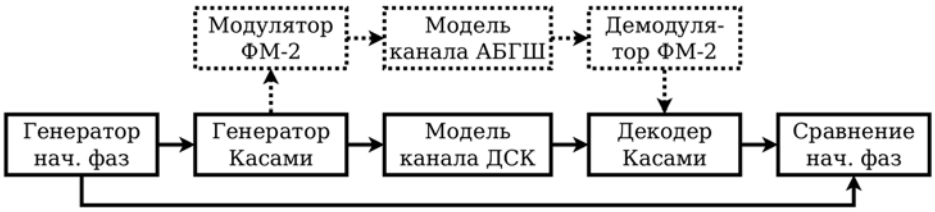


Рис. 1. Модель системы передачи для определения вероятностных характеристик синхронного декодирования последовательности Касами по методу двойственного базиса

Графики вероятностных характеристик приведены на рис. 2.

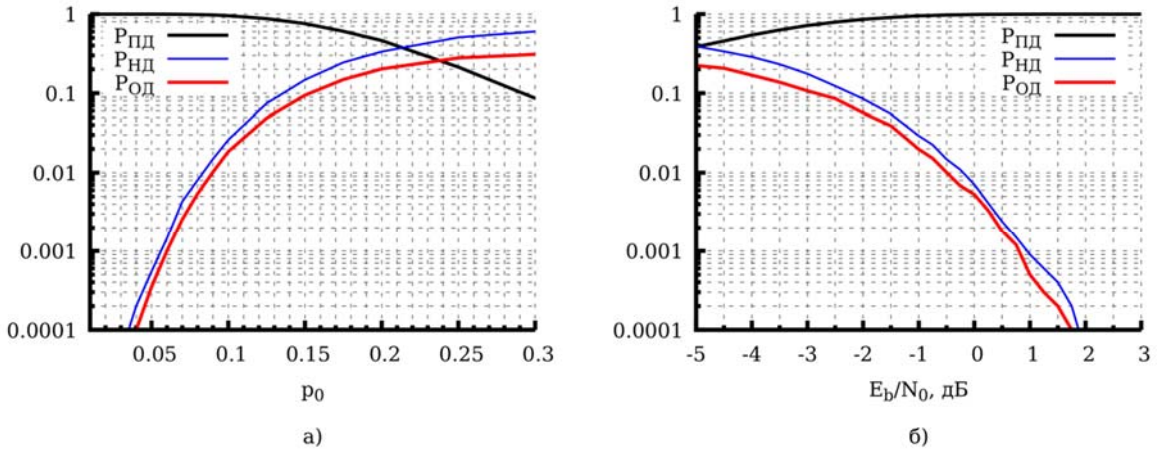


Рис. 2. Вероятностные характеристики декодера последовательностей Касами на основе двойственного базиса при синхронном декодировании:
а) для канала ДСК; б) для канала АБГШ с манипуляцией ФМ-2

В дальнейшем авторы планируют рассмотреть вопросы декодирования укороченных последовательностей малого семейства Касами, декодирование последовательностей большого семейства Касами и методы повышения вероятности правильного декодирования методом постобработки последовательности.

Список используемых источников

1. Лосев В. Р., Бродская Е. Б., Коржик В. И. Поиск и декодирование сложных дискретных сигналов. М. : Связь, 1979. 302 с.

2. Диксон Р. К. Широкополосные системы; пер. с англ. / Под ред. В. И. Журавлева. М. : Связь, 1979. 304 с.

3. Ипатов В. П. Широкополосные системы и кодовое разделение сигналов. Принципы и приложения. М. : Техносфера, 2007. 488 с. ISBN 978-5-94836-128-4

4. Kasami, T. (1966). Weight Distribution Formula for Some Class of Cyclic Codes. Technical report R285. April 1966. Illinois : University of Illinois. 32 p.

5. Yefeng H. E., Wenping M. A. Generalized Kasami Sequences: The Small Set // Journal of Computational Information Systems. No. 7. 2011. PP. 4065–4070.

6. Когновицкий О. С. Двойственный базис и его применение в телекоммуникациях. СПб. : Линк, 2009. 424 с. ISBN 978-5-98595-020-5.

УДК 004.056.53

СТРАТЕГИИ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОСТИ ОБЛАКОВ

В. Н. Волкогонов, А. В. Иванов

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

В данной статье рассматриваются вопросы обеспечения конфиденциальности облаков. Так же, как и у других систем безопасности, под конфиденциальностью облаков понимается конфиденциальность данных и вычислений. Нарушение облачной конфиденциальности может привести к утечке личной информации клиентов. Сохранение конфиденциальности – это более строгая форма первоначального термина, так как оно тоже предотвращают утечку информации. Поэтому если нарушается конфиденциальность облака, то нарушается и сохранение конфиденциальности. Существует несколько базовых подходов сохранения конфиденциальности облаков. Использование информационного центра безопасности, доверенных вычислений и криптографических протоколов. На основе данных подходов выстраиваются стратегии защиты, предлагаемые авторами статьи.

конфиденциальность, облако, криптографические протоколы, защита.

Обеспечение конфиденциальности облаков сложная задача. Как видно из таблицы (см. ниже) существует три главных подхода обеспечения сохранности конфиденциальности, на основе которых выстраиваются стратегии защиты [1].

Полностью гомоморфное шифрование – стратегия защиты, основанная на использовании криптографических протоколов. Данная стратегия предполагает вычисление зашифрованных данных на не доверенных серверах. Данные могут обрабатываться без расшифровки. Сами же облачные сервера

почти не обладают сведениями о входящих данных. Следовательно, передача вычислений полностью конфиденциальна. Данный инструмент очень надежен, но из-за использования больших объемов вычислений, не является эффективным для использования на практике [2].

ТАБЛИЦА. Подходы обеспечения сохранности конфиденциальности

Подход	Описание	Пример
Информационный центр безопасности	Данные объектов обладают своими политиками контроля	Передача данных осуществляется при использовании криптографических протоколов и систем доступа [Di Vemercati, 2007]
Доверенные вычисление	Система будет ожидаемо вести себя с помощью программного и аппаратного обеспечения	Доверенная облачная вычислительная платформа [Santos, 2009]
Криптографические протоколы	Использования Криптографических инструментов и техник для обеспечения конфиденциальности	Полностью гомоморфное шифрование [Gentry, 2009]

Для решения проблем, связанных с эффективностью применения стратегии защиты, была разработана следующая стратегия. Менеджер конфиденциальности использует техники обфускации. Частный менеджер может обеспечить сервисы обфускации и деобфускации, что позволяет уменьшить количество важной информации в облаке. Подробно технику обфускации описали Красов А. В. и Шариков П. И. в статье «Методика защиты байт-кода java-программы от декомпиляции и хищения исходного кода злоумышленником» [3]. Главная идея заключается в том, чтобы зашифровать не все данные, а только частные данные клиентов. Все процессы с данными осуществляются только на зашифрованных данных. Проблема в реализации заключается в том, что нужно договариваться с провайдерами на реализацию дополнительных услуг по защите конфиденциальности [4].

Использование криптографических решений на основе гомоморфном и проверяемом шифровании страдают высокой задержкой, так как они обеспечивают практически безопасную передачу данных на не доверенных серверах. Что бы обойти данную проблему предлагается объединить надежный аппаратный токен с функцией оценки безопасности. Идея заключается в том, чтобы вычислить произвольные функции на данных, которые все еще находятся в зашифрованном виде. Вычисления не содержат никакой информации и подлежат проверке. Если у токена есть подозрения в ненадежности,

то обработка данных клиента может быть выполнена на токене, который привязан к другому серверу. Данные свойства токена гарантируют легитимность всех вычислений, а также возможность их проверки. Следует только не допустить несанкционированного доступа на этапе предварительной обработки и установки. В последующей онлайн фазе в облаке выполняются только симметричные операции, не требующих взаимодействий с токеном [5].

Общая структура обеспечения защиты данных для решения проблем с конфиденциальностью состоит их трех ключевых блоков:

1) Стратегия ранжирования политик, помогающая облачным клиентам идентифицировать облачного провайдера, который наиболее полно удовлетворяет их требования конфиденциальности.

2) Механизм автоматической генерации политик, который сравнивает требование клиента и политики поставщика и предлагает им оптимальную политику.

3) Обеспечение соблюдения политик.

Прямой путь получения рейтинга политик – это сравнение требований клиента с политиками нескольких поставщиков услуг и получения политики с наивысшим рейтингом. Сравнение может происходить на стороне клиента, провайдера или третьего лица [6].

Криптография сама по себе не может обеспечить полное решение всех проблем конфиденциальности в облачных вычислениях, даже с помощью таких мощных инструментов как полное гомоморфное шифрование. Поэтому можно разделить проблемы с конфиденциальностью на классы, а затем применять конкретные приложения. Было доказано, что при распределении данных между клиентами, криптографические протоколы не могут быть реализованы так, чтобы обеспечить конфиденциальность. Задача облака состоит в том, чтобы в зависимости от проблемы, запускать конкретное приложение [7]. Классы проблем:

1) Частные вычисление одного клиента.
2) Частные мультиклиентские вычисления.
3) Частные мультиклиентские вычисления с учётом состояния.

Приложения для частных вычислений одного клиента обрабатывают только данные, принадлежащие одному клиенту. Ни одна другая сторона не может узнать какую-либо информацию о внутреннем процессе. Примером является программа подготовки налоговых деклараций входящий финансовые данные клиента, не должны быть доступны другим клиентам и самому облаку. Данный класс проблем может быть решен полным гомоморфным шифрованием.

Приложения для частных мультиклинетских вычислений работают с набором данных, принадлежащих нескольким клиентам. Так как клиентов несколько, конфиденциальность данных среди этих клиентов сохраняется

более сложным образом. Существуют политики контроля доступа, которые должны соблюдаться при обработке данных. Приложение представляют собой систему социальных сетей, где у каждого клиента есть личный ключ. Клиент может указать, с помощью каких ключей можно просмотреть его данные. Было доказано, что частные мультклиентские вычисления недостижимы с использованием криптографии.

Приложения для последнего класса очень похожи на приложения для частных мультиклиентских вычислений. Разница заключается в том, что политика контроля и доступа данных для клиента зависит от истории выполнения приложения [8].

Вывод. Конфиденциальность представляет собой критическую проблему в отношении облачных вычислений из-за того, что данные клиентов находятся среди не доверенных облачных серверов. Следовательно, существуют потенциальные риски раскрытия конфиденциальных данных. Чтобы личные данные не раскрывались, конфиденциальность становится незаменимой. Все атрибуты безопасности прямо или косвенно влияют на конфиденциальность. По мнению авторов статьи, лучшей стратегией защиты является использование надежного аппаратного токена. Данная стратегия обеспечивает хорошую эффективность и защиту, а также обладает не сложной реализацией.

Список используемых источников

1. Di Vimercati S. D., Foresti S., Jajodia S., Paraboschi S., and Samarati P. A data outsourcing architecture combining cryptography and access control // Proc. 2007 ACM workshop on Computer security architecture, 2007, pp. 63–69.

2. Gentry C. Fully homomorphic encryption using ideal lattices // In STOC, 2009, pp. 169–178.

3. Красов А. В., Шариков П. И. Методика защиты байт-кода java-программы от декомпиляции и хищения исходного кода злоумышленником // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2017. № 1. С. 47–50.

4. Santos N., Gummadi K. P., and Rodrigues R. Towards trusted cloud computing // Proc. 2009 conference on Hot topics in cloud computing, 2009.

5. Sadeghi A. R., Schneider T., and Winandy M. Token-Based Cloud Computing // Trust and Trustworthy Computing, 2010, pp. 417–429.

6. Pearson S., Shen Y., and Mowbray M. A privacy manager for cloud computing // Cloud Computing, 2009, pp. 90–106.

7. Van Dijk M. and Juels A. On the Impossibility of Cryptography Alone for Privacy-Preserving Cloud Computing // IACR ePrint 2010, vol. 305.

8. Chow R., Golle P., Jakobsson M., Shi E., Staddon J., Masuoka R., and Molina J. Controlling data in the cloud: outsourcing computation without outsourcing control // Proc. 2009 ACM workshop on Cloud computing security, 2009, pp. 85–90.

УДК 004.056.53

МЕТОДЫ ВЛОЖЕНИЯ ЦИФРОВЫХ ВОДЯНЫХ ЗНАКОВ В 32-БИТНЫЕ PE-ФАЙЛЫ

В. Н. Волкогонов, В. Е. Радынская

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

В основе любого программного продукта лежит интеллектуальная собственность его разработчиков, поэтому возникает вопрос защиты авторских прав. Статья посвящена методам внедрения цифровых водяных знаков в PE-файлы, с целью их защиты. Водяные знаки вкладываются с помощью некоторых эквивалентных изменений в исходном тексте программы. Предполагается, что такие знаки будут не заметны для злоумышленника, и как следствие, устойчивы к атакам.

цифровые водяные знаки, PE-файлы.

В основе любого программного продукта лежит интеллектуальная собственность его разработчиков, поэтому возникает вопрос защиты авторских прав. Самым распространенным форматом программных продуктов является portable executable (далее PE) – основной формат исполняемых файлов приложений в 32 и в 64-разрядных системах Microsoft Windows [1].

Одним из способов защиты PE-файлов [2] является метод цифровых водяных знаков (далее ЦВЗ). Этот метод уникален тем, что нацелен не на предотвращение пиратства программных продуктов, а на доказательство того, что пиратство произошло и нелегально скопированное программное обеспечение принадлежит человеку, который заявил о нарушении авторских прав [1].

Программные ЦВЗ могут быть статические или динамические. В свою очередь статистические ЦВЗ делятся два типа: ЦВЗ данных и ЦВЗ кода. ЦВЗ данных вкладывается непосредственно в секцию данных PE-файла, а ЦВЗ кода, соответственно, в секцию кода [2]. Простой ЦВЗ кода основывается на перестановке порядка некоторых инструкций в программе.

Вложение ЦВЗ в PE-файлы имеет свои значительные особенности. Например, нельзя произвести вложение путем прямого изменения некоторых бит исполняемых файлов, потому что подобные изменения, в большинстве случаев, разрушат алгоритм работы программы или сделают ее полностью неработоспособной [3]. Один из вариантов «безопасного» вложения ЦВЗ в GUI-приложение основывается на изменении цвета пикселя какой-либо кнопки. Цвет пикселя и будет ЦВЗ в программе. Но такой вариант

не всегда удобен и с высокой долей вероятности, злоумышленнику не составит труда удалить или изменить такой ЦВЗ.

Скрыть ЦВЗ, внедрив его в PE-файл можно несколькими методами:

1. Вложение в заголовок. После таблицы секций (перед данными первой секции) есть интервал, заполненный нулями, появившийся в результате файлового выравнивания (значение *FileAlignment* в заголовке файла). Этот интервал подходит для внедрения ЦВЗ [4], но в нем очень мало места, или оно может вовсе отсутствовать (как в приложениях *Windows*). Следовательно, внедряемый код должен быть также очень мал. Но несомненным преимуществом этого способа является неизменность размера файла.

2. Запись в конец последней секции. Суть способа заключается в добавлении ЦВЗ в конец последней секции с изменением атрибутов данной секции, если это необходимо (например, если внедряется ЦВЗ кода, то необходимо добавить атрибут «E», который указывает на то, что секция является выполняемой). Следует отметить [5], что данным способом можно внедрить любое количество кода, но, разумеется, при этом размер файла увеличится.

3. Добавление новой секции. Способ аналогичен предыдущему, однако, в данном случае создается собственная новая секция [6].

Кроме этих способов можно вложить ЦВЗ в PE-файл, просто записав данные в конец самого файла, но если эти данные представляют собой исполняемый код, то этот способ не подходит, так как данные, записанные в конец файла, не влияют на функциональность PE-файла.

Не трудно заметить, что ЦВЗ, вложение которых производится на основе данных методов, могут быть подвержены атакам удаления и изменения. Чтобы этого избежать, можно создать ЦВЗ кода, удаление которого нарушит работоспособность программы.

Предположим, что в программный продукт, с целью защиты авторских прав, необходимо вложить ЦВЗ «BONCH» [3]. Сопоставим ASCII-символам данного ЦВЗ опкоды ассемблера. Пример показан в таблице 1.

ТАБЛИЦА 1.Сопоставление ascii-символов и опкодов

ASCII-символ	Опкод	Команда ассемблера
B	42	inc edx
O	4F	dec edi
N	4E	dec esi
C	43	inc ebx
H	48	dec eax

В итоге получается следующий набор инструкций, показанный в таблице 2.

ТАБЛИЦА 2. Набор инструкций

inc	edx
dec	edi
dec	esi
inc	ebx
dec	eax

Эти инструкции могут быть внедрены несколькими способами:

1. На этапе написания программы (если используется высокоуровневое программирование – в качестве ассемблерной вставки) [7]. При этом этот код может быть, как функционально важным, удаление которого полностью изменит алгоритм работы программы, так и быть «мертвым кодом», «спрятанным» между важных инструкций. Разумеется, первый вариант является наиболее перспективным, но и наиболее сложным в реализации.

2. В уже скомпилированное приложение. Код может внедряться методами, описанными выше. Реализация этого варианта не представляет сложности. Более интересным является внедрение с помощью «морфинга» ассемблерных инструкций. Известно, что любая ассемблерная команда имеет множество эквивалентных синонимов, которые могут выступать, как в виде одной команды, так и в виде нескольких инструкций. Например [8], команда mov eax, 0 заменяется на команду xor eax, eax. А команды: mov ecx edx add ecx eax; inc ecx заменяются на команду: lea ecx, dword ptr [edx + eax + 01].

Таким способом можно полностью или частично изменить инструкции скомпилированного приложения, приведя несколько из них, к выбранному ЦВЗ (в примере выше ЦВЗ – «BONCH»). В таком случае, с высокой вероятностью, наличие ЦВЗ не будет заметно. Но если обнаружение ЦВЗ все-таки произойдет, то, просто удалить его будет нельзя, т. к. нарушится алгоритм работы программы. Но, к сожалению, на сегодняшний день неизвестно алгоритмов реализации подобного метода внедрения ЦВЗ.

Список используемых источников

1. Коржик В. И., Небаева К. А., Герлинг Е. Ю., Догиль П. С., Федянин И.А. Цифровая стеганография и цифровые водяные знаки / Под общ. ред. проф. В. И. Коржика. СПб. : СПбГУТ. 2016. 226 с.

2. Shterenberg S. I., Krasov A. V., Ushakov I. A. Analysis of using equivalent instructions at the hidden embedding of information into the executable files // Journal of Theoretical and Applied Information Technology. 2015. Т. 80. № 1. PP. 28–34.

3. Шариков П. И., Красов А. В., Штеренберг С. И. Методика создания и вложения цифрового водяного знака в исполняемые java файлы на основе замен опкодов // T-Comm: Телекоммуникации и транспорт. 2017. Т. 11. № 3. С. 66–70.

4. Красов А. В., Верещагин А. С., Цветков А. Ю. Аутентификация программного обеспечения при помощи вложения цифровых водяных знаков в исполняемый код // Телекоммуникации. 2013. № S7. С. 27–29.

5. Красов А. В., Шариков П. И. Методика защиты байт-кода java-программы от декомпиляции и хищения исходного кода злоумышленником // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2017. № 1. С. 47–50.

6. Шариков П. И., Красов А. В. Исследование уязвимости сериализации и десериализации данных в java // Региональная информатика и информационная безопасность. Сборник трудов. Выпуск 3, СПОИСУ. СПб. 2017. С. 332–335.

7. Шариков П. И. Методика нахождение величины наиболее выгодного контейнера в форматах исполняемых файлов // Наукоемкие технологии в космических исследованиях Земли. 2015. Т. 7. №5. С. 58–62.

8. Хомяков И. Н., Красов А. В. Анализ возможностей скрытого вложения информации в структуру байт-кода java // Актуальные проблемы инфотелекоммуникаций в науке и образовании. II Международная научно-техническая и научно-методическая конференция. СПбГУТ. СПб., 2013. С. 859–861.

УДК 621.39

ИССЛЕДОВАНИЕ ВОЗМОЖНОСТИ РАСШИРЕНИЯ СПЕКТРАЛЬНОГО ДИАПАЗОНА УСИЛЕНИЯ ОПТИЧЕСКИХ УСИЛИТЕЛЕЙ EDFA

С. А. Гагарина, В. С. Кузнецов, Д. С. Микутавичайте

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

В данной работе рассматривается одна из важнейших задач в области инфокоммуникаций – расширение спектрального диапазона усиления оптических усилителей EDFA. Определены способы смещения спектрального диапазона за счёт использования нескольких оптических усилителей, рассмотрены влияния конфигурации усилителей на смещение диапазонов усиления, подобраны оптимальные уровни мощности усиливаемых сигналов и параметры усилителей в моделирующей программе для каждого из диапазонов. Полученные результаты могут быть использованы в качестве рекомендаций для разработчиков оптических усилителей и проектировщиков волоконно-оптических линий связи.

эрбиевые оптические усилители, спектральный диапазон, смещение, уплотнение каналов.

Исследование возможности передачи в одном волокне как можно больше длин волн позволяет значительно увеличить пропускную способность системы связи. Оптические усилители EDFA (*Erbium Doped Fiber Amplifier*) работают в стандартном С-диапазоне, включающий длины волн от 1530 нм до 1565 нм, что позволяет использовать такие усилители на магистральных волоконно-оптических линиях связи с системами плотного спектрального мультиплексирования DWDM (*Dense Wavelength Division Multiplexing*). Однако, для расширения рабочего диапазона усиления необходимо попытаться задействовать коротковолновый S-диапазон и длинноволновый L-диапазон.

Прежде чем моделировать схему с большим количеством каналов, необходимо определить оптимальные параметры оптического усилителя. Для этого был исследован узкий диапазон длин волн, вблизи центральной длины волны 1550 нм. Исследование проводилось для различных конфигураций оптического усилителя. Так, в моделирующей программе GainMaster [1] были получены оптимальные параметры для системы связи с одним оптическим усилителем: уровень мощности входного усиливаемого сигнала −30 дБм, эрбиевое волокно I-4 длиной 14 м, способ включения сигнала накачки – попутный, уровень мощностью накачки 20 дБм.

Исследование всего диапазона с подобранными оптимальными параметрами оптического усилителя в рамках моделирующей программы, позволяющей использовать длины волн от 1520 нм до 1617 нм, приведено на рис. 1.

Рис. 1. Моделирование диапазона 1520-1617 нм с попутным включением сигнала накачки с уровнем мощности −30 дБм, эрбиевым волокном I-4 длиной 14 м и уровнем усиливаемого сигнала −30 дБм

Уровни мощности выходного сигнала в диапазонах S и L значительно ниже по сравнению с сигналами в стандартном диапазоне. Следовательно, помимо расширения спектрального диапазона оптического усилителя необходимо учитывать равномерность спектра усиленного сигнала во всем диапазоне для упрощения системы связи.

Одним из способов решения проблемы неравномерности спектра является разбиение спектрального диапазона на участки и использование отдельных усилителей на каждый диапазон [2] Для этого в структурную схему усилительного пункта необходимо добавить WDM-демультиплексор

для разделения каналов по диапазонам и WMD-мультиплексор для их объединения и передаче по одному волокну (рис. 2),

где ОП – оконечный пункт;
УП – усилительный пункт;
ОВ – оптическое волокно;
EDFA – оптический усилитель;
DMUX – демультиплексор;
MUX – мультиплексор;
ЭОВ – эрбиевое оптическое волокно.

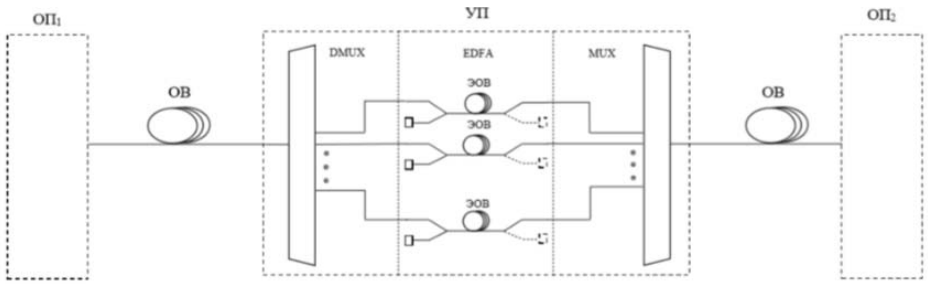
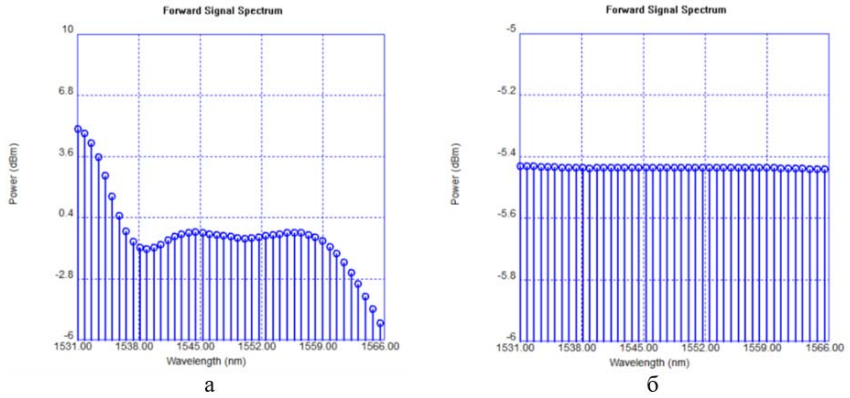


Рис. 2. Структурная схема исследуемого усилительного пункта

Для сглаживания спектра неравномерного усиленного сигнала при моделировании стандартного диапазона необходимо использовать фильтр с оптимизацией GFF (*Gain Flatting Filter*). Фильтр GFF автоматически генерирует желательный спектр для селективного фильтра. После прохождения через фильтр оптический сигнал снизился во всем исследуемом стандартном диапазоне длин волн (рис. 3).



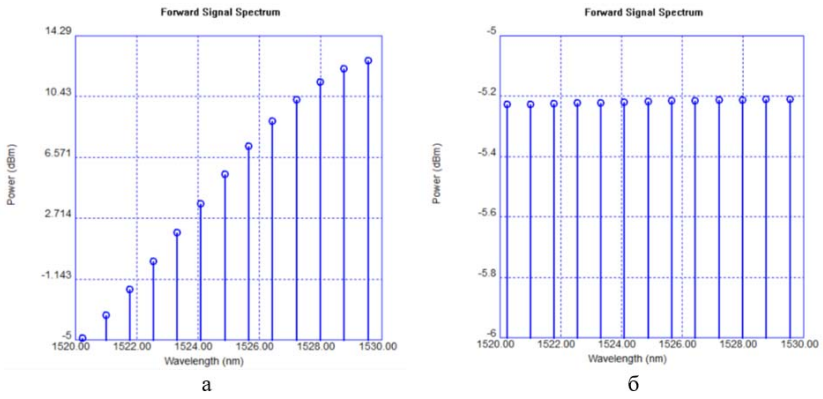
а б

Рис. 3. Спектрограммы усиленного сигнала стандартного диапазона без использования фильтра GFF (а) и с использованием фильтра GFF (б). Попутное включение накачки с уровнем мощности 20 дБм, эрбиевое волокно I-4 длиной 14 м, уровень мощности усиливаемого сигнала −30 дБм

Добавление к С-диапазону длин волн из диапазонов S и L и использование фильтра позволяет добиться неравномерного спектра, но приводит

к значительному снижению уровня усиленного сигнала. Поэтому целесообразно отделить области диапазонов S и C, а для диапазона L поделить спектр сигнала на небольшие участки порядка 10 нм для уменьшения неравномерности коэффициента усиления и получения высокого уровня усиленного сигнала. Фильтр GFF в области диапазона L не влияет на конечный результат и далее не используется.

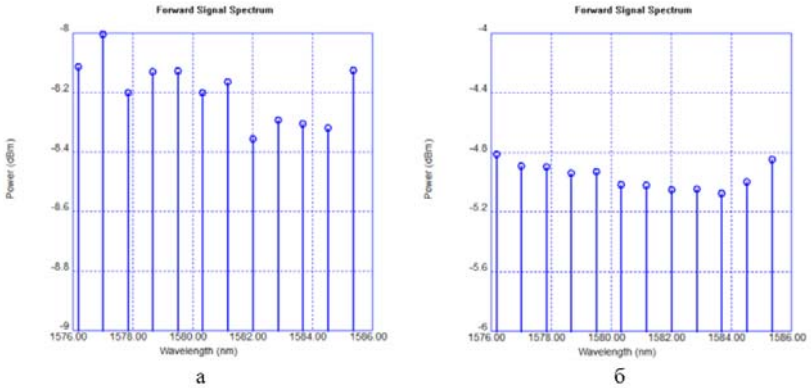
На рис. 4 приведена спектрограмма усиленного сигнала для длин волн S-диапазона 1520-1530 нм. Для этой области характерно использование короткого эрбиевого оптического волокна и большой мощности источника накачки по сравнению с моделированием в области C-диапазона.



а б

Рис. 4.Спектрограмма усиленного сигнала диапазона 1520-1530 нм без использования фильтра GFF (а) и с использованием фильтра GFF (б). Попутное включение накачки с уровнем мощности 26 дБм, эрбиевое волокно I-4 длиной 9 м, уровнем усиливаемого сигнала −30 дБм

Для длин волн L-диапазона характерно увеличение длины эрбиевого волокна и увеличение усиливаемого сигнала до уровня −20 дБм (рис. 5).



а б

Рис. 5. Спектрограмма усиленного сигнала диапазона 1575-1585 нм. Попутное включение накачки с уровнем мощности 15 дБм, эрбиевое волокно I-25 длиной 50 м, уровень мощности усиливаемого сигнала −30 дБм (а), попутное включение накачки с уровнем мощности 15 дБм, эрбиевое волокно I-25 длиной 8, уровень мощности усиливаемого сигнала −30 дБм

Моделирование проводилось с использованием различных эрбиевых волокон с различным параметром насыщенности. Результаты моделирования с наиболее оптимальными выходными характеристиками усиленных сигналов во всем исследуемом диапазоне усиления ОУ предоставлены в таблице.

ТАБЛИЦА. Сравнение наиболее оптимальных результатов моделирования для нескольких спектральных диапазонов длин волн с использованием различных конфигураций ОУ и уровнем информационного сигнала

Длины волн, нм	$p_{s\text{-}out}$, дБм	Тип ЭОВ	Длина ЭОВ l, м	p_p, дБм	$p_{s\text{-}in}$, дБм	G, дБм	ΔG, дБ
1520–1530	−4,231 (с фильтром)	I-4	9	23	−20	15,796	0,013
1535–1565	−4,646 (с фильтром)	I-4	14	20	−30	25,324	0,073
1565–1575	−5,488	I-4	50	15	−20	14,512	0,364
1575–1585	−5,564	M-12	16	14	−20	14,436	1,123
1585–1595	−4,858	I-25	7	16	−20	15,415	0,348
1595–1605	−7,106	M-12	20	15	−20	9,379	0,706
1605–1615	−8,984	M-12	17	14	−20	11,016	2,484

Таким образом, определены способы расширения спектрального диапазона за счет использования нескольких оптических усилителей для отдельных узких спектральных диапазонов длин волн, подобраны оптимальные уровни мощности усиливаемых сигналов и параметры усилителей в моделирующей программе для каждого из диапазонов.

Несмотря на то, что большое количество оптических усилителей EDFA в усилительном пункте ведет к удорожанию системы связи, в частности, за счет использования WDM-мультиплексоров и демультиплексоров, такое решение оправдывается экономией оптического волокна на магистральных линиях.

Список используемых источников

1. GAINMASTER™ Amplifier Designed Software Manual Revision1. – «Fibercore Limited», 2016. 16 с.

2. Курков А. С., Наний О. Е. Эрбиевые волоконно-оптические усилители // Ligtwave − russian edition 2003. № 1. 21 с.

Статья предоставлена заведующим кафедрой, кандидатом технических наук, доцентом С. Ф. Глаголевым.

УДК 656.254

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ВОЛОКОННО-ОПТИЧЕСКИХ СИСТЕМ СВЯЗИ БОЛЬШОЙ ПРОТЯЖЕННОСТИ С МУЛЬТИПЛЕКСИРОВАНИЕМ В ВОЛНОВОЙ ОБЛАСТИ

С. Ф. Глаголев, С. Э. Доценко, В. В. Котов

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

В статье проведено моделирование волоконно-оптических систем связи большой протяженности с мультиплексированием в волновой области, состоящих из отдельных усилительных участков. Исследовались ВОСС с различными типами одномодовых телекоммуникационных и компенсирующих хроматическую дисперсию оптических волокон.

моделирование волоконно-оптических систем связи (ВОСС), DWDM, оптическое волокно, компенсация хроматической дисперсии.

В настоящее время широко используются высокоскоростные волоконно-оптические системы связи (ВОСС) большой протяженности с технологией мультиплексирование в волновой области (DWDM) и применением каскадного усиления оптических сигналов [1]. При многовариантном проектировании таких ВОСС для выбора элементной базы и оптимальных технических решений целесообразно использовать моделирующие программы, например, OptiSystem.

В работе моделировались многопролетные ВОСС с амплитудной (АМ) и фазовой (ФМ) модуляциями при энергетическом приеме модулированных сигналов. Исследовалось влияние на качество связи типа и параметров кодирования (RZ, NRZ), а также мощности источников излучения. Схема моделируемой четырехканальной ВОСС с АМ показана на рис. 1.

Она содержит на передающей стороне 4 одномодовых излучателя, 4 амплитудных модулятора и терминальный мультиплексор. Линейный оптический тракт (ЛОТ) состоит из нескольких участков (колец), которые содержат основное и компенсирующее оптические волокна (ОВ) и 2 оптических эрбиевых усилителя (EDFA). В каждом кольце полностью компенсируется затухание и хроматическая дисперсия на одной из несущих частот. Демультиплексор разделяет выходной сигнал ВОСС между 4 приемниками. Входя-

щие в схему измерительные приборы позволяют определять уровни мощности, контролировать форму сигнала и его спектр в любой точке ЛОТ. Качество связи (*Q*-фактор, глаз-диаграмма и коэффициент ошибок) на выходе ЛОТ определяется анализатором ошибок.

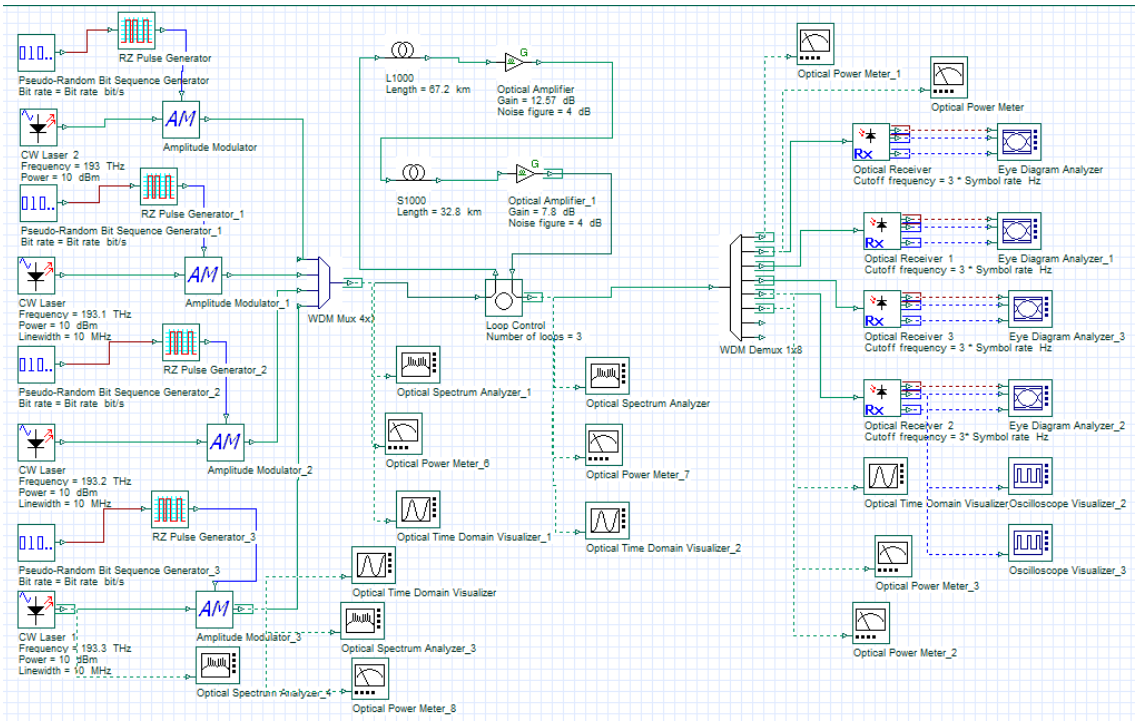


Рис. 1. Схема моделирования ВОСС с АМ и DWDM

Исследовались 4 варианта построения ВОСС с общей длиной усилительного участка 100 км, включая основное и компенсирующее ОВ. Параметры основных и компенсирующих ОВ [2, 3] приведены в таблице 1.

Отметим, что пара ОВ *Vascade L*1000 и *S*1000 (1 вариант в таблице 1) была создана компанией *Corning* для подводных магистралей большой протяженности с полной компенсацией хроматической дисперсии (ХД) [2]. Другие варианты исследований соответствуют параметрам ОВ, рекомендованных компанией *Furukawa* [3].

Длины основного и компенсирующего ОВ для длины волны λ определялись системой двух уравнений, а решения помещены в таблицу 1.

$$\left[D_{SF}(\lambda_c)+S_{SF}\cdot(\lambda-\lambda_c)\right]\cdot l_{SF}+\left[D_{DCF}(\lambda_c)+S_{DCF}\cdot(\lambda-\lambda_c)\right]\cdot l_{DCF}=\Delta t=0$$

$$l=l_{SF}+l_{DCF}=100\,км,$$

где l_{SF} и l_{DCF} – длины основного и компенсирующего ОВ, соответственно; $D_{SF}(\lambda_c)$, $D_{DCF}(\lambda_c)$ – коэффициенты ХД для стандартного и компенсирующего ОВ на длине волны λ_c = 1550 нм; Δt – расширение импульса за счет ХД на длине волны λ, $S_{SF}(\lambda_c)$, $S_{DCF}(\lambda_c)$ – наклоны коэффициентов ХД ($dD_{SF}/d\lambda$

и $dD_{DCF}/d\lambda$) для стандартного и компенсирующего ОВ на длине волны λ_c = 1550 нм.

ТАБЛИЦА 1. Параметры оптических волокон

№ вар	ОВ	Длина, км	Затухание, дБ	ХД, пс/(нм км)	Наклон ХД, пс/(нм^2 км)	Усиление ОУ, дБ	Эфф. площадь, мкм^2
1	L1000	67,3	0,187	18,5	0,06	12,58	100
	S1000	32,7	0,235	–38	–0,12	7,68	27
2	SF	85,83	0,2	17	0,058	17,17	82
	DCF	14,17	0,4	–103	–0,35	5,67	21
3	TrueWave	93,37	0,22	4,5	0,045	20,45	52
	DCF	6,63	0,4	–63,4	–0,634	2,65	17
4	LEAF	91,73	0,2	4,2	0,085	18,35	72
	DCF	8,27	0,4	–46,6	–0,932	3,31	13

Моделировалась четырехканальная ВОСС с DWDM со скоростью передачи 10 Гбит/с. Были выбраны несущие частоты источников 193, 193.1, 193.2 и 193.3 ТГц. Уровень мощности источников излучения устанавливался равным 10 дБм. Количество пролетов (усилительных участков) изменялось от 1 до 10, что позволило исследовать изменения качества связи при изменении длины линии от 100 до 1000 км.

На рис. 3 приведены изменения среднего для всех каналов *Q*-фактора при изменении длины линии для различных вариантов исследования (табл. 1) при АМ и кодировании RZ-50. На рис. 4 приведены результаты аналогичных исследований при NRZ кодировании.

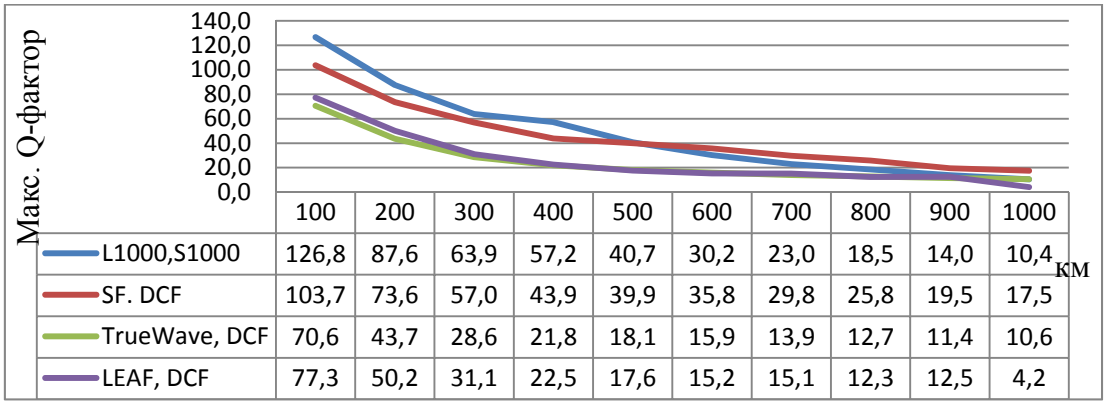
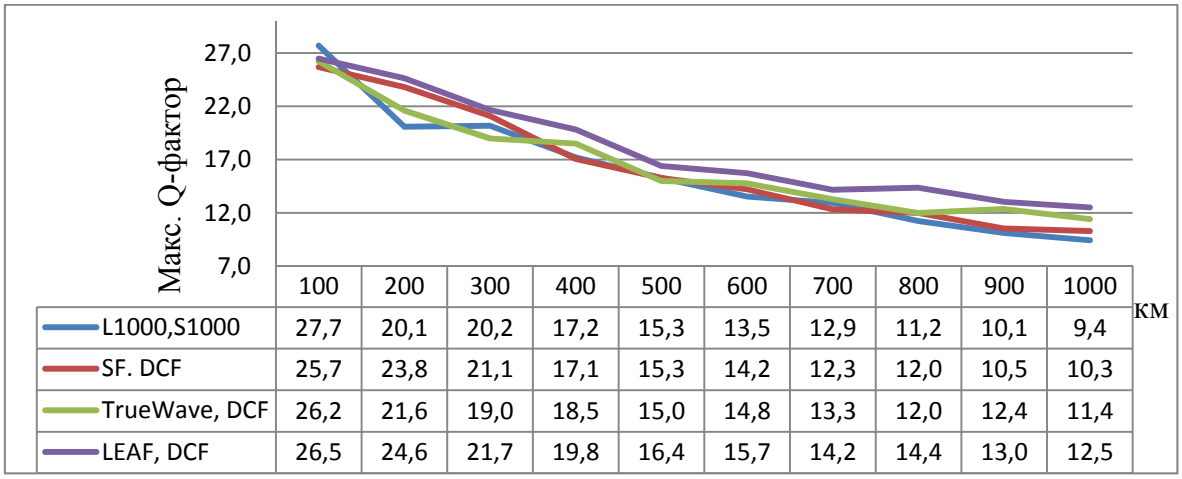


Рис. 3. Изменения среднего *Q*-фактора с увеличением длины линии при АМ и кодировании RZ50



	100	200	300	400	500	600	700	800	900	1000 км
L1000,S1000	27,7	20,1	20,2	17,2	15,3	13,5	12,9	11,2	10,1	9,4
SF. DCF	25,7	23,8	21,1	17,1	15,3	14,2	12,3	12,0	10,5	10,3
TrueWave, DCF	26,2	21,6	19,0	18,5	15,0	14,8	13,3	12,0	12,4	11,4
LEAF, DCF	26,5	24,6	21,7	19,8	16,4	15,7	14,2	14,4	13,0	12,5

Рис. 4. Изменения среднего *Q*-фактора с увеличением длины линии при АМ и кодировании NRZ

Результаты исследований показывают, что для одного усилительного участка (УУ) значение *Q*-фактора максимально для кода RZ-50 и комбинации ОВ L1000 (S1000). С увеличением количества УУ значение *Q*-фактора уменьшается, сохраняя, однако достаточно большую величину на расстоянии 1000 км для кодов NRZ и RZ-33.

На рис. 5 показана схема моделирования 4-х канальной ВОСС (DWDM) с бинарной ФМ (DPSK), которая имеет такой же линейный тракт, как и на рис. 1. При моделировании использовалась ФМ с кодированием RZ-33. Для преобразования бинарной ФМ в АМ используется оптическая схема включающая интерферометр Маха-Цендера, в одно плечо которого включается устройство задержки на один тактовый интервал.

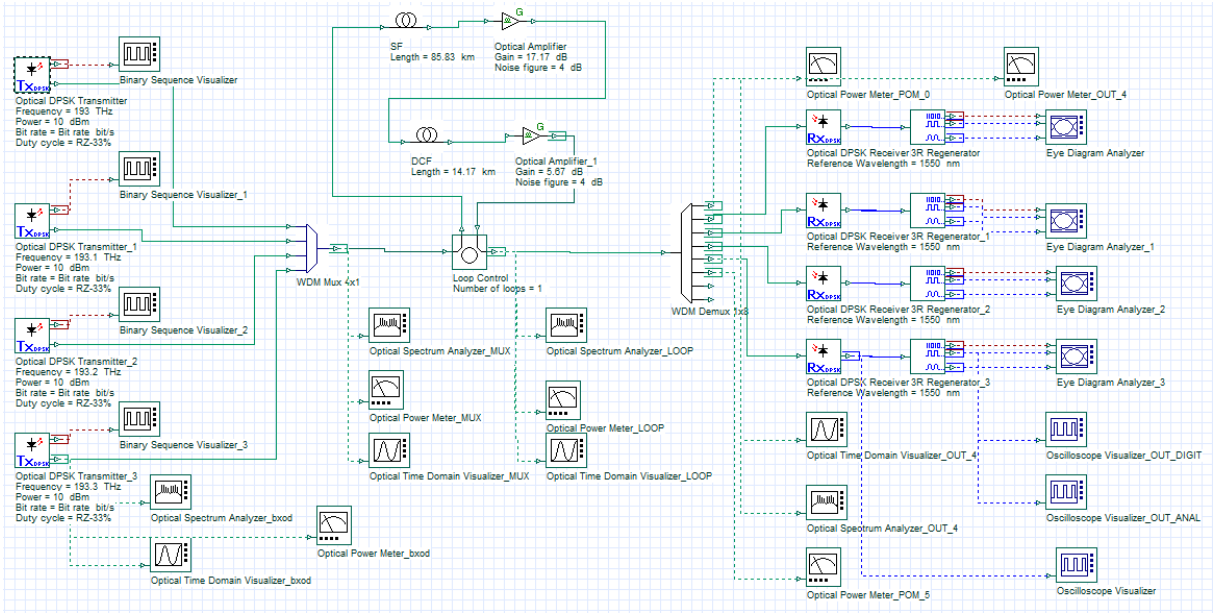
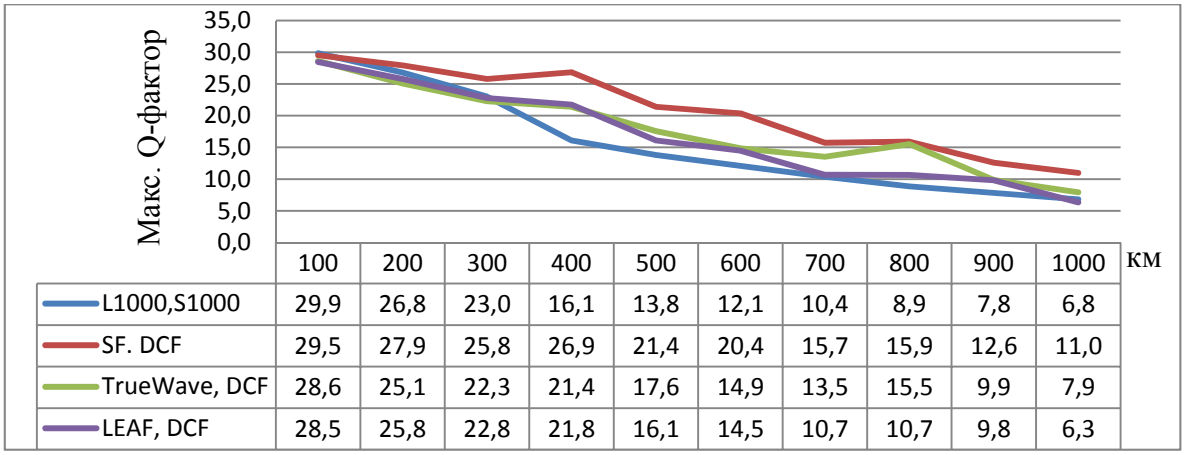


Рис. 5. Схема моделирования ВОСС с ФМ и DWDM

Результаты моделирования ВОСС с модуляцией *DPSK* и кодированием RZ-33 приведены на рис. 6.



	100	200	300	400	500	600	700	800	900	1000 км
L1000,S1000	29,9	26,8	23,0	16,1	13,8	12,1	10,4	8,9	7,8	6,8
SF. DCF	29,5	27,9	25,8	26,9	21,4	20,4	15,7	15,9	12,6	11,0
TrueWave, DCF	28,6	25,1	22,3	21,4	17,6	14,9	13,5	15,5	9,9	7,9
LEAF, DCF	28,5	25,8	22,8	21,8	16,1	14,5	10,7	10,7	9,8	6,3

Рис. 6. Изменения среднего *Q*-фактора с увеличением длины линии при бинарной ФМ (DPSK) с кодировании RZ-33

Результаты моделирования не показали явного преимущества ВОСС с ФМ по качеству связи.

Авторы будут продолжать начатые исследования и сравнительный анализ ВОСС с энергетическим и когерентным приемом, расширяя диапазон скоростей передачи, видов модуляции и кодирования.

Список используемых источников

1. Листвин В. Н., Трещиков В. Н. DWDM системы. М. : Наука, 2013. 300 с.
2. URL: www.corning.com/opticalfiber
3. URL: www.fujikura.co.jp/

УДК 621.391

ОБЗОР КЛЮЧЕВЫХ ВОЗМОЖНОСТЕЙ ПРОТОКОЛА QUIC

В. Ю. Гойхман, А. В. Масюкайте

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

Всемирно известная компания Google разработала новый протокол QUIC, который объединяет в себе преимущества HTTP/2, TCP и TLS. В качестве транспорта

используется протокол UDP. Работа поверх UDP позволяет ускорить выполнение операций в браузере в несколько раз, по сравнению с использованием традиционных технологий. В статье рассмотрены важные преимущества протокола QUIC и основы его реализации.

QUIC, Google, протокол.

QUIC (сокр. от англ. *Quick UDP Internet Connections*) – новый экспериментальный интернет-протокол, разработанный Google.

QUIC применяет современные механизмы, которые делают его привлекательным универсальным транспортом: обеспечивает мультиплексирование и управление потоком, эквивалентное HTTP/2, по безопасности не уступает протоколу шифрования TLS, а также аналогичен TCP по семантике соединения, надежности и контролю перегрузок [1].

Наглядно позиция протокола QUIC в соответствии с уровнями модели OSI показана на рис. 1.

Важной задачей QUIC является создание быстрого транспорта за счет сокращения циклов отправки-приёма сообщений (информирования удаленной стороны), для этого в протоколе должны быть убраны избыточные изменения в TCP и TLS, которым свойственны длинные циклы итерации (в том числе, трехсторонние «рукопожатия»).

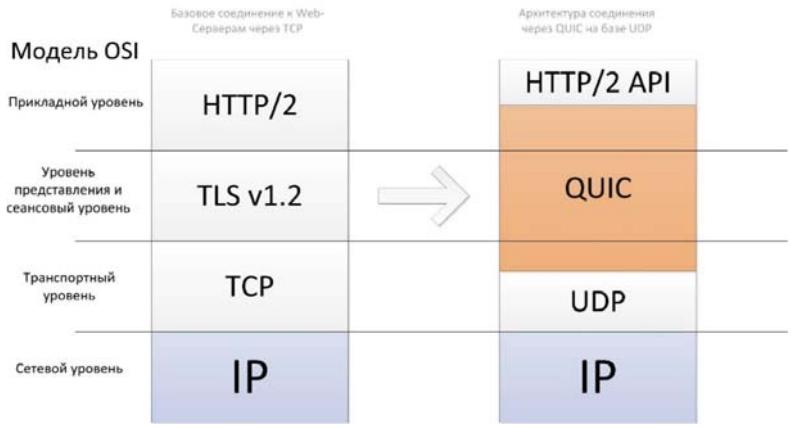


Рис. 1. Определение протокола QUIC в соответствии с моделью OSI

Основные возможности QUIC

Ключевыми возможностями и преимуществами протокола являются следующие [2]:

1) Значительное сокращение времени установления соединения.

QUIC не требует постоянного выполнения процедуры квитирования перед отправкой полезной нагрузки, в отличие от TCP + TLS соединения, которому требуется для установления сеанса от 1 до 3 циклов.

Первый раз, когда клиент QUIC подключается к серверу, он должен выполнить 1-цикл рукопожатия, чтобы получить необходимую информацию для завершения рукопожатия. Клиент отправляет пустые сообщения CHLO (*empty*), сервер посылает отказ (REJ-*reject*) с информацией, которую клиент должен направить в следующем действии (запрос за 1 цикл всей необходимой информации сразу). Эта информация включает в себя маркер адреса источника, используемый для проверки IP-клиента на последующем CHLO (клиентского приветствия) и все необходимые серверные сертификаты. В следующий раз, когда клиент отправляет CHLO серверу, он может использовать кэшированные учетные данные из предыдущего соединения, чтобы немедленно посылать зашифрованные запросы к серверу [3].

2) Улучшенное гибкое управление перегрузками.

QUIC имеет расширенный контроль перегрузки, и предоставляет более обширную информацию для алгоритма управления перегрузкой, чем TCP. В текущая реализация QUIC использует перераспределение TCP Cubic; но в настоящее время разработчики экспериментируют с альтернативными подходами [1].

3) Мультиплексирование без блокировки начала очереди (параллельное мультиплексирование потоков от приложений).

При использовании TCP-соединении большим недостатком является блокировка начала очереди (*Head-of-line blocking*), поскольку крайне важна обработка пакетов в правильном порядке. Протокол QUIC решает данную задачу путем использования в качестве транспорта протокола UDP, который не требует соблюдения порядка обработки принимаемых пакетов [3].

Поскольку QUIC изначально разработан для мультиплексирования, то потерянные пакеты переноса данных преимущественно влияют на один конкретный поток, а не на все потоки соединения (рис. 2). Каждый поток кадров по прибытию может быть немедленно отправлен в этот поток (групповой мультиплексированный поток) так, что потоки без потерь пакетов могут быть повторно собраны и переданы дальше к приложению [2].

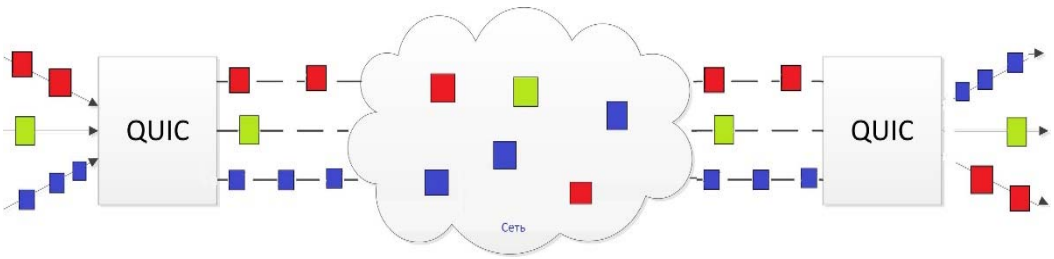


Рис. 2. Мультиплексирование в QUIC

4) Аутентификация и шифрование заголовка и полезной нагрузки – прямое исправление ошибок FEC.

Для того, чтобы восстановить потерянные пакеты, не дожидаясь повторной передачи, QUIC в настоящее время использует простой логический оператор XOR на основе схемы FEC. Каждый пересылаемый пакет содержит в себе некоторое количество данных других пакетов, что позволяет реконструировать любой потерянный пакет по данным соседних пакетов, без необходимости запрашивать переотправку потерянного пакета и дожидаться его содержимого. Это, по сути, реализация RAID 5 на сетевом уровне.

5) Миграция соединения.

Смена IP-адреса или порта не влияет на соединение, не происходит разрыв соединения, удобен при переходе с одной сети в другую. Соединения TCP определяются по 4 полям: IP-адреса источника (*source IP address*), порт источника (*source port*), IP-адрес назначения (*destination IP address*) и порт назначения (*destination port*). Хорошо известной проблемой TCP является то, что соединения прерываются после изменения IP-адреса (например, за счет перехода от Wi-Fi к сотовой связи) или изменения номера порта. Соединения QUIC идентифицируют 64-битовый идентификатор подключения (Connection ID, CID), генерируемый случайным образом клиентом. За счет этого не происходит разрывов соединения при изменении указанных параметров.

QUIC также обеспечивает автоматическую криптографическую проверку мигрирующего клиента, так как клиент продолжает использовать тот же ключ сеанса для шифрования и дешифрования пакетов. Для обеспечения безопасности используется протокол QUIC crypto, который является частью протокола QUIC, обеспечивающей безопасность соединения. Данный протокол не имеет будущего и используется временно, в дальнейшем должен быть заменен на TLS 1.3 [1].

В текущем QUIC crypto, когда клиент собирает информацию о сервере, он может установить зашифрованное соединение без круговой задержки (*round trips*). В отличие от TLS, который устанавливает, по меньшей мере, тройное рукопожатие TCP. Рукопожатие QUIC должно быть примерно в 5 раз эффективнее, чем аналогичное соединение TLS (2048-bit RSA) и с более высоким уровнем безопасности.

Типы и форматы пакета QUIC

QUIC имеет четыре типа пакетов [2]:

1. Пакеты согласования версии (*Version Negotiation Packets*).

2. Пакеты кадров (*Frame Packets*): пакеты для создания соединения, обмена сообщениями.

3. FEC пакеты (*FEC Packets*), для восстановления потерянных или поврежденных от ошибок пакетов.

4. Пакеты открытого сброса, пример пакета: PUBLIC_RESET (*Public Reset Packets*).

Все пакеты QUIC должны быть определенного размера, заданного MTU, для того, чтобы избежать IP фрагментации. На данный момент в QUIC реализован максимальный размер пакетов (MTU – *maximum transport unit,* max кол-во передаваемых байт на канальном уровне) 1350 байт для IPv6 и 1370 для IPv4.

Общий заголовок пакета QUIC

Все пакеты QUIC в соединении начинаются с общего заголовка размером от 2 до 21 байт.

Общий формат заголовка выглядит следующим образом (рис. 3).

Пакеты QUIC аутентифицированы и зашифрованы. Первая часть заголовка до порядкового номера является аутентифицированной, но не в шифрованном виде, а остальная часть пакета, начиная с поля Private Flags (закрытые флаги) – зашифрована.

Рис. 3. Формат пакета QUIC

Заключение

QUIC основан на мультиплексировании нескольких потоков данных между двумя компьютерами, является функциональным эквивалентом TCP+TLS+HTTP/2, но реализованным поверх UDP.

В настоящее время QUIC только частично реализован в браузере Chrome, но в ближайшее время разработчики планируют полностью перевести браузер на использование данного протокола.

Список используемых источников

1. QUIC: A UDP-Based Multiplexed and Secure Transport [Электронный ресурс]. Режим доступа: https://tools.ietf.org/html/draft-ietf-quic-transport-08

2. The Chromium Projects [Электронный ресурс]. Режим доступа: https://www.chromium.org/quic

3. Протокол QUIC: переход Web от TCP к UDP [Электронный ресурс]. Режим доступа: https://habrahabr.ru/company/infopulse/blog/315172/

УДК 004

РАЗРАБОТКА ЗАЩИЩЕННОЙ СИСТЕМЫ ГОЛОСОВАНИЯ НА БАЗЕ ТЕХНОЛОГИИ BLOCKCHAIN ДЛЯ СПБГУТ

В. Ю. Гойхман, А. В. Помогалова

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

Технология Blockchain набирает все большую популярность, расширяя область собственной применяемости. Изначально технология разрабатывалась как финансовая система и имела довольно узкое направление развития. С разработкой и запуском программной платформы Ethereum взгляд на технологию кардинально изменился, позволяя использовать ее в совершенно новых областях, таких как разнообразные децентрализованные приложения или система голосования, разработке которой и посвящена данная работа.

Blockchain, распределенный реестр, умные контракты, Ethereum, система голосования.

С каждым днем активность использования технологии Blockchain возрастает. Такой рост обусловлен не только перспективностью технологии в области финансов, но также функциональностью программных объектов, в основе которых используется эта технология. Настоящий прорыв был совершен Виталиком Бутериным и его командой разработчиков, запустивших программную платформу Ethereum.

Сеть Ethereum и ее компоненты

Программная платформа Ethereum – открытая программная среда, основанная на технологии Blockchain и работающая на базе умных контрактов, предназначенных для запуска различных децентрализованных приложений. На ее основе были спроектированы также тестовые сети, позволяющие имитировать работу реальной сети Ethereum без финансовых затрат.

Умный контракт – это программный код, созданный для организации обмена деньгами, какими-либо ценностями, контентом, который после записи в Blockchain-сеть исполняется автоматически при наступлении условий, описанных в программном коде.

Такой подход позволил отойти от узкой области финансов и разрабатывать приложения другой направленности. В качестве примера разносто-

ронности применения технологии Blockchain нами была разработана система голосования для Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича (СПбГУТ).

Логика работы созданной системы голосования

Логика разработанной системы голосования заключается в следующем: каждый студент имеет личный электронный кошелек, который может являться идентификатором голосующего. На счету каждого кошелька лежит 1 «голос» – токен стандарта ERC20 [1]. Каждый кандидат (предмет голосования) также имеет электронный уникальный кошелек. Голосующие знают адреса (публичные ключи) кошельков кандидатов и переводят свой голос на счет того кандидата, кому отдают свое предпочтение. Итоги голосования наглядно видно по итоговому балансу на счетах кандидатов.

Плюсами такой системы является анонимность (если голосующий сам не покажет другим участникам публичный ключ своего кошелька), честность (количество выпускаемых токенов соответствует количеству голосующих, а перевод токенов на другие адреса кошельков программно ограничен), технологичность и функциональность (при проведении нового голосования выпускаются новые уникальные токены с новым или же с уже использованным названием, в зависимости от необходимости и типа голосования).

В случае нашей системы голосования были разработаны токены GUT (полное название – *BonchToken*) стандарта ERC20, поддерживающие только функцию «transfer», то есть функцию перевода, тиражом 1000 токенов.

Под токеном чаще всего подразумевают единицу учета, которую используют для представления баланса в некотором активе. Токены могут представлять собой акции компании, отображать ценность чего-либо, являться криптовалютой компании и др. В нашем случае токены – это «голоса» участников.

Разработанный умный контракт состоит из описания токена, его функций, отвечает за автоматическое распределение токенов по адресам. Написан на языке программирования Solidity, который является наиболее популярным среди разработчиков умных контрактов.

Результаты тестирования работоспособности разработанного умного контракта

Итоговый программный проект умного контракта должен состоять из файлов, описывающих логику и составляющие системы, файлов для ин-

теграции в сеть Ethereum (в случае нашего проекта – в тестовую сеть *Ropsten*), а также файлы для тестирования контракта перед его запуском в эксплуатацию.

Тестирование программного кода крайне необходимо, так как после записи умного контракта в сеть изменить его будет невозможно. Мы использовали Framework Truffle – среду разработки и тестирования кода умных контрактов, с помощью которой также возможна запись умного контракта в Blockchain-сеть Ethereum [2].

В процессе тестирования была проверена функциональность контракта, возможность записи его в сеть Ethereum и тестовые сети, функция перевода токенов, функции проверки адреса и баланса контракта. После успешного тестирования умный контракт был записан в тестовой сети Ropsten. Данная сеть была разработана одной из первых и имеет идентичную функциональность, что и сеть Ethereum, что и послужило причиной выбора именно этой тестовой сети.

Электронные кошельки, как аналог электронной подписи

Далее было создано 10 электронных кошельков, 4 из которых отводились для кандидатов, а 6 использовались, как кошельки голосующих. Для создания кошельков использовался онлайн-сервис https://www.myetherwallet.com/, который генерирует публичный и приватный ключи и прочие файлы, необходимые для работы в разных сервисах.

Еще одним необходимым для голосования условием является наличие плагина MetaMask (расширение для браузеров Chrome, FireFox: https://metamask.io/). Дело в том, что для произведения любых транзакций (перевода токенов в том числе) необходимо иметь синхронизированную с Blockchain базу данных (его копию), что очень затратно в плане ресурсов памяти (50 Гб для основной сети и 11 Гб для тестовой сети). Но использование плагина MetaMask позволяет не иметь локальную синхронизированную копию Blockchain, так как плагин обращается к своим серверам, которые имеют актуальную копию (все ключи хранятся локально, что позволяет повысить уровень безопасности).

На этом этапе разработка умного контракта системы голосования может считаться завершенной, так как разработаны и созданы следующие объекты: электронные кошельки с токенами, сам код умного контракта, протестированный и записанный в сеть Ropsten, а также установлено расширение MetaMask. С технической точки зрения пользователь уже способен производить транзакции и принимать участие в голосовании, но это может вызвать затруднения у среднестатистического пользователя. Чтобы избежать таких проблем нами был разработан Web-интерфейс системы голосования, показанный на рисунке.

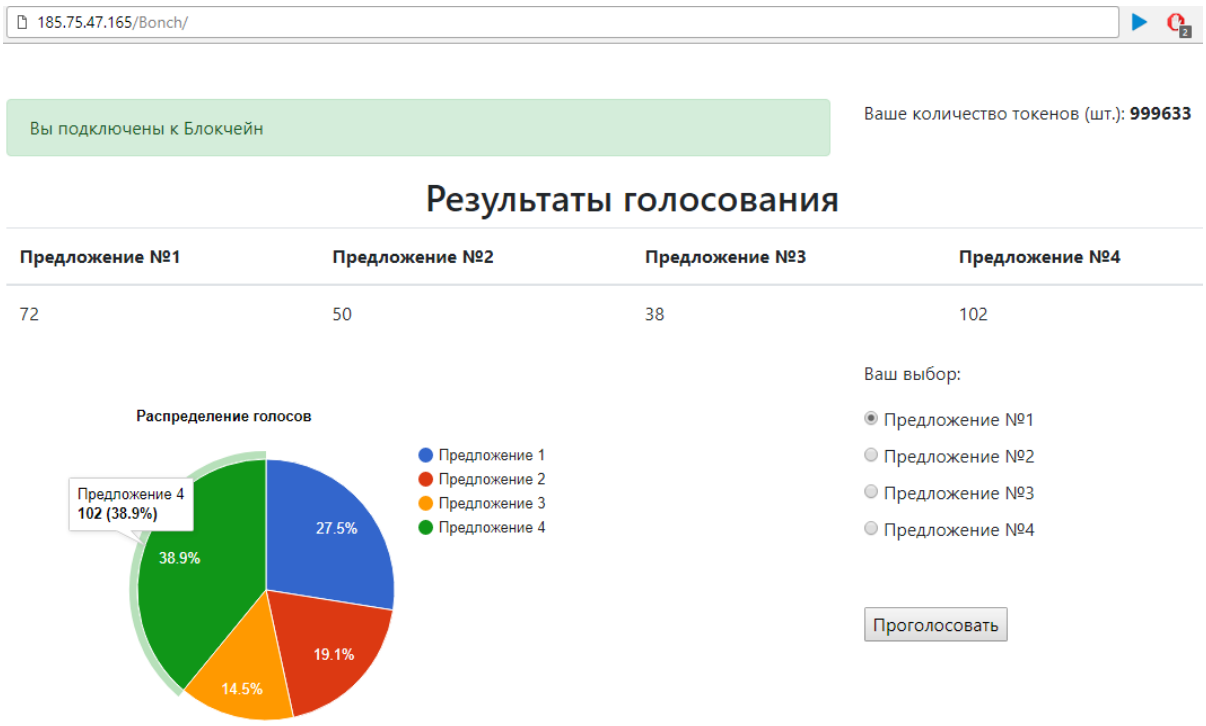


Рисунок. Web-интерфейс разработанной системы голосования

Также стоит помнить, что каждая транзакция в сети Ethereum является платной, что также может быть использовано для обеспечения защищенности голосования. Оплата транзакций происходит с помощью газа – меры того, сколько процессорной мощности потребует программа. Если ограничить количество тестового Эфира (монет (*coin*), в которых выражается стоимость газа) на балансе голосующих, то повторный перевод токенов не будет произведен в связи с недостатком средств. С коммерческой точки зрения стоимость одной транзакции, которая будет обработана в течение 1 минуты, составит не более 5 рублей (по состоянию курса эфира к рублю на 15.03.2018).

Выводы

Разработанная система голосования подтверждает на своем примере практическую возможность ввода в эксплуатацию подобных систем голосования и делает использование технологии Blockchain уместным, так как записи перевода голосов являются общедоступными и неизменяемыми. Любой желающий может проверить список транзакций с помощью сервиса https://etherscan.io/, убедиться, что токены не переводятся ни на чей иной счет, кроме адресов кандидатов, тем самым уничтожая проблемы недоверия, свойственные мероприятиям, подобных голосованию.

Список используемых источников

1. Группа разработчиков EIP. Стандарт ERC20 [Электронный ресурс] // GitHub, Inc 2018. URL: https://github.com/ethereum/EIPs/blob/master/EIPS/eip-20.md (дата обращения 17.03.2018).

2. Truffle Framework. Документация, руководство пользователя [Электронный ресурс] // Consensys 2017. URL: http://truffleframework.com/docs/ (дата обращения 18.03.2018).

УДК 65.01

ТЕХНОЛОГИЯ BLOCKCHAIN – НОВОЕ ПОКОЛЕНИЕ СЕТИ ИНТЕРНЕТ: ИНТЕРНЕТ ЦЕННОСТЕЙ

В. Ю. Гойхман, А. В. Помогалова

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

Централизованные узлы управления – крайне уязвимое место в любой системе. На помощь в таких условиях приходят децентрализованные системы, которые не имеют центрального узла управления, тем самым предотвращая атаку на центр управления с риском потери всех данных. Технология Blockchain позволяет не только перейти к децентрализованности, но также взглянуть на Интернет с новой стороны. Защищенность, открытость, распространенность – три главных преимущества, соединенных вместе в одной технологии, получившей название Интернет Ценностей (Internet of Value: https://ripple.com/insights/the-internet-of-value-what-it-means-and-how-it-benefits-everyone/).

Blockchain, Internet of Value, распределенный реестр, умные контракты, Ethereum.

В настоящее время остро стоит вопрос перехода от централизованных серверов и централизации в целом к децентрализованным базам данных, серверам, приложениям, поскольку наличие центрального управляющего узла является слишком ненадежным элементом любой сети.

Общие понятия технологии Blockchain

Технология Blockchain является одним из шагов перехода к децентрализации, что и делает ее достаточно популярной и потенциально выигрышной технологией [1]. Технология Blockchain (дословно «цепь блоков») – это сеть с распределенной базой данных (реестром). Данные записываются в блоки и выстраиваются по мере заполнения блоков цепочкой. База данных не хранится в каком-либо одном месте, что значит, что она общедоступна

и позволяет легко проверять совершенные действия любым пользователем. Эти характеристики делают ее защищенной от взлома и изменения уже записанных данных. Одна и та же копия базы данных одновременно размещена на сотнях компьютеров, это гарантирует, что информация не будет подделана или удалена.

Различают два основных типа сетей, построенных на технологии Blockchain: публичные и частные.

Публичная Blockchain-сеть является открытой и общедоступной, имеет открытый исходный код, список произведенных транзакций доступен каждому, любой человек может стать участником и произвести транзакцию. Примеры: Bitcoin, Ethereum, Litecoin (https://myfin.by/crypto-rates).

Частная Blockchain-сеть – закрытая сеть, с ограниченным уровнем допуска. Проведение транзакций в такой сети доступно строго определенному кругу лиц, а доступ к чтению произведенных транзакций может быть ограничен, либо открыт в зависимости от решения владельцев. Примеры: MONAX (monax.io), Multichain (www.multichain.com).

Безопасность и неподдельность технологии Blockchain заключается не только в децентрализованности. Подделать записи в блоке цепочки практически невозможно. Как уже описывалось, данные записываются в блоки. Для безопасности каждая запись хэшируется, после чего все записи складываются по алгоритму дерева Меркла, после множественных сложений хэшей записей остается один итоговый хэш, блок считается завершенным, но еще не записанным в общую Blockchain-сеть. Так как в сети находятся тысячи компьютеров, есть вероятность, что несколько машин одновременно закончат формирование блока и тогда будет невозможно решить, чей блок поставить в очереди первым. В связи с этим все машины, заполнившие блок транзакциями, решают одинаковую задачу – ищут такое число «nonce», после сложения, с которым итоговый хэш примет значения с 10 нулями в начале. Математиками доказано, что найти такое значение нельзя никаким иным способом, кроме перебора, а значит, что ничто не влияет на результат, кроме теории вероятности. Процесс поиска числа «nonce» носит название майнинга. Майнеры – люди, поддерживающие Blockchain-сеть в работоспособном состоянии, занимающиеся записью блоков в цепь.

В качестве вознаграждения за потраченную вычислительную мощность майнеры получают определенное количество биткоинов или других монет, в зависимости от Blockchain-сети, за каждый записанный блок. Кроме того, после записи некоторых транзакций майнер получает комиссию за запись, если автор транзакции желает, чтобы она была записана в кратчайший срок. Запись блока в цепь происходит раз в 10–12 минут.

Данный алгоритм поиска блоков и записи их в цепь называется Proof of Work (дословно: доказательство работы). Он используется в качестве

средства достижения консенсуса, то есть общего решения о том, какая версия Blockchain является корректной. Кроме алгоритма доказательства работы существует множество алгоритмов принятия консенсуса: PoS (доказательство доли владения), LPoS (арендованное подтверждение доли), DPoS (делегирование подтверждения доли), PoI (подтверждение важности), PoA (доказательство активности), PoC (доказательство вместимости).

Наиболее популярной и применимой в среде Blockchain-сетей является PoS (*Proof of Stake*). В данном алгоритме большую вероятность получить право записи блока в цепь имеет узел с большим балансом монет (количеством токенов) на своем счету.

Вышеупомянутый узел (*node*) – часть архитектуры Blockchain-сети. Это компьютер, подключенный к сети Blockchain с использованием клиента, который выполняет задачу проверки и ретрансляции транзакций, получает копию всех цепей блоков, которые автоматически загружается при подсоединении к сети. В процессе записи блоков в цепь каждый узел, который получил право записи блока в цепь, к итоговому хэшу также добавляет адрес своего электронного кошелька, куда будет переведено его вознаграждение.

Электронный кошелек (*wallet*) – это своего рода аналог электронной подписи. Он состоит из приватного и публичного ключей. Публичный ключ – номер кошелька, его адрес. Пользователи, знающие приватный ключ могут переводить монеты или токены на адрес кошелька. Приватный ключ – полный доступ к управлению кошельком и его содержимым. Приватный ключ хранится не в сети, а на самой машине, чтобы злоумышленники не могли получить к нему доступ по сети. Способов создания кошелька несколько – можно воспользоваться онлайн-сервисами, либо произвести генерацию ключей на компьютере. На балансе кошелька могут находиться как различные криптовалюты, так и токены.

Криптовалюта – это виртуальные деньги, не имеющие физического выражения, содержащие закодированную информацию. Единицей такой валюты является монета (coin). Особенность валюты состоит в том, что она защищена от подделки, так как в ней зашифрованы данные, не подлежащие дублированию.

Токен – это единица учета, используемая для представления цифрового баланса в некотором активе. Токены могут представлять акции компании, отображать какую-то ценность в рамках бизнес-модели онлайн-платформы (репутация, рейтинг, опыт), цифровые обязательства на реальные товары или услуги.

Биткоин – децентрализованная цифровая валюта, работающая только в сети интернет, основанная на математических вычислениях, чтобы обмен

монетами происходил без централизованного контроля и с малыми задержками. Количество биткоинов в сети ограничено 21 миллионом. Биткоин может дробиться на крайне малые составляющие, так как это цифровая валюта.

Кроме биткоина появилось множество других криптовалют, таких как: ETH (*Ethereum*), BCH (*Bitcoin Cash*), LTC (*Litecoin*) и др.

Потенциал технологии Blockchain

В связи с тем, что биткоин позволяет производить только финансовые операции, что делает применение технологии Blockchain достаточно ограниченной, Виталик Бутерин (https://wsjournal.ru/vitalik-buterin-sovremennyj-kriptobog/) с командой разработчиков запустил программную платформу Ethereum (https://www.ethereum.org/). Как и Bitcoin, Ethereum является открытой Blockchain сетью. Но, несмотря на мелкие технические различия и валюту, используемую в Ethereum (Эфиры), главным отличием между ними являются преследуемые цели и возможности [2]. Если Bitcoin работает как равноправная электронная система наличных денег, позволяющая производить финансовые онлайн операции в криптовалюте Bitcoin, Ethereum фокусируется на запуске программного кода любых децентрализованных приложений посредством умных контрактов.

Умный контракт представляет собой программный код, написанный на языке программирования (чаще всего *Solidity*), который разработчик загружает в сеть Blockchain. Обычно они имеют структуру “if/then”, т. е. при осуществлении определенных условий, программа выполняет условия контракта. Например, контракт загружен в сеть на месяц раньше, чем необходимо заказчику и дожидается наступления необходимой даты для перехода в активную стадию выполнения.

Каждая программа на платформе Ethereum использует определенный объем вычислительной мощности, так как программа управляется узлами (*nodes*), что приводит к избыточной активности, которую необходимо исключить. С этой целью используется газ (*gas*), в единицах которого приходят счета за каждый умный контракт. Газ – мера того, сколько процессорной мощности потребует программа, с возрастанием потребности в газе, возрастает и количество Эфира (Ether), который необходимо потратить. Таким образом, исключается злонамеренное использование вычислительной мощности этой сети.

Биткоин также может запускать умные контракты, но его программный язык является достаточно примитивным и не позволяет прописать даже цикл, что делает использование умных контрактов крайне непродуктивным и малоэффективным.

Безусловно, у подобных контрактов существуют и свои недостатки, проявляющиеся в человеческом факторе – если программист допустит

ошибку в контракте, то нет никаких гарантий корректного выполнения контракта сетью Ethereum. Однажды записывая умный контракт в сеть уже нет возможности удалить его, либо внести изменения, исправить ошибки, единственный способ – написать новый контракт.

Одним из наиболее ярких примеров применения умных контрактов может служить сфера сделок. Пример: сторона А впервые работает со стороной В и, следовательно, не имеет к ней никакого доверия. Между ними находится посредник – сторона С, которой обе предыдущие доверяют. Сторона С следит, чтобы В выполнила свою часть обязательств и условий, описанных в заключенных между А и В соглашениях, чтобы все происходило справедливо, и В получила свое вознаграждение, а сторона А объективно оценивала результат работы стороны В. При использовании умных контрактов сторона С просто исчезает, так как в ней нет необходимости. Умный контракт нельзя изменить, он не является заинтересованной стороной, что позитивно сказывается на итоговом решении, принятом на основании фактов.

Еще одним ярким примером может являться интеграция технологии Blockchain в сферу Интернета вещей. Например, поставка товара, изначально описанного и учтенного в базе данных Blockchain. По мере следования поставки идут записи в реестр из каждой точки о количестве товара и времени его поставки в тот или иной пункт. Такая система позволяет отследить, чтобы весь товар был доставлен и все условия были соблюдены.

Отдельного внимания заслуживает процесс распространения технологии Blockchain в различных странах. Часть стран осознало силу и перспективность технологии, и активно внедряют ее, другие же наоборот относятся крайне недоверчиво и придерживаются мнения о необходимости запрета интеграции технологии в сферы финансов и управления. Например, в Российской Федерации в ближайшее время планируется принятие законопроекта, регулирующее использование технологии Blockchain. Но процесс повсеместного распространения остановить не представляется возможным, капитализация рынка криптовалют приближается к таким финансовым гигантам, как Apple, в то время как промежуток времени активного развития сократился на десятки лет (Apple понадобилось 42 года, в то время как Биткоину 9 лет). Развитие технологии идет неоднородно и даже хаотично, а скорость и масштабы ее проникновения в сферы жизни крайне велики.

Список используемых источников

1. Tapscott D., Tapscott A. Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World. M., 2017. 324 с.

2. Любимова О. Создатель Ethereum: «Блокчейн поможет искоренить коррупцию» [Электронный ресурс] // Inc. 2017. URL: https://incrussia.ru/understand/sozdatel-ethereum-vitalik-buterin-blokcheyn-pomozhet-iskorenit-korruptsiyu/ (дата обращения 15.03.2018).

УДК 621.372.88

УПРАВЛЕНИЕ ТЕЛЕКОММУНИКАЦИЯМИ КАК ТЕХНИЧЕСКАЯ СИСТЕМА

А. Б. Гольдштейн

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

Целью данной работы является обсуждение инженерных и научных проблем управления перспективными телекоммуникационными сетями NGN/IMS и пост-NGN.

OSS/BSS, пост-NGN, мультиагентные системы, теория массового обслуживания.

Управление телекоммуникационными сетями

Управление сетями связи – согласно закону «О связи» – это совокупность организационно-технических мероприятий, направленных на обеспечение безотказного и согласованного функционирования сети связи, в том числе регулирование трафика, наблюдение и контроль состояния сетевых элементов, каналов транспортной сети и взаимодействий узлов, а также управление работой приложений и предоставлением новых инфокоммуникационных услуг [1].

При переводе на инженерный язык это означает, что системы управления сетями связи предназначены для поддержки операционной деятельности телекоммуникационных Операторов. В их состав, прежде всего, входят системы технического учета сетевых ресурсов NRI (*Network Resource Inventory*), системы Fault Management (сбора и обработки аварийных сообщений), Trouble Ticketing (устранения неисправностей разного рода), Fraud Management (борьбы с мошенничеством), Performance Management (управления производительностью), Order Management (управление заказами на подключение и предоставление услуг) и др. входящие в симбиоз двух фундаментальных комплексных систем: системы поддержки операций (OSS) и системы поддержки бизнеса (BSS).

Системы поддержки операций охватывают набор бизнес-процессов, которые требуются телекоммуникационному Оператору для обеспечения, мониторинга, анализа и управления телекоммуникационной сетью; для контроля и устранения неисправностей; для организации взаимодействия с пользователя. По сути поддержка операций включает все, подразумеваемое под исторически сложившимся термином *управление сетью связи* – контроль и управление элементами сети.

Системы поддержки бизнеса охватывают технологии, которые необходимы сервис-провайдеру для того, чтобы поддерживать взаимоотношения с клиентами, партнерами и поставщиками.

Граница между поддержкой операций и поддержкой бизнеса размытая: функции поддержки бизнеса являются ориентированным на клиента подмножеством поддержки операций. Процессы поддержки бизнеса, например, получая запрос от клиента на новую услугу, должны перетекать в процессы поддержки операций, чтобы сконфигурировать ресурсы, необходимые для предоставления этой услуги. Системы поддержки поэтому часто обозначаются как системы OSS/BSS.

Эволюция подходов к управлению сетями связи

Первые системы OSS/BSS, как показали исторические изыскания автора[1], были созданы в 1951 г. в английской компании J. Lyons, занимавшейся чаем, мороженым и кондитерскими изделиями. Они включали приложения Inventory, Order Management и т. п. Результаты учета и транзакции сравнивались с планами и бюджетами. Аппаратное обеспечение для этого приложения также было создано в J. Lyons — это была бизнес-версия компьютера EDSAC, разработанного в Кембриджском университете, позже она получила название LEO. В итоге получилась работающая в реальном времени система OSS/BSS с обработкой деловой информации и поддержкой принятия решений, которой многие Операторы позавидовали даже сегодня [2].

Непосредственно в телекоммуникациях системы эксплуатационного программного обеспечения появились в середине 70-х годов прошлого века и были написаны, как правило, на малоизвестных языках программирования типа рекомендованного ITU-T языка CHILL и размещались на специализированных электронных управляющих машинах (ЭУМ), аналогичных большим универсальным ЭВМ (мэйнфреймам). Точно так же, как это имело место в модели интеллектуальной сети IN (*Intelligent Network*) начала 90-х годов прошлого века, такие технологии централизованной технической эксплуатации на мэйнфреймах обусловили создание архитектуры TMN, а затем и более сложных систем OSS/BSS и другие инициативы Telemanagement Forum.

Эволюцию управления сетью связи можно проследить через уже упоминавшиеся в предыдущем параграфе стандарты: модель управления сетью связи OSI, модель управления Интернет, архитектура TMN, модели и стандарты TMF. Цели и характер систем управления изменяются в ходе этой эволюции. На рис. 1 показаны три стадии современной эволюции систем управления телекоммуникационными сетями.

[1] Имеются и другие исторические версии возникновения OSS/BSS

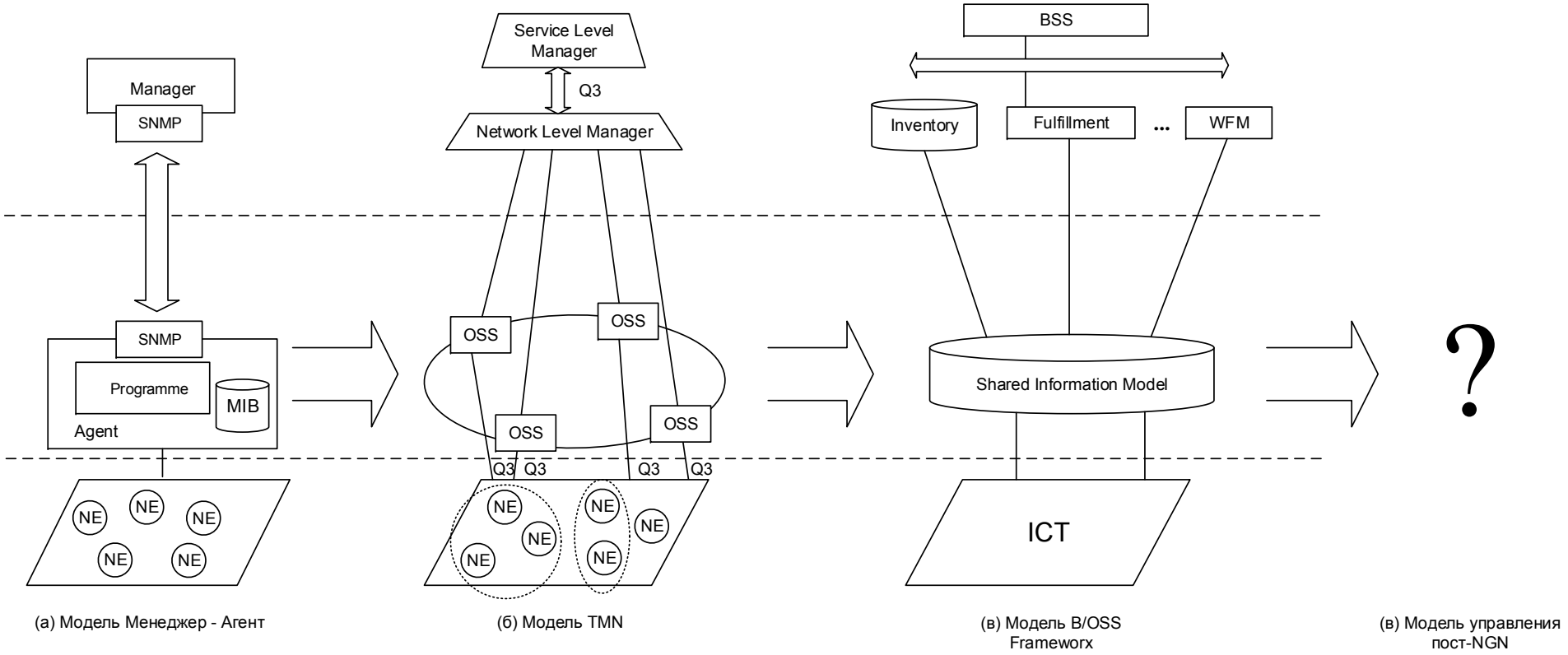


Рис. 1. Эволюция систем управления инфокоммуникациями от простых структур «менеджер – агент» до сложных распределенных структур

Первоначально стандарты OSI, модели IETF и рекомендации ITU-T серии M базировались на концепции Менеджер-Агент, как показано на рис. 1*а*. Управляемый элемент в модели Менеджер-Агент представлен определенным набором информации, которая называется Management Information Base (MIB). В рекомендации M.3010 дано определение концепции Менеджер/Агент и описаны многосторонние отношения между ролями в плане информационного взаимодействия и выполнения. Как кратко сформулировано в [3], Агент *уведомляет*, а Менеджер *управляет.*

Следующая фаза эволюции на рис. 1*б* соответствует дальнейшему развитию концепции TMN и рассмотрена, в частности, в статьях автора [4].

Современная парадигма управления телекоммуникациями

Современная парадигма построения систем управления телекоммуникациями в соответствие с последними разработками TMForum представлен на рис. 1*в*. Эта парадигма глубоко обсуждается в множестве публикаций, включая и ряд статей автора данной диссертации. Ей же соответствуют современные версии OSS/BSS систем ведущих мировых вендоров. Некоторые остающиеся открытыми вопросы таких систем управления исследованы в данной диссертации.

При всей упрощенности представленного на рис. 1 подхода он адекватно отображает этапы эволюции систем управления телекоммуникациями последовательно по сменам парадигм а), б) и в), а затем уводя их и далее вправо за пределы этих трех парадигм на рис. 1, к пока еще не полностью специфицированной парадигме г), о которой ниже.

В контексте общей эволюции сетей пост-NGN с переходом на программно-конфигурируемые сети SDN и виртуализацию сетевых услуг NFV предлагается модель управления телекоммуникациями нового поколения, представленная на рис. 2 (см. ниже). Этот подход может дать отрасли новые возможности развития виртуальных сред и создания новых Операторских приложений в самых разных предметных областях. Перспективы NFV и соответствующих систем OSS/BSS заставляют серьезно задуматься о том, как будет выглядеть и как управляться будущая сеть связи пост-NGN, базирующаяся на технологической сингулярности, где не будет различия между физическим и виртуальным телекоммуникационным оборудованием.

Инженерные применения BI в системе «Аналитика»

В заключительном разделе статьи рассмотрим подробнее вопрос о высокоуровневых задачах поддержки принятия своевременных и обоснованных бизнес-решений, а также отслеживания эффективности автоматизированных бизнес-процессов с помощью систем бизнес-аналитики BI.

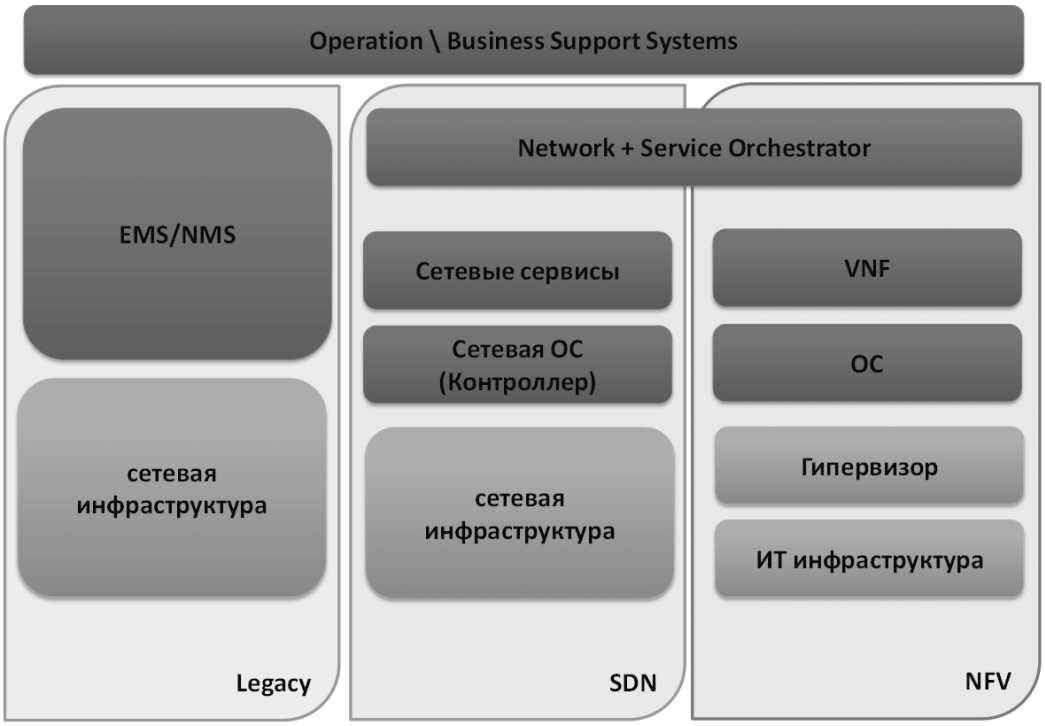


Рис. 2. Обобщённая структура нового OSS/BSS-комплекса сетей пост-NGN

Известно, что массивы данных, хранящиеся в OSS системах, содержат определенное количество полезной информации – иными словами, эти данные хранят в себе знания о каждой области деятельности компании, необходимые руководству высшего и среднего звена. Однако не так просто извлечь знания из массивов «сырых» данных: их объем огромен, хранятся они в разрозненных источниках и имеют различные типы и форматы. Для того чтобы получить эти знания, а также на основе них сделать выводы и прогнозы, требуются специализированные инструменты анализа данных, из которых и строятся системы бизнес-анализа.

Эффективным средством решения таких задач является система «Аналитика», которая может рассматриваться как своего рода натурный эксперимент для теоретической модели на рис. 2.

Система «Аналитика» рассчитывает KPI (ключевые показатели эффективности), которые позволяют оценить состояние каждой области деятельности оператора связи. Такая оценка помогает принимать решения в реальном времени и ориентируясь на актуальные данные. Показатели эффективности можно рассматривать в разных разрезах, сравнивая значения между филиалами, службами, услугами и т.п., быстро и с высокой степенью точности выявляя слабые места в сквозных бизнес-процессах.

Предлагаемая система рассчитывает KPI для таких областей анализа, как служба Service Desk, управление взаимоотношениями с клиентом, управление продуктами, развитие и планирование сети, качество обслуживания и др., а также создает специальные формы просмотра и управления

KPI – дашборды (*dashboards*). Дашборд – это панель управления, на которой можно отслеживать все показатели, интересные в рамках решения тех или иных задач. Дашборды позволяют оценивать текущую ситуацию в рамках той или иной области анализа, например, текущий процент неразрешенных инцидентов, а также позволяют оценивать долгосрочные показатели эффективности деятельности компании в целом, такие как, например, динамика роста клиентской базы, эффективность продуктов, и т. п.

Для решения таких задач в системе «Аналитика» реализованы инструменты класса Data Mining, основное предназначение которых – выявление новых, полезных и ранее неизвестных знаний в большом объеме статистической информации. Например, выявление корреляции между событиями (увеличением количества жалоб на услугу и аварией в определенном районе), выявление нелояльных клиентов, сегментирование клиентской базы на основании сведений о поведении и предпочтениях абонентов – все это задачи инструментов Data Mining.

Помимо информации о текущей ситуации в компании, интерес для руководителя представляет прогноз будущей ситуации. Важнейшим критерием полезности таких прогнозов является точность, поэтому автоматизированный анализ предпочтителен для решения задач прогнозирования. Еще одним аргументом в пользу системы «Аналитика» является ее возможность учитывать одновременно множество факторов, которые могут влиять на прогноз. При построении прогнозов вручную многомерный анализ оказывается затруднительным и неэффективным.

Отслеживая значения показателей эффективности, система «Аналитика» может стоить тренды, показывающие, как значение показателя изменится в будущем при текущей динамике роста/спада, причем тренд может оказаться нелинейным. В случае если значение показателя в ближайшее время выйдет за рамки допустимых значений, система уведомит об этом пользователя, позволяя ему вовремя принять необходимые меры.

К тому же система дает инженерному персоналу инструменты для самостоятельного анализа, которые позволяют ему просматривать многомерные зависимости данных в виде наглядных кросс-таблиц (с возможностями применения сложных фильтров и изменением глубины детализации выводимых данных), диаграмм, гистограмм и графиков. Проанализировав существующие статистические данные, система «Аналитика» может построить предложенные в диссертации модели, которые исследуют характер зависимостей между различными показателями. Построенные модели позволяют персоналу Оператора произвести анализ «что если» и принять решение, перебрав несколько возможных вариантов развития ситуации и выбрав лучший из них.

Для этого система «Аналитика» оснащена такими важными элементами, как хранилище данных (*Data warehouse*), средства трансформации

и очистки данных (ETL) и инструмент для быстрой обработки многомерных данных OLAP. Эти элементы необходимы для того, чтобы процесс анализа данных был быстрым, а результаты анализа – точными и безошибочными.

Представленная на рисунке 3 структура обеспечивает своевременную замену неэффективного тарифа, таргетированные продажи узким клиентским сегментам, оптимизацию структуры технической поддержки, выбор наиболее надежного поставщика оборудования и множество других важных бизнес-решений благодаря предложенным инструментам автоматизированного анализа данных. Таким образом система повышает эффективность деятельности оператора связи, помогая ему выявлять возможные точки утечки дохода и развивать наиболее доходные каналы продаж.

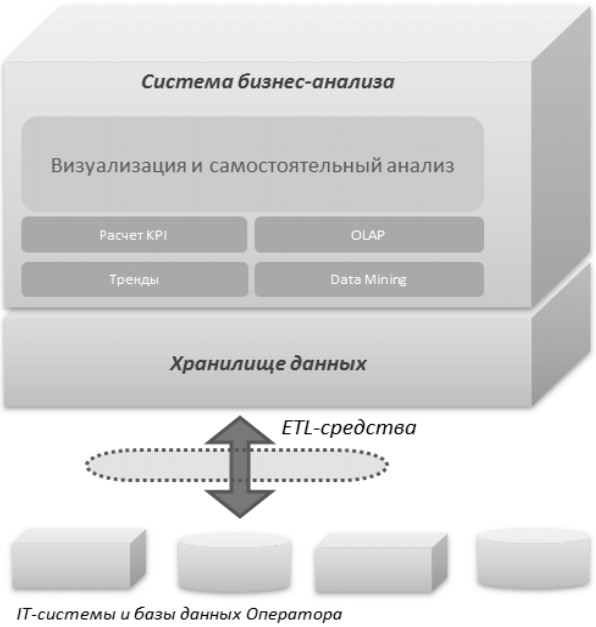


Рис. 3. Структура системы BI

Список используемых источников

1. Гольдштейн Б. С., Кучерявый А. Е. Сети связи пост-NGN. СПб. : БХВ-Петербург, 2013. 160 с.: ил. ISBN 978-5-9775-0900-8.

2. Гласс Р. Креативное программирование 2.0. СПб. : Символ#Плюс, 2009. 352 с. ил. ISBN 978-5-9328-6152-3.

3. Резникова Н. П., Голышко А. В., Булгак В. Б., Демина Е. В. Менеджмент в телекоммуникациях (Серия «Инженерная энциклопедия: Технологии Электронных Коммуникаций»). М. : Эко-Трендз, 2005. 392 с. ISBN 5-88405-065-8.

4. Самуйлов К. Е., Чукарин А. В., Яркина Н. В. Бизнес-процессы и информационные технологии в управлении современной инфокоммуникационной компанией. М. : Альпина Паблишерз, 2015. 511 с. : ил. ISBN 978-5-9614-5272-3.

УДК 004.891.2

АНАЛИЗ ЭФФЕКТИВНОСТИ АНСАМБЛЕВЫХ МЕТОДОВ ПРОГНОЗИРОВАНИЯ ОТТОКА КЛИЕНТОВ

А. Б. Гольдштейн, В. А. Поздняков, М. Ю. Скоринов

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

Отток клиентов – актуальная проблема для всех операторов связи. Для её решения разрабатывается комплекс мер, направленный на определение риска ухода абонентов и их удержание. Для построения эффективной модели прогнозирования – одной из перспективных мер решения проблемы оттока – необходимо предварительно проводить сравнительный анализ доступных методов. В статье приведены результаты сравнения популярных методов ансамблевой группы. Эффективность определена на основе ROC-анализа и набора часто используемых бизнес-метрик.

ансамблевые методы, «случайный лес», бустинг, бэггинг, дерево решений, отток клиентов, прогноз, анализ эффективности, ROC-анализ.

Концепция борьбы с оттоком клиентов содержит целый комплекс мероприятий, таких как квалификация клиентов по склонности к оттоку, выработки сценариев удержания, работы с претензиями и много другого. В статье мы сосредоточимся на процессе прогнозирования оттока клиентов, который по сути сводится к задаче бинарной классификации, имеющей два типа меток классов «1» и «0». Обычно метку «1» присваивают классу клиентов, ушедших от оператора связи, а метку «0» – клиентам, продолжающим взаимодействие с оператором связи. Эту задачу можно решить при помощи методов, которые на основе накопленных (исторических) данных могут сформировать прогноз оттока для обслуживаемых клиентов. Накопленные данные содержат информацию об использовании абонентами услуг связи, которая формирует признаковое пространство, и об их распределении по классам {1, 0}. Одними из наиболее перспективных для данной задачи методов, представляются методы ансамблевой группы.

Основное назначение ансамблевых методов: комбинация нескольких базовых классификаторов таким образом, чтобы улучшить обобщающую способность формируемого прогноза оттока клиентов за счёт уменьшения влияния выбросов в исторических данных.

Обычно ансамблевые методы разделяют на два типа:

1. Усредняющие методы – одновременно и независимо строятся базовые классификаторы, а затем производится усреднение их прогнозов. Таким образом можно снизить дисперсию.

2. Бустинг-методы – последовательно добавляются базовые классификаторы к ансамблю так, чтобы каждый добавляемый уменьшал смещение прогноза, сделанного ансамблем.

Для сравнения выбраны наиболее популярные методы, являющиеся представителями одного из указанных типов, а именно: Boosting (бустинг), Bagging (бэггинг), случайный лес. В связи с тем, что в русском языке пока нет устоявшейся терминологии для названий методов: “Boosting” и “Bagging”, далее будут использоваться термины, применяемые в околотематической среде, а именно: бустинг и бэггинг.

Бэггинг (*Bagging, Bootstrap aggregation*) – усредняющий ансамблевый метод, который строит базовые классификаторы на случайно выбранных подмножествах накопленного множества данных и затем формирует итоговый прогноз оттока клиентов путём усреднения индивидуальных прогнозов базовых классификаторов [1]. В качестве базовых выбираются «сильные» классификаторы, обладающие высокой точностью, например, полные решающие деревья. Выбор подмножества основан на статистическом бутстреп-методе (*bootstrap*), а разбиение накопленного множества производится по экземплярам (абонентам).

Суть бутстрэп-метода заключается в следующем. Пусть имеется выборка X, размер которой n. Из X равномерно (с вероятностью $1/n$) берут n объектов с возвращением. В результате получают новую выборку X_1, размер которой равен n. Повторяя процедуру M раз, можно получить M новых бутстрэп выборок $X_1, X_2, \ldots X_M$ [1]. Получается, что базовый классификатор обучается на одной из M бутстреп выборок.

Случайный лес (*Random Forest*) – усредняющий ансамблевый метод, который объединяет в ансамбль только решающие деревья [2], что обусловлено рядом причин, в числе которых выделяют способность достигать нулевую ошибку на любой выборке и возможность обработки и количественных, и категориальных признаков.

Основное отличие рассматриваемого метода от бэггинга заключается в том, что разбиение исходного признакового пространства производится не только по абонентам, но и по признакам. То есть каждое решающее дерево обучается по одной из выборок, полученных аналогичным бэггингу методом, но в процессе формирования решающего дерева при каждом разделении учитываются не все признаки, а только их часть, выбранная случайным образом. Вследствие этого незначительно увеличивается смещение прогноза оттока клиентов ансамбля, а дисперсия значительно уменьшается относительно прогноза отдельного решающего дерева, построенного по всем признакам.

Итоговый класс для абонента может определяться либо путем мажоритарного голосования базовых классификаторов, либо путем усреднения апостериорных вероятностей принадлежности абонента к конкретному классу [2].

Градиентный бустинг деревьев решений (GTB, *Gradient Tree Boosting*) – ансамблевый бустинг-метод, объединяющий в ансамбль базовые классификаторы, которые последовательно строятся на всем признаковом пространстве [1]. Выделяют ряд отличий от вышеупомянутых методов. Во-первых, в качестве базовых выбираются «слабые» классификаторы, которые незначительно превосходят случайное угадывание. Во-вторых, построение ансамбля осуществляется так, чтобы каждый добавляемый классификатор улучшал результат всего ансамбля. GTB чаще всего строится на регрессионных деревьях решений фиксированной глубины и минимизирует функцию потерь для улучшения результата всего ансамбля. Поэтому GTB часто обозначают GBRT (*Gradient Boosted Regression Trees*). Построенный классификатор способен определять не только класс, но и вероятность принадлежности абонента к классу.

Анализ эффективности методов проводят с помощью инструментов, основанных на концепции таблицы сопряжённости (рис. 1) [3].

Спрогнозированный класс \ Истинный класс	1	0
1	TP True Positive Истинно-положительные значения	FP False Positive Ложно-положительные значения
0	FN False Negative Ложно-отрицательные значения	TN True Negative Истинно-отрицательные значения

Рис. 1. Таблица сопряженности для случая бинарной классификации с метками классов {0,1}

Таким образом ошибки классификации бывают двух типов: FP и FN. На основе данных таблицы сопряжённости рассчитывают следующие бизнес-метрики.

Accuracy – достоверность – доля правильно классифицированных абонентов (1). Не в полной мере характеризует классификатор при несбалансированных классах [4].

$$\text{accuracy} = \frac{\text{TP} + \text{TN}}{\text{TP+TN+FP+FN}} \quad (1)$$

Precision – точность (2) – доля абонентов, отнесённых к классу «1», которые на самом деле являются объектами класса «1», из всех абонентов, отнесенных (классифицированных) к классу «1» [4]. Характеризует способность классификатора отличать абонентов класса «1» от класса «0».

$$\text{precision} = \frac{\text{TP}}{\text{TP} + \text{FP}} \quad (2)$$

Recall – полнота (3) – доля правильно классифицированных абонентов класса «1» из всех абонентов, принадлежащих к классу «1» [4]. Демонстрирует способность классификатора обнаруживать ушедших абонентов.

$$\text{recall} = \frac{\text{TP}}{\text{TP} + \text{FN}} \quad (3)$$

Анализируемые в данной статье методы могут давать полное распределение вероятности принадлежности абонентов к классам. Поэтому целесообразно применить ROC-анализ, а именно построить ROC-кривые (*Receiver Operating Characteristic*, рабочая характеристика приемника) [5]. Наклон ROC-кривой или ее крутизна показывают компромисс между долями TP и FP, так как при формировании прогноза оттока клиентов стремятся максимизировать значение TP, при этом минимизировать значение FP. Поэтому ROC-кривая должна стремиться к точке (0, 1). Важное значение имеет площадь под ROC-кривой (AUC, Area Under Curve). AUC дает представление о качестве классификатора. Чем больше AUC, тем лучше. В идеальном случае AUC равен 1 [5].

В таблице и на рис. 2 представлены результаты исследования эффективности следующих методов прогнозирования оттока клиентов: бэггинг, построенный на деревьях решений, общее количество которых равно 91 и максимальная глубина каждого равна 6; случайный лес, состоящий из 31 дерева решений, максимальная глубина которых равна 15, а максимальное количество признаков, по которым производится разбиение в каждом узле дерева, равно 7; GBRT, состоящий из 153 деревьев решений, максимальная глубина которых равна 3. В качестве программного обеспечения использовалась библиотека scikit-learn. Набор данных для исследования принадлежит американскому мобильному оператору и состоит из 18 признаков и 3333 абонентов. Этот набор данных включает в себя следующие признаки: буквенный код штата и префикс номера (категориальные); наличие подключенных услуг роуминга и голосовой почты (бинарные); длительность обслуживания клиента оператором, количество голосовых сообщений и обращений в службу поддержки (количественные); длительность разговоров, количество звонков и стоимость за день/вечер/ночь и для международной связи (количественные).

ТАБЛИЦА. Значения метрик, характеризующих эффективность методов

Название модели	Достоверность	Точность	Полнота	Площадь под кривой
Случайный лес	0,954	0,939	0,699	0,903
Бэггинг	0,949	0,902	0,690	0,920
Градиентный бустинг	0,956	0,932	0,720	0,916

На основании анализа таблицы и рис. 2 можно сделать вывод, что ансамблевые методы позволяют построить сравнительно точную прогнозную модель оттока клиентов для наборов данных, схожих по своей структуре с исследуемым. Среди этой группы методов почти по всем показателям лидирует бустинг (GBRT), несколько уступая только случайному лесу по способности отличать абонентов одного класса от другого (метрика *precision*) и также незначительно проигрывая бэггингу по качеству классификации (метрика AUC). В сравнении с остальными методами, GBRT предоставляет лучший компромисс между долями TP и FP, что видно по его ROC-кривой: она обладает большей крутизной наклона, поскольку проходит ближе всех к точке (0, 1).

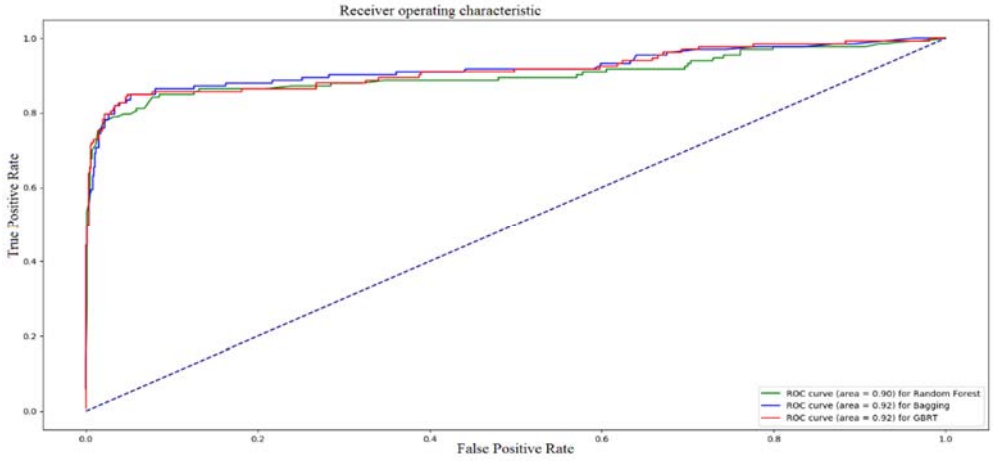


Рис. 2. ROC-кривые для анализируемых методов

Исходя из всех вышеперечисленных преимуществ, для построения модели оттока эффективнее использовать GBRT. Хотя два других метода показывают соизмеримые с GBRT результаты тестов и тоже могут быть использованы для построения прогнозной модели оттока абонентов, качество классификации все-таки ухудшается.

Список используемых источников

1. Hastie T., Tibshirani R., Friedman J. The Elements of Statistical Learning: Data Mining, Inference, and Prediction. M.: Springer, 2009. Second Edition, 764 p. ISBN 978-0-387-84857-0.

2. Breiman L. Random Forests // Machine Learning. 2001. N 45 (1). PP. 5–32.

3. Бринк Х., Джозеф Р., Феверолф М. Машинное обучение. М., СПб. : Питер, 2017. 336 с. ISBN 978-5-496-02989-6.

4. Powers D. Evaluation: From precision, recall and F-measure to ROC, informedness, markedness & Correlation // Journal of Machine Learning Technologies. 2011. N 2 (1). PP. 37–63.

5. Fawcett T. An introduction to ROC analysis // Pattern Recognition Letters. 2006. N 27. PP. 261–874.

УДК 65.011.56

ПРОГНОЗИРОВАНИЕ С ПРИМЕНЕНИЕМ НЕЙРОННОЙ СЕТИ В СИСТЕМАХ УПРАВЛЕНИЯ КЛАССА BI

А. Б. Гольдштейн, А. А. Шестакова

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

Системы класса BI являются особо востребованными для компаний, которые подчеркивают клиентоориентированность своего бизнеса, работающих в условиях высокой конкуренции и динамичности. Они дают инструментарий для детального анализа коренных причин текущей ситуации в компании. Средства BI превращают информацию в знания, которые позволяют быстро принимать решения.

В сочетании с нейронными сетями системы класса BI становятся мощнейшим инструментом для бизнеса. Свойство нейронной сети обучаться делает её наиболее привлекательной. Процесс обучения нейронной сети заключается в подстройке ее внутренних параметров под конкретную задачу. Процесс обучения осуществляется на обучающей выборке. Выборка включает в себя входные значения и соответствующие им выходные значения набора данных.

В системах класса BI нейронные сети чаще всего используются для прогнозирования. В сфере телекоммуникаций прогнозу могут подлежать такие параметры, как лояльность клиентов, отток клиентов и вероятность принятия предложения.

системы класса BI, нейронная сеть, лояльность, отток клиентов, вероятность принятия предложения.

В настоящее время всё больше компаний начинают искать пути для сокращения издержек. Такими путями могут стать отбрасывание балласта, жесткое контролирование расходов, повышение требований к производительности труда сотрудников.

Одним из главных инструментов для проведения подобных мероприятий являются системы класса BI [1].

Такие системы наиболее интересны для компаний, работающих в условиях высокой конкуренции и быстро изменяющейся среды, ориентированных на удовлетворение клиентов. В первую очередь к ним относятся телекоммуникации, розничная и оптовая торговля, страхование, банки. В статье более подробно рассмотрено применение BI-систем для сферы телекоммуникаций.

В большинстве случаев BI-система дополняет уже имеющийся в компании комплекс программных средств, получает из них данные в режиме реального времени и приводит их к виду, который позволяет видеть полное текущее состояние дел. Она дает инструментарий для детального анализа

коренных причин текущей ситуации в компании – носящих как позитивный, так и негативный характер.

BI-система особенно эффективна в период кризиса, когда жизненно необходимо непрерывное повышение плодотворности работы компании.

Средства BI превращают информацию в знания, которые позволяют быстро принимать решения. Эти средства интегрируют данные из OLTP-систем типа:

– ERP (*Enterprise Resource Planning*);
– SCM (*Supply chain management*);
– CRM (*Customer relationship management*)

и преобразуют их в сведения о том, как сделать бизнес более эффективным и отвечающим динамике рынка [2].

В сочетании с нейронными сетями, BI становится мощнейшим инструментом для бизнеса. Нейронная сеть обладает таким важным свойством, как возможность к обучению, что безусловно делает её ещё более привлекательной.

Среди всех методов обучения можно выделить два класса:

1. Детерминированный метод итеративно корректирует параметры сети, основываясь на ее текущих параметрах, величинах входов, фактических и желаемых выходах. Пример: метод обратного распространения ошибки.

2. Стохастические методы изменяют параметры сети случайным образом. При этом сохраняются только те изменения, которые привели к улучшениям. Такие методы могут попасть в «ловушку» локального минимума.

В системах BI нейронные сети чаще всего применяются для прогнозирования. Основной идеей прогнозирования является то, что предыдущие изменения действительно в какой-то степени предопределяют будущие.

В сфере телекоммуникаций прогнозу могут подлежать такие параметры, как лояльность клиентов, отток клиентов и вероятность принятия предложения.

Ухудшение качества предоставляемых услуг может подталкивать клиентов к отказу от их использования или полному уходу от оператора связи. Уровень лояльности клиента имеет существенное значение при определении комплексного уровня лояльности клиентов к услуге связи и оказывает влияние на величину комплексной оценки качества обслуживания клиентов на региональном уровне.

Лояльность и склонность к оттоку – разные понятия. Часто для выделения группы клиентов, склонных к оттоку, можно обозначить так называемые предикторы оттока. К ним можно отнести баланс счёта клиента, наличие трафика, статистику с портов оборудования (наличие/отсутствие ошибок), поступление платежей (регулярность, отсутствие задолженности).

Вероятность принятия предложения – это то, с какой вероятностью клиент захочет подключить себе новую услугу, наличие у него технической возможности реализации услуги. Расчёт такой вероятности полезен в первую очередь для отдела продаж, так как позволяет формировать списки клиентов, потенциально готовых к заключению новых договоров с оператором связи или модернизации уже используемых ими услуг.

Наиболее часто используемой структурой нейронной сети является однослойная нейронная сеть с прямым распространением – однослойный парцептрон, состоящий из искусственных нейронов. Искусственный нейрон имитирует в первом приближении свойства биологического нейрона, главная функция которого – формировать выходной сигнал в зависимости от сигналов, поступающих на его входы [3].

На вход искусственного нейрона поступает некоторое множество сигналов, каждый из которых является выходом другого нейрона. Каждый вход умножается на соответствующий вес, аналогичный синаптической силе, и все произведения суммируются, определяя уровень активации нейрона.

На рис. 1 представлена модель, реализующая эту идею. Множество входных сигналов, обозначенных x_1, x_2,…, x_n, поступает на искусственный нейрон.

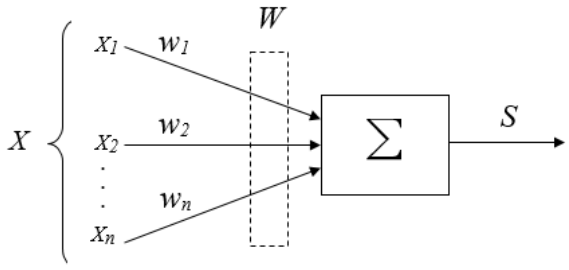


Рис. 1. Модель искусственного нейрона

Каждый вес соответствует «силе» одной биологической синаптической связи. Текущее состояние нейрона определяется как взвешенная сумма его входов:

$$S = \sum_{i=1}^{n} x_i w_i,$$

где n – число входов нейрона; x_i – значение i-го входа нейрона; w_i – вес i-го синапса.

Процесс обучения нейронной сети заключается в подстройке ее внутренних параметров под конкретную задачу. Алгоритм работы нейронной сети является итеративным, его шаги называют эпохами или циклами.

Эпоха – одна итерация в процессе обучения, включающая предъявление всех примеров из обучающего множества и, возможно, проверку качества обучения на контрольном множестве.

Процесс обучения осуществляется на обучающей выборке. Обучающая выборка включает входные значения и соответствующие им выходные значения набора данных. В ходе обучения нейронная сеть находит некие зависимости выходных полей от входных.

В качестве входных данных используются исторические данные, учитывающие некоторые параметры, составляющие «портрет» клиента.

К ним могут относиться:

– техническая возможность подключения определённой услуги – необходима для однозначного определения пула технологий и услуг, которые могут быть доступны и интересны клиенту;

– уже подключённые клиенту услуги – используется для исключения повторного предложения услуги, уже имеющейся у клиента;

– продолжительность пользования услугами – чем дольше клиент является пользователем тех или иных услуг в совокупности с отсутствием зарегистрированных по ним клиентских инцидентов, тем больше вероятность того, что клиент захочет приобрести дополнительные услуги;

– регион предоставления услуги – служит для поиска «похожих» клиентов по территориальному признаку;

– результат обзвона, взятый из импортированного в систему файла – учёт результата непосредственного общения с пользователем позволяет однозначно выявить его отношения к качеству предоставляемых услуг и учесть это при проставлении вероятности.

Набор параметров изменяется в соответствии с поставленной задачей прогнозирования.

Так, для определения вероятности принятия предложения, в качестве входных параметров могут использоваться уже подключенные клиенту услуги и техническая возможность подключения новых (рис. 2).

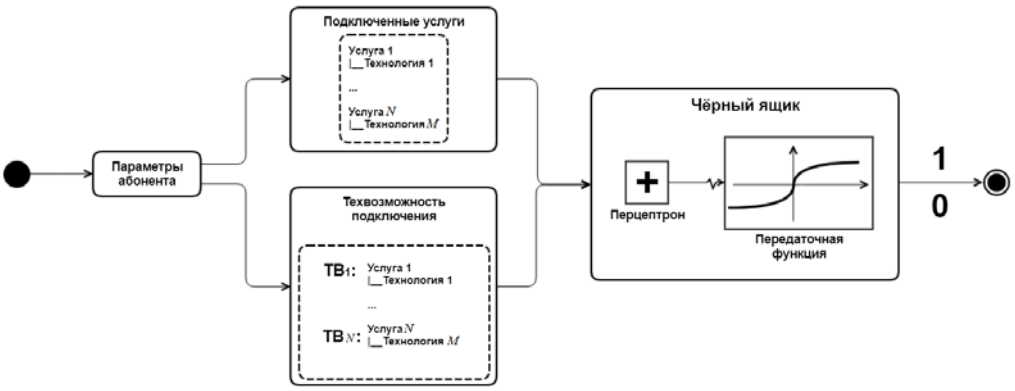


Рис. 2. Определение вероятности принятия предложения

Алгоритм работы нейронной сети выглядит следующим образом:

1. Получение клиентских данных.

2. Подача значений на сумматор нейрона (сумматор имеет множество входов – принимает большое количество данных, и единственный выход).

3. Определение значения прогнозируемого параметра.

4. Запись значения в таблицу фактов.

5. Если это последний клиент в таблице – завершение работы, если нет – возврат к пункту 1 основного потока.

В заключении отметим: BI-системы в совокупности с нейронными сетями – это сбор, управление, распределение и анализ информации с целью выработки такого видения проблемы, которое позволяет принять наилучшее решение. Такая система поддерживается данными из хранилищ, методами разработки данных, технологиями поддержки принятия решений, способствует увеличению доходов операторов связи, повышению лояльности клиентов и продаже пакетов услуг с заданной вероятностью.

Список используемых источников

1. Colin Ashford, Pierre Geuthier: OSS Design Patterns. M: Springer, Berlin, 2009. 151 p.

2. TM Forum [Электронный ресурс] // URL: https://www.tmforum.org, (дата обращения 10.01.2018).

3. Галушкин А. И. Нейронные сети. Основы теории. М. : Горячая линия – Телеком, 2012. 496 с.

УДК 004.031.43

ВИРТУАЛИЗАЦИЯ СЕТЕВЫХ ФУНКЦИЙ И OSS РЕАЛЬНОГО ВРЕМЕНИ. НОВЫЕ АСПЕКТЫ УПРАВЛЕНИЯ СЕТЯМИ

Б. С. Гольдштейн, А. К. Гринёва

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

Технологии SDN и NFV приобретают все большую популярность благодаря тому, что предлагают динамическое, гибкое и, что немало важно, более дешевое развертывание программных сетевых функций OSS систем на сети оператора. В статье рассмотрена архитектура SDNFV, которая сочетает в себе достоинства обеих технологий и предоставляет возможность по-другому рассмотреть задачу управления сетью.

управление сетями, виртуализация, SDN, OSS системы.

В настоящее время построенная операторами архитектура усложнена различными сетевыми функциями. Это могут быть как функции для межсетевого взаимодействия (система NAT, Proxy и т. д.), так и функции для реализации внутренних бизнес-процессов (подробнее описаны в картах TAM и eTOM). Такие технические решения зачастую выполнены в виде отдельных аппаратных надстроек к уже существующей сети. Как и любые

надстройки, они могут вызывать определенные трудности при эксплуатации. С целью ухода от вопроса аппаратной совместимости, была разработана архитектура NFV (*Network Function Virtualization* – Виртуализация сетевых функций), которая предлагает любые дополнительные сетевые функции реализовывать на виртуальных машинах, не требующих для себя аппартно-специализированных серверов. Таким образом, оператор имеет возможность расширять сетевые возможности своей сети, закупая обыкновенные ×86 сервера и специализированное программное обеспечение у вендеров, что, кроме упомянутого преимущества, также позволяет сэкономить расходы оператора на оборудовании.

Не стоит забывать и о том, что главное предназначение сетей заключается в пересылке пакетов между узлами. Для оптимизации данного процесса была разработана архитектура SDN (*Software Defined Network* – Программно-конфигурируемых сетей), которая разделяет сеть на простейшую плоскость данных и сложную программную плоскость, отвечающую за гибкость в пересылке потоков пакетов.

Объединяя две данные технологии, было предложено рассмотреть сеть SDNFV, архитектура которой включает следующие элементы: SDNFV коммутаторы, SDN контроллер и сервер SDNFV приложения [1].

SDNFV коммутаторы, кроме традиционной для SDN таблицы OpenFlow, имеют в своем составе платформы сетевых функций, которые позволяют к пересылаемым пакетам применять дополнительную обработку. Все платформы сетевых функций внутри коммутатора контролируются Менеджером сетевых функций.

Благодаря вводимым в состав коммутатора сетевым функциям, обеспечивается применение дополнительных возможностей и следующую затем пересылку пакетов практически в реальном времени, ограниченном лишь аппаратными возможностями оборудования.

SDN контроллер имеет два интерфейса: северный и южный. Через свой южный интерфейс он общается с SDNFV коммутаторами, управляя заполнением таблиц OpenFlow, а также расположением сетевых функций на них. Через свой северный интерфейс контроллер общается с SDNFV приложением, которое полностью координирует работу и размещение сетевых функций на коммутаторах.

SDNFV приложение является сложным программным элементом, включающим в себя как минимум четыре структуры: Оркестратор сетевых функций, Менеджер сервисных цепочек, Классификатор потоков и Механизм размещения.

Оркестратор выполняет главенствующую роль, получая запросы от других элементов сети (как SDNFV приложения, так и всей сети в целом). Именно он размещает новые виртуальные платформы на коммутаторах,

а также следит за их работоспособностью и синхронизацией между различными экземплярами.

Менеджер сетевых цепочек определяет последовательность проходимых сетевых функций потоком пакетов.

Классификатор потоков обозначает определенную ранее последовательность конкретным потоком. Сопоставление может быть назначено как администратором сети, так и выполняться динамически.

Механизм размещения, на основании получаемых данных о работе текущих сетевых функций и доступного ресурса, выполняет функцию маршрутизации и принимает решения о создании на определенном контроллере нового экземпляра одной или нескольких сетевых функций.

При маршрутизации пакета внутри сервисной цепочки могут возникнуть ситуации неопределенности. Такое возможно при запланированном поступлении пакета с одинаковым кортежем на один и тот же коммутатор.

Например, пакет внутри потока должен пройти последовательно от сетевой функции 1 (NF1), через NF2, до NF3. Причем NF1 и NF2 находятся на коммутаторе 1, а NF2 – на коммутаторе 2 (рис.). Предположим, что порт входа пакета на коммутатор 1 всегда одинаков, таким образом, IP 5-кортеж (IP адрес и порт) и входной порт коммутатора не позволят нам однозначно определить, на каком этапе сервисной цепочки находится пришедший пакет, и он каждый раз будет отправлен на NF1. Такую неопределенность при зацикливании пакета необходимо решать на коммутаторе SDNFV, и способом для ее решения является тегирование пакетов.

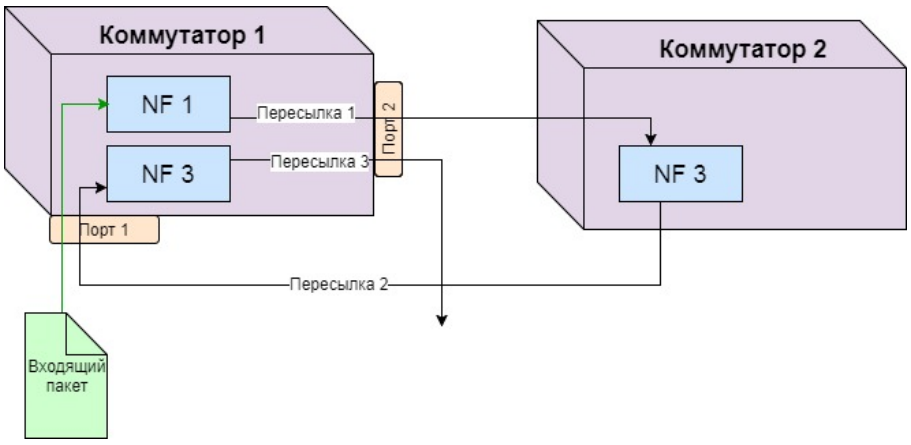


Рисунок. Неопределенность маршрутизации пакета в сервисной цепочке

По результатам вывода NF, пакету присваивается тег, который в дальнейшем будет использоваться при анализе для решения неопределенности в маршрутизации. Теги бывают локальные и глобальные. Первые используются лишь внутри одного коммутатора, другие же необходимы при пересылке пакета на следующие SDNFV коммутаторы.

Глобальные теги присваивают пакету Менеджер сетевых функций, однако контроллер SDN также принимает участие в тегировании потоков глобальными тегами. При настройке таблиц OpenFlow на коммутаторах он будет включать действие «вставить тег» на коммутаторе, выпускающем поток пакетов и добавлять критерий «наличие тега» в правило для рассмотрения на коммутаторах, которые принимают данные потоки. Глобальный тег становится частью пакета.

В случае динамических сервисных цепочек на маршрутизацию пакета влияет также сам результат обработки пакета внутри сетевой функции. Подобные результаты не являются частью пакета, а записываются в его дескриптор, соответственно, используются лишь Менеджером сетевых функций внутри коммутатора и не передаются дальше. Наличие возможности обеспечения динамических сервисных цепочек предоставляет Приложению SDNFV право назначать и управлять пересылкой потоков пакетов в зависимости от результатов обработки их внутри коммутаторов.

В заключении следует заметить, что рассмотренная архитектура имеет ряд преимуществ по сравнению с уже разработанными SIMPLE, Steering и FlowTags.

Архитектура SIMPLE не поддерживает возможность динамических цепочек маршрутизации [2].

Архитектура Steering опосредует изменение сервисных цепочек через SDN контроллер, что создает дополнительную и неоправданную нагрузку на него, а также не поддерживает сложную маршрутизацию и развертывание нескольких экземпляров одной NF на контроллере [3].

Архитектура FlowTags не экономит количество используемых тегов, применяя их не только в случаях неопределенности, но и при любом решении о пересылке [4].

Таким образом, архитектура SDNFV предлагает оптимальное решение для построения гибкой, масштабируемой сети с возможностью добавления новых сетевых возможностей OSS систем по запросу оператора сети.

Список используемых источников

1. Ali Mohammadkhan, Guyue Liu, Wei Zhang, K. K. Ramakrishnan, and Timothy Wood. Protocols to Support Autonomy and Control for NFV in Software Defined Networks // IEEE Conference on Network Function Virtualization and Software Defined Network, 2015.

2. Qazi Z. A. et al. Simple-fying middlebox policy enforcement using SDN // In SIGCOMM Computer Communication Review, 2013.

3. Zhang Y.et al. Steering: A software-defined networking for inline service chaining // In ICNP, 2013.

4. Fayazbakhsh S. K. Enforcing network-wide policies in the presence of dynamic middlebox actions using flowtags. NSDI ’14.

УДК 004.725

О ТУМАННЫХ ВЫЧИСЛЕНИЯХ В МИРЕ ИНТЕРНЕТА ВСЕГО. ПАРАДИГМА FOE

Б. С. Гольдштейн, С.М. Елисеев

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

Наступающая эра «Интернет Будущего» представляет собой две парадигмы: Fog Computing и Internet of Everything. Туманные вычисления – совершенно новая вычислительная парадигма, которая направлена на перемещение объектов и служб Cloud Computing в сеть доступа. Главная задача – экономить энергию и пропускную способность, одновременно повышая уровень QoS, предоставляемый пользователям.

туманные вычисления, интернет всего, облачные вычисления, интернет вещей, туман всего.

Интернет всего

Последние годы характеризовались двумя, казалось бы, противоречивыми технологическими тенденциями. Первая из них рассматривала модель «облака» как вездесущую вычислительную парадигму и связанный с этим сдвиг функций вычисления, контроля и хранения информации в удаленные крупные центры обработки данных. Вторая тенденция касалась увеличения числа разнородных пользовательских устройств доступа и датчиков, таких как планшеты, смартфоны, смарт-бытовая техника, точки доступа, кросс-маршрутизаторы, смарт-счетчики для электрических сетей, интеллектуальные системы управления для промышленных предприятий и др.

Общей особенностью всех этих устройств является то, что они являются вещами, которые работают на краю сети. Это область так называемой парадигмы Internet of Everything (IoE, Интернет всего) [1].

Парадигма IoE представляет собой ряд новых задач, которые не могут быть объективно решены только облачными и размещенными (хостинговыми) вычислительными моделями.

Вот некоторые из них:

– Сокращение задержек связи – промышленные системы управления (например, производственные предприятия и интеллектуальные энергосистемы) обычно требуют задержки связи между датчиком и контроллером порядка миллисекунд.

– Рациональное использование пропускной способности Интернета – быстро растущее число соединенных устройств создает большие потоки данных с экспоненциальной скоростью.

– Ограничения ресурсов устройств IoE – многие устройства IoE (например, датчики, исполнительные механизмы, контроллеры и встроенные системы) ограничены как ресурсом, так и ограничены по мощности. Поэтому они не могут полагаться исключительно на собственные возможности, чтобы выполнить свои вычислительные и коммуникативные задачи.

– Непрерывное сетевое подключение – чтобы поддерживать мобильность устройств, должны быть гарантированы надежные сетевые подключения между устройствами и облаком [1].

Все эти задачи IoE открывают двери для парадигмы Fog Computing (FC, Туманные вычисления) [1].

Основные атрибуты модели туманных вычислений

Модель туманных вычислений основана на предположении, что вычислительные задачи могут выполняться узлами, расположенными на краю сети доступа, а также между удаленным облаком и устройствами IoE. Конечной целью является увеличение вычислительных и сетевых ресурсов обслуживаемых устройств, не увеличивая при этом слишком большие результирующие задержки обслуживания.

Как следствие, Fog Nodes (FNs, туманные узлы) являются виртуализированными сетевыми центрами обработки данных, которые работают поверх (как правило, беспроводных) точек доступа на краю сети. FNs развертываются в сети доступа, а расстояние между устройством и узлом тумана обычно ограничено до одного шага.

С целью динамически мультиплексировать доступные физические вычислительные ресурсы, хранилища и сетевые ресурсы по спектру обслуживаемых устройств, а также обеспечить однородный пользовательский интерфейс поверх (возможно) гетерогенных обслуживаемых устройств, в центрах обработки данных «Тумана» применяется технология виртуализации. Грубо говоря, в виртуализированных центрах обработки данных каждое обслуживаемое физическое устройство отображается в виде виртуального клона, который действует как виртуальный процессор и выполняет программы от имени клонированного устройства [1].

Для достижения виртуализации устройств можно использовать две основные технологии виртуализации: традиционную технологию на основе виртуальной машины (VM) и новую технологию CoNTainer (CNT). Их основные архитектурные различия заключаются в том, что виртуальная машина оборудована собственной гостевой операционной системой, в то время как контейнер содержит только связанные с приложениями (обычно легкие) библиотеки и совместно с другими контейнерами операционную систему физического сервера.

Из-за ожидаемого большого числа устройств, которые должны быть виртуализованы в средах приложений IoE, использование виртуализации на основе CNT позволило бы увеличить количество виртуальных клонов на физический сервер (так называемую плотность виртуализации). Именно по этой причине предложенная парадигма туманных вычислений построена на технологии виртуализации контейнеров [1].

Каждый FN оснащен (ограниченным) количеством физических серверов, которые связаны между собой проводной сетью внутри тумана (обычно, *Ethernet*). FN покрывает пространственную область определенного диаметра и служит кластером вещей [2].

Система IoE – «Туман» – «Облако»

В вычислительных системах, которые используют только удаленные облачные центры обработки данных, IoE устройства на краю сети могут связываться с облачными серверами посредством использования многопоточных WANs (*Wide Area Network*) [3].

Все ресурсы для вычисления и хранения находятся в удаленных облаках, и IoE устройства могут обращаться к этим удаленным ресурсам путем использования клиент-серверной модели [2].

Картина радикально меняется в рамках трехуровневой системы IoE – «Туман» – «Облако». В этой системе физические ресурсы больше не сосредоточены в удаленном «облаке». Фактически, FNs позволяют приблизить вычислительные ресурсы и ресурсы для хранения к требуемым устройствам [2].

Интеграция IoE и Fog Computing открывает двери для новой парадигмы Fog of Everything (FoE, Туман всего).

На рисунке представлена базовая архитектура технологической платформы для поддержки предлагаемой парадигмы FoE [1].

Предлагаемая архитектура состоит из интеграции следующих шести основных блоков:

– *уровень IoE*, где ряд (возможно, разнородных) *вещей* работает на нескольких пространственных кластерах. Согласно лексикону IoE, *вещь* – это ограниченное по ресурсам пользовательское устройство, которое нуждается в увеличении ресурсов, чтобы выполнить свою рабочую нагрузку. Вещь может быть фиксированной, кочевой или подвижной;

– *беспроводная (возможно, мобильная) сеть доступа*, которая поддерживает передачу данных Туман-Вещь(F2T) и Вещь-Туман(T2F) через соединения TCP / IP, работающие на IEEE802.11/15 каналах с одним «хопом»;

– *набор взаимосвязанных FN*;

– *внутритуманная магистраль* (возможно, беспроводная), обеспечивающая внутритуманную связь и возможное объединение ресурсов между узлами тумана;

– *уровень виртуализации*, который позволяет каждой вещи увеличивать свои ограниченные ресурсы, используя вычислительные возможности соответствующего виртуального клона. Последнее выполняется на физическом сервере FN, который в данный момент обслуживает клонированную вещь;

– результирующая наложенная *межклоновая виртуальная сеть*, которая позволяет организовать межклоновую связь P2P путем использования сквозных транспортных соединений TCP / IP.

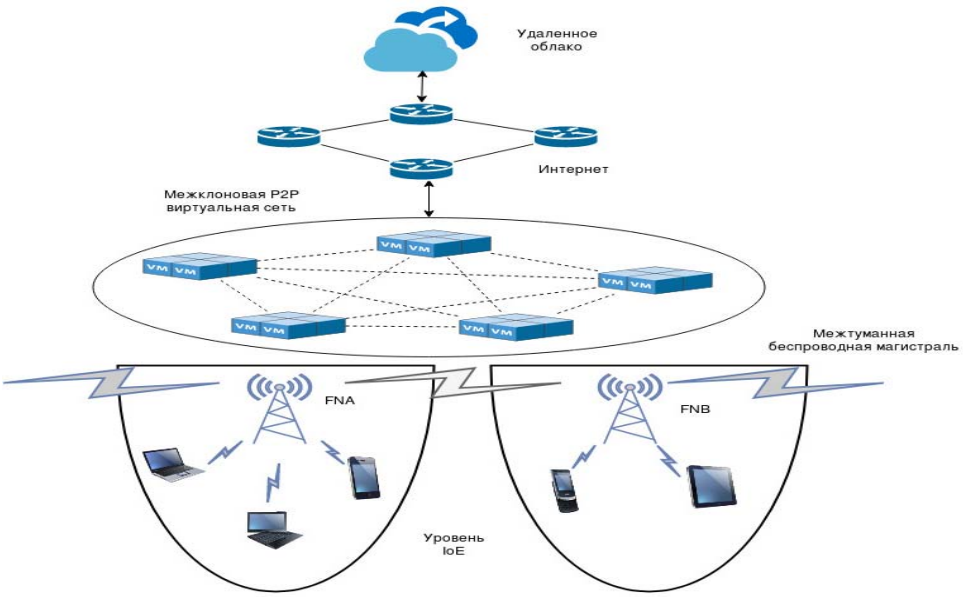


Рисунок. Архитектура FoE

Также в архитектуре присутствует удаленное облако, которое связано сетью интернет с набором FN.

Основной особенностью предложенной парадигмы FoE является то, что наложенная сеть позволяет перемещать реализацию соединений между устройствами с физического нижнего уровня на базе устройства на виртуальный верхний уровень на основе клонирования. Эта особенность, в свою очередь, позволяет заменить ненадежные, неуправляемые и мобильные D2D физические соединения на надежные, статические и основанные на TCP/IP межклоновые виртуальные транспортные соединения [1].

Заключение

Представленная парадигма FoE предоставляет технологическую платформу для таких проектов, которые на сегодняшний день невозможно реа-

лизовать. Например: Интернет Энергии, Умный город, Industry 4.0 (Четвертая промышленная революция) и др. Поскольку модель FoE проистекает из двух возникающих парадигм – FC и IoE – она находится в зачаточном состоянии и, следовательно, непрерывно развивается.

Список используемых источников

1. Enzo Baccarelli, Paola G. Vinueza Naranjo, Michele Scarpiniti, Mohammad Shojafar, Jemal H. Abawajy: Fog of Everything: energy-efficient networked computing architectures, research challenges, and a case study. 2017.
2. OpenFog Consortium Architecture Working Group: OpenFog Reference Architecture for Fog Computing. Feb, 2017.
3. Гольдштейн Б. С., Кучерявый А. Е. Сети связи пост-NGN. 2014. СПб.: БХВ-Петербург, 2014. 160 с.: ил. ISBN 978-5-9775-0900-8.

УДК 004.725

ИНЖЕНЕРНЫЕ АСПЕКТЫ ПРОГРАММНО-КОНФИГУРИРУЕМЫХ СЕТЕЙ. ИНТЕРФЕЙСЫ, СТАНДАРТИЗАЦИЯ И ВАРИАНТЫ РЕАЛИЗАЦИИ

Б. С. Гольдштейн, И. И. Жуковский

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

Программно-конфигурируемые сети в настоящее время становятся все более и более популярной темой. На исследования и стандартизацию в этой области направлены большие усилия. И это неудивительно, ведь применение программно-конфигурируемых сетей, основанных на открытых стандартах, сулит не только техническую, но и экономическую выгоду всем игрокам рынка телекоммуникаций.

программно-конфигурируемые сети, стандартизация, интерфейсы.

Программно-конфигурируемые сети (*Software Defined Network* – SDN). ПКС – сетевая парадигма, которая подразумевает отделение устройства передачи от принятия управляющих решений о передаче. Такое разделение позволяет сильно упростить управление сетью, ее развитие и модернизацию. Основная идея Программно-конфигурируемых сетей заключается в том, чтобы позволить программным приложениям управлять ресурсами сети так же как они управляют ресурсами компьютера. В ПКС вся логика управления сети централизована в одном месте – в контроллере (плоскость

управления “*control plane*”), что позволяет упростить сетевые устройства, сделав их просто устройствами пересылки пакетов (плоскость данных “*data plane*”), управляемых контроллером по открытому интерфейсу [1].

Как видно на рис. 1, вынесение управления в отдельное устройство и отделения его от плоскости передачи данных позволяет упростить разворачивание новых приложений и протоколов на сети, облегчить управление сетью и собрать различные дополнительные устройства (NAT, межсетевой экран и т. д.) в виде приложений, запущенных на контроллере.

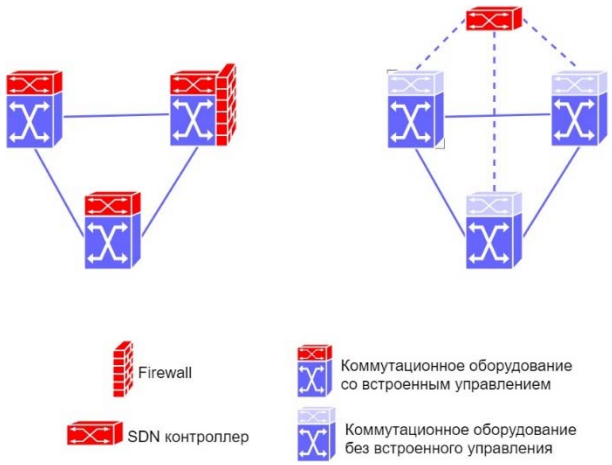


Рис. 1. Архитектура ПКС

На данный момент наиболее известная и стандартизованная архитектура ПКС – OpenFlow. Несмотря на то, что эта архитектура весьма популярна, есть ряд моментов, которые в ней еще не до конца стандартизованы или вообще не входят в стандарт OpenFlow.

В концепции OpenFlow контроллер реализует программный интерфейс для взаимодействия управляющего приложения сетевых ресурсов. Контроллер имеет два интерфейса, так называемые северный и южный мосты (рис. 2).

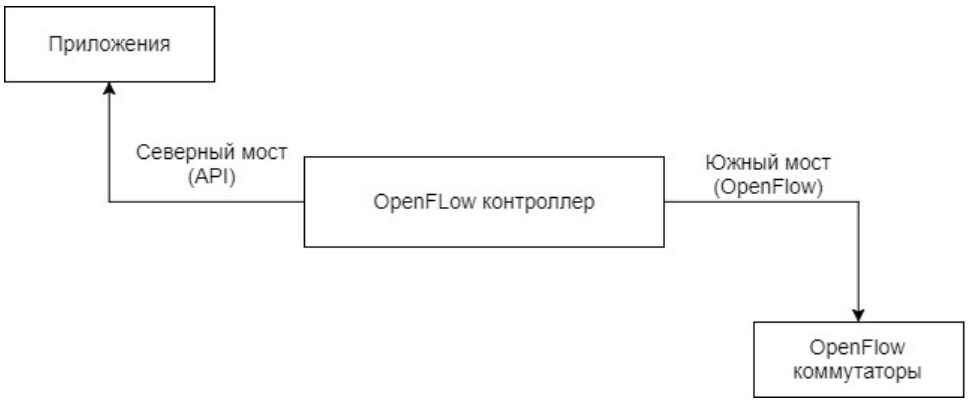


Рис. 2. Интерфейсы OpenFlow контроллера

Южный мост отвечает за связь контроллер-коммутатор, это взаимодействие достаточно хорошо стандартизовано и описывается протоколом OpenFlow. Стоит отметить, что для безопасности в OpenFlow 1.3.0. реализуется обмен сертификатами между коммутаторами и контроллером, формат которых не стандартизован.

Северный мост осуществляет взаимодействие контроллер-приложение, обеспечивая приложение информацией о сети и возможностью применения политик на сеть. Взаимодействие контроллер-приложение является полностью программной абстракцией, неким API. При чем этот API не стандартизован и зависит от конкретной реализации контроллера. До принятия такого стандарта каждый контроллер будет иметь собственный API и как следствие ограниченный набор приложений, разработанных специально под данный API, что значительно снизит возможности модернизации и развития сети. Тем не менее, введение стандарта для северного моста котроллера необходимо, чтобы операторы связи могли получить преимущество от развертывания ПКС в виде возможности свободного комбинирования приложений и контроллеров различных производителей.

Программно-Конфигурируемые сети построенные на основе протокола OpenFlow предполагают централизованное управление. Это может стать проблемой в распределенных сетях, где коммутаторы сильно удалены от контроллера. С увеличением длины соединения контроллер-коммутатор возрастает задержка, что отрицательно сказывается на производительности всей сети. Очевидным решением является установка дополнительного контроллера для управления удаленными коммутаторами. Но такому решению препятствует слабая стандартизация интерфейса взаимодействия контроллер-контроллер, что превращает запуск территориально распределенной сети ПКС в сложную задачу. Тем не менее, стандартизация такого интерфейса необходима, так как множество операторов владеют большими, территориально распределёнными сетями и невозможность развертывания на них ПКС снижает привлекательность технологии.

В Программно-Конфигурируемых сетях контроллер представляет собой единую точку отказа, при неисправности контроллера вся сеть выходит из строя. Эта проблема решается путем добавления избыточности в плоскость управления, другими словами, подключение нескольких контроллеров к коммутатору, что позволяет запасному контроллеру взять управление на себя в случае сбоя.

Попытки решения проблемы излишней централизации в сетях OpenFlow были предприняты в рамках проектов Onix [2] и HyperFlow [3]. HyperFlow представляет собой приложение для контроллера NOX. В этом проекте контроллер будучи физически распределенным (рис. 3) остается логически единой сущностью. Это позволяет поддерживать распределённые сети, путем установки дополнительных контроллеров для снижения задержек связи с удаленным коммутаторами, но при этом сохраняется возможность создавать приложения с централизованным управлением сетью. Однако недостатком такого подхода является возможность некорректной работы приложений, которым необходима точная информация о состоянии сети.

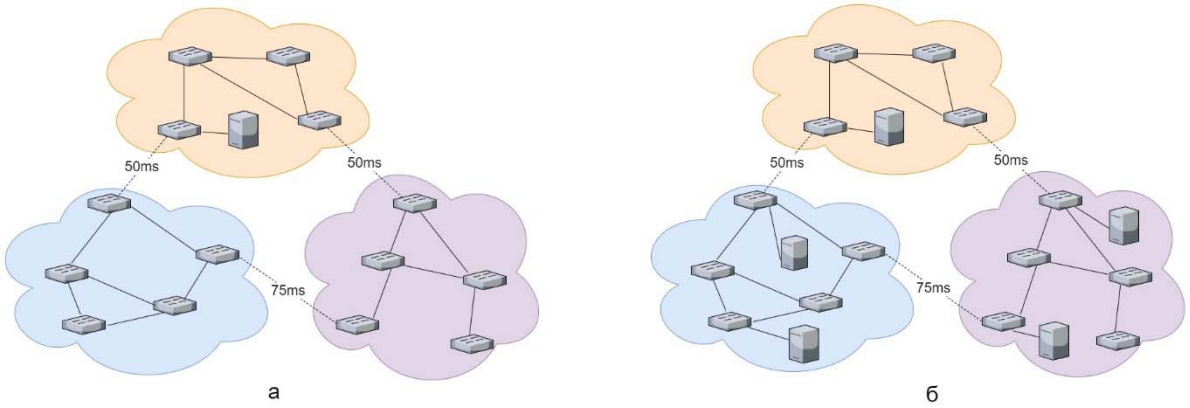


Рис. 3. а) распределенная OpenFlow сеть; б) распределенная OpenFlow сеть с HyperFlow

Так же интересен подход, предложенный в рамках проекта Kandoo [4]. Этот проект предлагает использовать локальные контроллеры для локальных нужд и перенаправлять запросы на главный контроллер только для решений, требующих централизованного управления сетью. Это уменьшает нагрузку на центральный контроллер, уменьшая количество запросов, а также обеспечивает плоскость передачи данных более быстрыми ответами на запросы, которые могут обрабатываться локальным управляющим приложением.

Несмотря на то, что в сферу ПКС направлено множество усилий научного и индустриального сообщества, остается достаточное количество элементов, которые необходимо стандартизировать и проблем, которые необходимо решить. Некоторые из них уже имеют намеченные пути решений (распределенный контроллер и проект *HyperFlow*), а некоторые только предстоит привести к одному стандарту (API контроллера).

Список используемых источников

1. Bruno Astuto A. Nunes, Marc Mendonca, Xuan-Nam Nguyen, Katia Obraczka, and Thierry Turletti. A Survey of Software-Defined Networking: Past, Present, and Future of Programmable Networks. Communications Surveys and Tutorials, IEEE Communications Society, Institute of Electrical and Electronics Engineers, 2014, 16 (3), pp.1617–1634. URL: http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=6739370

2. Koponen T., Casado M., Gude N., Stribling J., Poutievski L., Zhu M., Ramanathan R., Iwata Y., Inoue H., Hama T., et al. Onix: A distributed control platform for large-scale production networks. OSDI, Oct. 2010.

3. Tootoonchian A. and Ganjali Y. Hyperflow: A distributed control plane for openflow // In Proceedings of the 2010 internet network management conference on Research on enterprise networking, pages 3–3. USENIX Association, 2010.

4. Soheil Hassas Yeganeh and Yashar Ganjali. Kandoo: a framework for efficient and scalable offloading of control applications // In Proceedings of the first workshop on Hot topics in software defined networks, HotSDN ’12, pages 19–24, New York, NY, USA, 2012. ACM.

УДК 621.391

ПОВЫШЕНИЕ ПОМЕХОУСТОЙЧИВОСТИ НА ЛИНИЯХ СОВРЕМЕННОЙ ТРОПОСФЕРНОЙ СВЯЗИ

А. В. Гончаров[1], М. И. Петренко[1], Ю. Д. Украинцев[2], А. Д. Юшкевич[1]

[1]Военная академия связи им. Маршала Советского Союза С. М. Буденного
[2]Ульяновский государственный технический университет

В современных радиоприемных устройствах порог решающей схемы определяется на основе классического байесовского подхода, предполагающего, что статистические характеристики сигнала и помех (их смеси) подчиняются априорно известной нормальной плотности распределения вероятностей мгновенных значений огибающей, наблюдаемой на его входе. Это не всегда соответствует реальной обстановке, требующей оценки не только параметров, но и самой ПРВ. В работе предлагается применение «наивного» метода Байеса, позволяющего восстановить ПРВ, что связано с необходимостью обработки статистических данных, снимаемых с определенного элемента радиоприемного тракта.

анализатор помеховой обстановки, вероятность ошибочного приема, парзеновская процедура восстановления ПРВ.

Введение

В настоящее время на линиях беспроводной связи широко применяется алгоритм решающей схемы радиоприемного устройства, основанный на классическом Байесовском подходе. Этот подход предполагает, что плотность распределения мгновенных значений огибающей смеси радиоприемного устройства априорно известна. Она основана на основе статистики, полученной за предыдущие несколько лет. При этом предполагают, что эта плотность распределения вероятностей (ПРВ) подчиняется нормальному закону распределения.

Исследования последних лет, связанных с бурным насыщением эфира радиоизлучениями различных диапазонов волн, убедительно показывают, что эти ПРВ лишь в 30 % сеансов связи подчиняются нормальному, в 60 % – релеевскому и в 10 % – логарифмически нормальному законам распределения [1, 2, 3, 4, 5]. Все это свидетельствует о необходимости текущей оценки ПРВ, отражающей состояние реальной радиотрассы. Возможность восстановления текущей ПРВ дает основания для использования «наивного» метода Байеса для определения порога решающей схемы радиоприемного устройства. Однако применение этого метода требует оценки качества определения порога решающей схемы.

Постановка задачи

Для повышения помехоустойчивости на линиях современной тропосферной связи предлагается использовать адаптивно-непараметрический классификатор, основанный на текущем восстановлении плотности распределения (ПРВ) мгновенных значений огибающей принимаемого сигнала в каждой ветви разнесения. Алгоритм работы восстановления ПРВ основан на непараметрической оценке ПРВ Парзена-Розенблатта, анализ которого проведен в работах [6, 7, 8]. При этом в ходе сеанса связи определяются наиболее вероятные значения сигнала (мода) при отсутствии и наличии помех, устанавливается в соответствии с реальной обстановкой на линии связи порог решающей схемы, а затем на основе сдвига мод принимается решение о вероятности ошибочного приема [9, 10, 11]. Для уточнения качества определения порога методом имитационного моделирования предлагается набрать достаточную статистику (репрезентативная выборка) мод сигнала, мод смеси сигнала и помехи, а также порога решающей схемы. На основе этих выборок построить ПРВ сигнала, ПРВ смеси сигнала с помехой и порога решающей схемы, что позволит определить дисперсию (разброс) указанных параметров.

Решение задачи

Оценка ПРВ основывается на рекуррентной парзеновской процедуре [10]:

$$W_N(X) = W_{N-1}(X) + \frac{1}{N}\left(W_{N-1}(X) + \frac{1}{h_N}K(y)\right),$$

где N – объем выборки достаточной статистики, h_N – ширина аппроксимирующей функции, $K(y)$ – аппроксимирующая функция.

Обоснование параметров оценки ПРВ представлено в работах [7, 8, 9]. На основе этой процедуры определяются ПРВ сигнала и ПРВ смеси сигнала и помехи. На основе классического метода Байеса известно, что ПРВ смеси сигнала и помехи будет сдвинута вправо относительно ПРВ сигнала. Место пересечения этих двух плотностей и является порогом решающей схемы радиоприемного устройства, т. е.

$$W(U_{\text{с}}) = W(U_{\text{с+п}}).$$

На основе полученных значений ПРВ принимаемого сигнала определяется значение ее моды в соответствии с выражением:

$$M(i,T) = \max_{(X)} W_N\,(X),$$

где: i – Временной интервал набора достаточной статистики, T – общее время, необходимое для набора статистики на заданном интервале.

На основе полученных значений ПРВ принимаемой смеси сигнала и помех определяется значение ее моды в соответствии с выражением:

$$M(i,T) = \max_{(X+\text{п})} W_N\,(X + \text{П}),$$

где: i – временной интервал набора достаточной статистики, T – общее время, необходимое для набора статистики на заданном интервале.

В дальнейшем вероятность ошибочного приема сигнала определяется, как и при классическом Байесовском подходе:

– если $U_\text{с} < U_\text{пор}$ – принимается решение об отсутствии помех;

– если $U_\text{с} > U_\text{пор}$ – принимается решение о наличии помех.

Учитывая, что порог решающей схемы определялся на основе обработки статистики, требуется уточнение точности его определения. Для этого набирается статистика мод, наиболее вероятного значения принимаемого сигнала, смеси сигнала и помехи, а также самого порога. На основе этих статистик с помощью представленной выше процедуры Парзена предполагается восстановить ПРВ мод сигнала, смеси сигнала и помехи, а также порога решающей схемы радиоприемного устройства. При этом обработке подвергнуться два наиболее часто встречающихся закона: нормальный и релеевский.

Список используемых источников

1. Васильев К. К., Глушков В. А., Дормидонтов А. В., Нестеренко А. Г. Теория электрической связи / Под общ. ред. К. К. Васильева. Ульяновск : УлГТУ, 2008. 452 с.

2. Гусятинский И. А., Немировский А. С. И др. Дальняя тропосферная радиосвязь. М. : Связь,1968, 246 с.

3. Немировский М. С., Шорин О. А., Бабин А. И., Сартаков А. Л. Беспроводные технологии от последней мили до последнего дюйма: учебное пособие. М. : Эко Тренз, 2010. 400 с.

4. Орлов А. И. Прикладная статистика. М. : Экзамен, 2004. 250 с.

5. Репин В. Г. Обнаружение сигнала с неизвестными моментами появления и исчезновения // Проблемы передачи информации. 1991. Т. 27. № 1. С. 61–72.

6. Смирнов Н. В. Асимптотическая мощность некторых непараметрических критериев // Труды Всесоюзного совещания по математической статистике, Ереван, 1960.

7. Украинцев Ю. Д., Украинцев К. Ю. Сравнительный анализ парзеновских (непараметрических) процедур восстановления ПРВ // Современные проблемы создания и эксплуатации радиотехнических систем. Сборник трудов шестой научно-практической конференции (с участием СНГ). Ульяновск : УлГТУ, 2009, С. 233–236.

8. Украинцев К. Ю. Селиверстов М.В. Методика определения порога решающей схемы адаптивно-непараметрического классификатора помеховой ситуации // Современные проблемы создания и эксплуатации радиотехнических систем: труды седьмой всероссийской научно-практической конференции (с участием стран СНГ), г. Ульяновск, 22–23 сентября 2011 г. Ульяновск : УлГТУ, 2011. 246 с.

9. Украинцев Ю. Д. Украинцев К. Ю. Обоснование параметров непараметрической процедуры восстановления априорно неопределенной плотности распределения вероят-

ностей // Ученые записки ульяновского государственного университета. Сер. Математика и информационные технологии. Вып. 1 (3) / Под ред. А. А. Смагина. Ульяновск : УлГУ, 2012. 286 с.

10. Parzen, On estimation of a probability density function and mode // Ann. Math. Statist. 33, 3 (1962), pp. 1065–1076.

11. Rosenblatt M. Remarks on some nonparametric estinates of a density function // Ann. Math/ Statist,, 27,3 (1956), pp. 832–837.

УДК 004.71

ОБЗОР РАЗНООБРАЗНЫХ МЕТОДОВ СБОРА ДАННЫХ ДЛЯ УМНОЙ ТРАНСПОРТНОЙ СИСТЕМЫ УМНОГО ГОРОДА

А. А. Гребенщикова, О. А. М. Махмуд, А. С. А. Мутханна, А. И.Парамонов

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

В работе рассматривается революционная технология, предполагающая обеспечить каждое техническое устройство способным подключиться к интернету. Эта концепция строится на объединении различных технологий, для возможного создания межмашинного взаимодействия, а не взаимосвязи между пользователем и машиной. Умный город – это более широкий подход, цель которого поднять уровень качества жизни для каждого человека за счёт объединения современных информационно – коммуникационных технологий и интернета вещей. Устройства, использующиеся в умном городе, смогут генерировать огромное количество данных, что в свою очередь должны своевременно накапливаться, обрабатываться и храниться для последующего анализа. Отсюда следует, что сбор данных – это важный аспект в построении умного города. В предложенной работе представлены различные методы накопления данных для умной транспортной системы.

умный город; интернет вещей; умная транспортная система.

Введение

Считается, что к 2050-му г. около 70 % всего населения будет жить в мегаполисах, в связи с ростом миграции сельского населения в города. Отсюда следует необходимость трансформировать существующие города в умные. «Умный город» – городское видение [1], в котором информационные технологии являются основой предоставления услуг жителям. Всё это фокусируется для интеграции различных информационно-коммуникационных технологических и Интернет вещей (IoT) решений путем внедрения

датчиков и оборудования в безопасном режиме [2]. В связи с широким использованием датчиков, для создания умного города необходимо изучить надлежащие способы сбора данных для надлежащего сбора этих данных, которые могут быть дополнительно проанализированы для предоставления нескольких услуг в умном городе [3]. Умный город построен с учетом различных областей, таких как: умная транспортная система, управление отходами, управление водными ресурсами, управление энергетикой, институт образования, недорогое доступное жильё, дискретизация или оцифровка, электронное государственное управление, здравоохранение, городская безопасность.

Из всего известного материала по поводу умного города, данная работа рассказывает о методах сбора данных умной транспортной системы. Городское население мира растет беспрецедентными темпами, благодаря чему для обеспечения устойчивости города требуется более совершенная и продуманная система. Умная транспортная система-это один из аспектов «умного города», которая призвана оказывать различные инновационные услуги, связанные с различными видами транспорта и организации дорожного движения и позволяют различным пользователям получать больше информации и сделать использование транспортных сетей более безопасным, более скоординированным, и умнее. К тому же всё это должно обеспечивать получение нужной информации в нужное время [4].

Из-за огромного объема данных, получаемых в умной транспортной системе и миллионов устройств, относящихся к интернет вещам, возникают такие задачи как, устранение разнородности, масштабируемости и совместимости [5].

Оставшаяся часть статьи структурирована следующим образом. Второй раздел содержит различные способы сбора данных в умной транспортной системе для полного понимания того, как данные генерируются. Чтобы получить представление о неоднородности, функциональной совместимости генерируемых данных, в разделе III показана таблица, в которой исследуются все способы сбора данных по различным параметрам. В разделе IV приводятся заключительные аргументы, обсуждаются основные вопросы, поднятые в документе.

Различные способы сбора данных в умной транспортной системе

Данные имеют решающее значение как для умных городов, так и для умной транспортной системы, чтобы облегчить принятие решений и действия в области транспортировки.

Индуктивный контур. Детектор индуктивной петли для идентификации и подсчета. Он обеспечивает альтернативный способ подсчета транс-

портных средств, а не с помощью пневматических труб. Индуктивный детектор петли состоит из встроенного токарного провода, генератора и удлинительного кабеля, с помощью которого сигналы передаются из петли в устройство для подсчёта. Транспортное средство, проходя мимо контура, приводит к изменению магнитного поля, которое в свою очередь активирует счетное устройство. Таким образом, обнаружение транспортного средства осуществляется с помощью индуктивной петли. Частота сбора данных составляет пять минут. Точность составляет ±2,96 %.

Индуктивные петли широко используются за счёт того, что они достаточно дешёвые и могут быть использованы для изучения движения в режиме постоянного времени. Одиночного контура недостаточно для оценки скорости автомобиля, так как требуется два контура. Это недостаток, связанный с индуктивным циклом.

Видеодетектор автомобиля: Видео-обнаружение транспортного средства является современным ненавязчивым методом для наблюдения отслеживания трафика и статистики потока данных, собранных в синхронном режиме. Он служит основной альтернативой обычным детекторам индуктивной петли. Этот способ сбора данных включает в себя захват различных данных, таких как передние движущиеся объекты (в основном транспортные средства) и вычитание фоновой среды. Он является наиболее подходящим для крупномасштабного сбора данных.

Таким образом сбор данных осуществляется с помощью камеры видеонаблюдения. Для получения наилучшего результата и правильной точности данных важно выбрать точку для фиксации камеры. Эта точность составляет ±3 %.

Работа является жизнеспособной в текущем сценарии, так как легко масштабируется и обеспечивает передачу данных трафика более безопасным способом. Но с другой стороны, затраты на внедрение и обслуживание обойдутся достаточно дорого.

На основе GPS. Сбор данных, основанный на GPS, используется либо в автомобиле виде GPS-навигатора или в смартфоне для вычисления скорости и интенсивности движения. Это синхронизированный ненавязчивый подход, когда GPS-датчики получают данные от группы спутников, вращающихся вокруг Земли. По доступности GPS датчики получают данные от 12-ти видимых спутников. Датчик GPS должен получить данные как минимум с 4-х из 12-ти видимых спутников для точного расчета положения объекта. В дополнение к этому водители автомобилей, оснащенные смартфонами, могут использовать свои данные акселерометра, чтобы узнать скорость автомобиля и качество дороги. Точность составляет ±7,8 метров.

Это обеспечивает несколько преимуществ, так как это дешево по сравнению с датчиками или камерами. Плюс ко всему это имеет низкое обслуживание и обеспечивает данные трафика в режиме реального времени.

Датчик CO2. Число транспортных средств растет с каждым днем, за счет чего увеличивается уровень загрязнения, который необходимо обрабатывать, чтобы обеспечить умную транспортную систему. Один промилле-это одна молекула загрязняющего вещества среди 1 млн молекул воздуха. Поэтому сбор данных об уровне присутствия CO2 необходим для разумной транспортировки. Датчики CO2 используются для измерения количества углекислого газа, присутствующего в атмосфере. Наиболее распространенные датчики CO2, которые используются для загрязнения трафика называются NIDR (недисперсионный ИК-датчик) датчик. Важными компонентами датчика NIDR являются инфракрасный источник, световая трубка, интерференционный фильтр и инфракрасный детектор. Используя этот путь, мы можем простимулировать движение путем знания уровня CO2 в настоящее время. Это синхронизированная ненавязчивая техника с частотой сбора данных в полсекунды и точностью ±2 %.

Противотуманные датчики. Плохая видимость из-за сильного тумана может привести к несчастным случаям или задержке во времени. Для этого вопроса, мы можем установить датчики тумана на соответствующие места для того чтобы обеспечить умную транспортную систему. Используя датчик тумана, мы можем измерить уровень тумана в атмосфере и таким образом мы можем предупредить водителей ездить медленнее и уменьшить шансы аварии.

Это синхронизированный ненавязчивый способ сбора данных. Точность ±20.

Ультразвуковые датчики. Ультразвуковые датчики установлены на полосу движения автомобиля. Когда ультразвуковой датчик воспринимает присутствие транспортного средства на полосе движения, то он сразу передает данные в виде двоичного значения 0 или 1 в счетчик единицы измерения. Пороговое значение устанавливается, значение 1 считается высоким, а 0 низким. Ультразвуковой датчик использован из-за высокого точного ряда и имеет зону радиовидимости.

Полезно при определении плотности движения. Синхронизированный и ненавязчивый подход с точностью ±0,05 %.

Датчик магнитометра. Этот способ сбора данных использует датчик магнитометра для классификации, обнаружения и оценки скорости автомобиля. Датчики магнитометра – еще одна альтернатива индуктивным петлям, собирающим данные синхронизированным и ненавязчивым способом. Он выводит данные в формате спектра с точностью ±5 %.

Все источники данных, описанные выше, генерируют огромный объем данных. Здесь мы показали расчетный образец генерации данных для CO2 и GPS-датчиков. Каждая запись, испускаемая узлом CO2, имеет средний размер 155 байт, при этом узел датчика измеряется каждые полсекунды.

Так, есть около 7200 измерений в час и значит около 172 800 в день. Следовательно, объем данных, генерируемых узлом датчика CO2 в сутки, равен (155 * 172800) = 26 784 000 байт ≈ 32 МБ. Есть тысячи таких узлов CO2, реализованных в умном городе, которые генерируют гигабайты данных в день.

Каждый приемник GPS-датчика генерирует запись размером 26 байтв секунду. Итак, есть 3600 измерений в час, 86400 в сутки. Следовательно, объем данных, генерируемых узлом датчика GPS в сутки, равен (26*86400) = 2 246 400 байт ≈ 2 МБ. Имеется сотни тысяч таких датчиков GPS в «умном городе», которые генерируют гигабайты данных в день.

Таким образом, как показано выше, мы можем вычислить количество данных, генерируемых для каждого источника в день. Из приведенного расчета можно получить представление об объеме данных, генерируемых в среде умной транспортной системы, и, следовательно, получить данные о различных способах сбора данных, что важны для дальнейшей обработки больших объемов информации.

В приведенной ниже таблице, рассмотрены все способы сбора данных по различным параметрам. Это табличное сравнение может быть полезно для правильного выбора способов сбора данных, которые будут реализованы в умной транспортной системе. Например, для подсчета автомобилей, если в приоритете точность, то лучше выбрать индуктивный контур, в то время как если в приоритете энергопотребление, то использовать приемлемее пневматические трубки. Таким образом, табличное сравнение может быть использовано для построения умного транспорта в умном городе.

ТАБЛИЦА. Методы сбора данных

Методы сбора данных	Энергопотребление	Необходимая пропускная способность
Пневматические трубки	Низкое	Низкая
Индуктивный контур	Среднее	От низкого до умеренного
Видеодетектор автомобиля	Высокое	Высокая
GPS	Среднее	Умеренная
Датчик Co2	Низкое	Низкая
Противотуманные датчики	Низкое	Низкая
Ультразвуковыем датчики	Среднее	Низкая
Датчик магнитометра	Низкое	Низкая

Заключение

В данной работе были рассмотрены различные способы сбора данных для умной транспортной системы умного города. Может быть больше ис-

точников сбора данных, чем описано выше. Кроме того, мы можем реализовать два или более способов сбора данных для того, чтобы два обеспечивают интеллектуальное решение транспорта в лучшем виде. Вышеприведенное исследование также показывает, что объем собранных данных высок, и в силу неоднородности собранных данных должен существовать определенный общий стандарт или формат.

Список используемых источников

1. Volkov A., Khakimov A., Muthanna A., Kirichek R., Vladyko A., and Koucheryavy A. Interaction of the IoT traffic generated by a Smart city segment with SDN core network // WWIC 2017 International Conference on Wired/Wireless Internet Communication, 115-126. 0302-9743eISSN: 1611-3349 Springer-Verlag GmbH (Heidelberg).

2. Кучерявый А. Е., Прокопьев А. В., Кучерявый Е. А. Самоорганизующиеся сети. СПб. : Любавич, 2011. 312 с.

3. Masek P., Fujdiak R., Zeman K., Hosek J., Muthanna A. Remote networking technology for iot: cloud-based access for alljoyn-enabled devices // Proceedings of the 18th Conference of Open Innovations Association FRUCT and Seminar on Information Security and Protection of Information Technology 2016. PP. 200–205.

4. Fujdiak R., Masek P., Mlynek P., Misurec J., Muthanna A. Advanced optimization method for improving the urban traffic management // Proceedings of the 18th Conference of Open Innovations Association FRUCT and Seminar on Information Security and Protection of Information Technology 2016. PP. 48–53.

5. Ateya A., Muthanna A., Gudkova I., Abuarqoub A., Vybornova A., Koucheryavy A. Development of intelligent core network for tactile internet and future smart systems // Journal of Sensor and Actuator Networks. 2018. 7. № 1. PP. 1.

УДК 519.81

МНОГОФАКТОРНЫЙ АНАЛИЗ ПРОЦЕССА ФОРМИРОВАНИЯ СИСТЕМЫ РАДИОМОНИТОРИНГА И РАДИОТЕХНИЧЕСКОГО КОНТРОЛЯ

А. А. Гудков[1], А. С. Малышев[2], С. Р. Малышев[1]

[1]Военная академия связи им. Маршала Советского союза С. М. Буденного
[2]ООО «Девелопонбокс»

В статье рассматривается оптимизационная задача многофакторного анализа отдельных центров радиомониторинга и радиотехнического контроля, в основе которого лежит формальный подход, задаются этапы построения данных систем, определяются показатели эффективности, включая требования к эффективности и критерии ее оценки.

многофакторный анализ; оптимизация; радиомониторинг; радиотехнический контроль.

Многофакторный анализ систем радиомониторинга и радиотехнического контроля (СРМРТК) состоит в выборе таких параметров системы, которые:

удовлетворяют принятому критерию пригодности системы для решения возложенных на нее задач в соответствующих условиях ее функционирования;

являются предпочтительными в смысле выбранного критерия оптимальности.

Данная задача в теории сложных систем называется задачей оценивания оптимальности системы или задачей оптимизации системы. В общем случае решение задачи построения любой сложной системы состоит в решении целого ряда оптимизационных задач, каждая из которых, в зависимости от условий в которых она решается, может характеризоваться использованием различных критериев оптимальности (как в зависимости от этапа построения, так и в зависимости от того: осуществляется ее решение в условиях детерминированной определенности относительно параметров, определяющих значение оптимизируемых показателей, либо в условиях неопределенности этих параметров как стохастического, так и не стохастического характера).

Разнообразие систем и специфические особенности их функционирования не позволяют сформировать единую методику, позволяющую осуществить анализ любой технической системы. В связи с этим анализ какой-либо конкретной системы представляет собой индивидуальный процесс. В то же время, для некоторых отдельных типов систем и при определенных условиях их функционирования такие методики могут создаваться. Однако, в отношении построения СРМРТК такой методики нет.

Рассматриваемая концепция многофакторного анализа СРМРТК основывается на общих принципах системного подхода, и, в то же время, включает в себя ряд отличительных черт, обусловленных особенностями анализируемой системы:

характером получаемых данных, технологическими особенностями их обработки и динамичностью условий функционирования системы;

принципиальной многовариантностью как первоначального облика системы, так и конкретного состава оборудования в рамках рассматриваемого варианта СРМРТК.

Общая постановка оптимизационной задачи

Процесс многофакторного анализа СРМРТК, как сложной военно-технической системы, может быть осуществлен в два этапа.

На первом этапе задаются:

показатели результатов – вектор показателей частных (единичных) результатов $X_{<n>} = <x_1, x_2, ..., x_n>$;

требования к результатам – вектор предельно допустимых значений $Y_{<n>} = <y_1, y_2, ..., y_n>$ показателей результатов $X_{<n>}$;

критерий для оценки качества результатов – 2n-местный неопределенный предикат:

$$G_1 : X_{<n>} \overset{<}{>} Y_{<n>}.$$

На втором этапе определяются:

показатель эффективности – вероятность выполнения целевой задачи, стоящей перед СРМРТК [1]:

$$P_B = P\left(X_{<n>} \overset{<}{>} Y_{<n>}\right),$$

требования к уровню эффективности – минимально допустимое (требуемое) значение P_B^{TP} вероятности выполнения задачи мониторинга;

критерий для оценки эффективности – одноместный предикат:

$$G_2 : P \geq P_B^{TP}.$$

Показатель эффективности функционирования СРМРТК является комплексным показателем качества, а критерий для оценки качества результатов работы системы указывает на цель ее функционирования и требуемую степень достижения этой цели.

В качестве наиболее информативного комплексного показателя эффективности функционирования СРМРТК целесообразно выбрать вероятность выполнения задачи (достижения цели функционирования):

$$P_B = P\left(X_{<n>} \overset{<}{>} Y_{<n>}\right) = \int_{-\infty}^{\infty} \dots \int_{-\infty}^{\infty} \Phi_{X<n>}(X_{<n>}) dF_{Y<n>}(Y_{<n>}),$$

где $\Phi_{X<n>}(X_{<n>}) \overset{d}{=} P\left(X_{<n>} \overset{<}{>} X^*_{<n>}\right) = P\left[\bigcap_{i=1}^{n}\left(x_i \overset{<}{>} x_i^*\right)\right]$ – интегральный закон распределения случайного вектора $X_{<n>}$;

$F_{Y<n>}(Y_{<n>}) \overset{d}{=} P\left(Y_{<n>} \overset{<}{>} Y^*_{<n>}\right) = P\left[\bigcap_{i=1}^{n}\left(y_i \overset{<}{>} y_i^*\right)\right]$ – функция распределения случайного вектора $Y_{<n>}$.

Это справедливо при любом характере результатов функционирования СРМРТК (случайном или детерминированном) и требований к ним. Если некоторые (или все) компоненты векторов $X_{<n>}$, $Y_{<n>}$ неслучайны и определены заданными значениями, то в выражениях для интегрального закона распределения случайного вектора $X_{<n>}$ и функции распределения случайного вектора $Y_{<n>}$ они будут фигурировать как константы.

Исходя из сказанного, математическая постановка задачи многофакторного анализа имеет детерминированный характер, полностью определяемой структурой СРМРТК [2].

В силу большого количества переменных, условий и ограничений, алгоритм решения поставленных задач должен исключать необходимость явного перебора всех допустимых альтернатив. Данная задача относится к задачам большой размерности, принадлежащих к классу NP-полных [3]. Все задачи из этого класса эквивалентны по вычислительной сложности в том смысле, что если одна из них имеет эффективное (с полиноминально ограниченным временем) решение, то все они имеют эффективное решение.

Одним из способов получения решения для подобного класса задач является применение метода так называемого децентрализованного управления, предложенного для задач линейного программирования блочного типа (метод декомпозиции Данцига-Вульфа), с дальнейшим выходом на целочисленную постановку задачи [4].

Постановка задачи определения оптимального состава СРМРТК

Постановка задачи определения оптимального состава аппаратно-программных средств (АПС) СРМРТК в общем виде может быть сформулирована и записана следующим образом:

$$\vec{f}\ (\vec{x}) = \left(f_1(\vec{x}), f_2(\vec{x}), ..., f_k(\vec{x})\right) \to \underset{\vec{x}\in\Delta\beta}{extr},$$

где Δ_β – конечное или счетное множество допустимых вариантов состава АПС, используемых для построения СРМРТК.

Конечное или счетное множество допустимых альтернатив во многом определяется значениями параметров, которые характеризуют качественный и количественный состав СРМРТК.

При решении задачи анализа основным параметром является стоимость СРМРТК, т. е. в качестве целевой функции будет выступать общая стоимость системы:

$$I^C = I^C_{S_L} + I^C_{S_V} + I^C_{S_N},$$

где индексы *L*, *V* и *N* подразумевают, соответственно, стоимостные характеристики энергозатрат; стоимостно-площадные характеристики и стоимостные характеристики по содержанию и обеспечению штатного состава.

Общая методика решения задачи многофакторного анализа СРМРТК

Исследования показали, что для каждой из выделенных подсистем с помощью разработанных математических подмоделей необходимо рассчитать оптимальный состав технических средств и программных продуктов.

При решении задач многофакторного анализа при заданных условиях и ограничениях традиционным путем, получение решения происходит с использованием методов динамического, линейного и целочисленного линейного программирования. Известные подходы в силу большой размерности задачи имеют ряд недостатков, к которым относятся низкое быстродействие алгоритмов и значительные затраты памяти ЭВМ, что затрудняет получение высокоэффективного программного продукта. Этим методом может быть модифицированный метод неявного перебора, который после соответствующей настройки на конкретную технологию решения задач анализа дает положительный эффект. Применение этого метода в сравнении с методом отсечения (Гомори), основанного на симплекс-методе (решении задачи линейного программирования) дает более эффективное решение.

Список используемых источников

1. Абчук В. А., Матвейчук Е. Т., Томашевский Л. П. Справочник по исследованию операций. М. : МО СССР, 1979, 736 с.

2. Морозов Л. М., Петухов Г. Б., Сидоров В. Н. Методологические основы теории эффективности: учебное пособие. Л. : МО СССР, 1979. 236 с.

3. Ахо А., Хопкрофт Дж., Ульман Дж. Построение и анализ вычислительных алгоритмов. М. : Мир, 1979. 536 с.

4. Вагнер Г. Основы исследования операций. Т. 2. М. : Мир, 1973. 490 с.

УДК 681.324

ОПТИМИЗАЦИИ ХАРАКТЕРИСТИК МНОГОУЗЛОВЫХ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ

З. Н. Гусейнов, П. Д. Мурадов, А. Ш. Сулейманов

Азербайджанский технологический университет

Основной отличительной особенностью современных телекоммуникационных сетей является доставка различного рода пакетов информации в пункт назначения по различным маршрутам. Основной целью настоящего исследования является определение зависимости потерь пакетов от загрузки и ресурсов сети. Предложены математические модели для расчетов вероятности отказов в обслуживании в многоканальных одноузловых и многоканальных многоузловых сетях с ограниченной очередью и абсолютным приоритетом.

качество обслуживания, Интернет протокол, система массового обслуживания, многоузловая, одноузловая, многоканальная сеть.

Производительность и качество обслуживания (*Quality of Service* – QoS) – это ключевые понятия для сети Интернета. Вопросы качества обслуживания (QoS) в сети Интернет в последнее время становятся особенно актуальными, поскольку от их решения напрямую зависит архитектура перспективной сети связи. За последние несколько лет в рамках организации IETF (*Internet Engineering Task Force* – проблемная группа инженерной поддержки Интернета) ведущими специалистами было предложено несколько архитектур и механизмов призванных в той или иной степени обеспечивать QoS. В работе [1] по результатам анализа новых протоколов сети Интернета, гарантирующих QoS, а также на основе конвергенции технологии ATM (*Asuchronous Transfer Mode* – асинхронный режим передачи) и IP (*Internet Protocol* – Интернет – протокол), предложена структура перспективной сети связи с коммутацией пакетов.

В перспективной сети связи с коммутацией пакетов ядро сети (магистральная сеть) строится с применением ATM, MPLS (*MultiProtocol Label Switching*-многопротокольная коммутация по меткам) и DiftServ (*Differentiated Services*, DS – архитектура дифференцированных служб). Сети доступа организуются с использованием IntServ (*Integrated Services Architecture* – архитектура интегрированных служб) и RSVP (*Resource reservation Protocol* – протокол резервирования ресурсов). Ядро сети обеспечивает QoS для сложного агрегированного трафика. Сеть доступа организует процедуры классификации, маркирования и измерения трафика, а также QoS для поступающего неагрегированного трафика.

В настояще работе оптимизируются характеристики такой сети в отношение QoS.

Рассмотрим многоканальную систему массового обслуживания (СМО), имеющую k мест ожидания. На вход системы поступают два потока требований с интенсивностями λ_1 и λ_2 соответственно. Функции распределения времени обслуживания требований первого и второго приоритетов экспоненциальные с параметром $\mu = 1$. В этом случае интенсивность входящей нагрузки первого и второго приоритетов будет соответственно равна ρ_1 и ρ_2. Первый поток имеет абсолютный приоритет перед вторым потоком.

В многоканальных одноузловых телекоммуникационных сетях с ограниченной очередью и абсолютным приоритетом вероятность отказа для потока запросов первого приоритета из-за ограниченности очереди в обслуживании определяется следующей зависимостью [2]:

$$P_1 = \frac{\rho_1^{\,s+k}}{s^k s!}\left[\sum_{\nu=0}^{s}\frac{\rho_1^{\,\nu}}{\nu!} + \frac{\rho_1^{\,s}}{s!}\sum_{j=1}^{k}\left(\frac{\rho_1}{s}\right)^j\right]^{-1}, \qquad (1)$$

где s – количество каналов; k – количество мест ожиданий; ρ_1 – нагрузка первого приоритета.

При $s=1$ можно получить зависимость для одноканальной сети с ограниченной очередью и абсолютным приоритетом.

Вероятность отказа в обслуживании для запросов второго приоритета равна вероятности того, что в очереди уже стоит k требований первого и/или второго приоритетов:

$$P_2 = \frac{(\rho_1+\rho_2)^{s+k}}{s^k s!}\left[\sum_{\nu=0}^{s}\frac{(\rho_1+\rho_2)^{\nu}}{\nu!}+\frac{(\rho_1+\rho_2)^{s}}{s!}\sum_{j=1}^{k}\left(\frac{\rho_1+\rho_2}{s}\right)^{j}\right]^{-1}, \qquad (2)$$

где ρ_1 – нагрузка первого приоритета; ρ_2 – нагрузка второго приоритета.

Для расчета разработан алгоритм решение задачи. Расчет по этому алгоритму выполнен с помощью программы Excel, также составлена программа на языках высокого уровня.

Переходим к получению математической модели для многоканальной многоузловой сети. Для получения математической модели можно использовать положение теории вероятности и математической статистики. Согласно которого последовательность $A_1, A_2, A_3, \ldots$ случайных событий называется монотонно возрастающей (неубывающей) или монотонно уменьшающий (невозрастающий), если $A_i \in A_{i+1}$ для каждого $n=1,2,3,\ldots$ Объединение всех событий такой последовательности будем записывать как [3]:

$$\sum_{i=1}^{\infty} A_i = \lim_{i\to\infty} A_i \quad \text{или} \quad \prod_{i=1}^{\infty} A_i = \lim_{i\to\infty} A_i\,. \qquad (3)$$

Так как в многоканальных многоузловых телекоммуникационных сетях с ограниченной очередью и абсолютным приоритетом вероятность отказа с увеличением количество используемых узлов коммутации увеличивается, с учетом (3) из выражений (1) и (2) для одноприоритетных и двухприоритетных обслуживаниях можно получить следующие математические модели для расчета вероятности отказов в многоканальных многоузловых телекоммуникационных сетях.

Если считать вероятности отказов узлов одинаковыми математическая модель для определения вероятности отказа в многоканальных многоузловых телекоммуникационных сетях для запросов первого приоритета из-за ограниченной очереди в обслуживании получить следующий вид:

$$P_{1m} = \sum_{i=1}^{N}\frac{\rho_{i1}{}^{s_i+k_i}}{s_i{}^{k_i} s_i!}\left[\sum_{\nu=0}^{s_i}\frac{\rho_{i1}{}^{\nu}}{\nu_i!}+\frac{\rho_{i1}{}^{s}}{s_i!}\sum_{j=1}^{k_i}\left(\frac{\rho_{i1}}{s_i}\right)^{j}\right]^{-1}, \qquad (4)$$

где N – количество узлов сети; ρ_i – нагрузка первого приоритета, s_i – количество каналов, k_i – количество мест ожиданий i-го узла сети.

Если считать вероятности отказов узлов одинаковыми математическая модель вероятности отказов в многоканальных многоузловых телекоммуникационных сетях для запросов второго приоритета из-за ограниченной очереди в обслуживании получить следующий вид:

$$P_{2m} = \sum_{i=1}^{N} \frac{\left(\rho_{i1} + \rho_{i2}\right)^{s_i + k_i}}{s_i^{k_i} s_i!} \left[\sum_{\nu=0}^{s_i} \frac{\left(\rho_{i1} + \rho_{i2}\right)^{\nu}}{\nu!} + \frac{\left(\rho_{i1} + \rho_{i2}\right)^{s_i}}{s_i!} \sum_{j=1}^{k_i} \left(\frac{\rho_{i1} + \rho_{i2}}{s_i} \right)^{j} \right]^{-1}, \quad (5)$$

где ρ_{i2} – нагрузка второго приоритета i-го узла сети.

Расчет выполнялся по разработанному алгоритму.

При проектировании конкретной сети связи необходимо учитывать реальной вероятности отказов проектируемых узлов сети.

Расчеты по полученным моделям выполнялись для различного количества узлов сети (N), количества мест ожиданий (k) и количества параллельных каналов (s). При получении численных расчетов и построения графиков использована программа Excel, а также составлена программа на языках высокого уровня.

В таблице 1 приведены результаты расчетов вероятности отказов в обслуживании для запросов первого и второго приоритетов при различном количестве узлов коммутации (N), параллельных каналов (s) и мест ожиданий (k). Нагрузка второго приоритета – $\rho_2 = 0{,}8$.

ТАБЛИЦА. Результаты расчетов вероятности отказов в обслуживании для запросов второго приоритета при различном количестве N, s и k ($\rho_2 = 0{,}8$)

ρ1	Вероятность отказа – P_{2m}								
	$N = 1$			$N = 2$			$N = 3$		
	$s = 2$	$s = 3$	$s = 4$	$s = 2$	$s = 3$	$s = 4$	$s = 2$	$s = 3$	$s = 4$
	$k = 20$	$k = 6$	$k = 3$	$k = 24$	$k = 8$	$k = 5$	$k = 26$	$k = 10$	$k = 5$
0,2	1,59E-07	8,31E-05	0,000239	1,99E-08	0,00002	2,99E-05	7,45E-09	3,08E-06	4,48E-05
0,4	6,58E-06	3,50E-04	0,0007	1,71E-06	0,00011	1,26E-04	9,21E-07	2,66E-05	1,89E-04
0,6	0,000138	1,11E-03	0,001682	6,63E-05	0,00048	4,12E-04	4,87E-05	1,58E-04	6,18E-04
0,8	**0,001651**	**2,95E-03**	**0,003491**	**0,001347**	**0,00168**	**1,11E-03**	**0,001292**	**7,20E-04**	**1,67E-03**
1	0,011433	6,68E-03	0,006476	0,014489	0,00478	2,61E-03	0,017389	2,58E-03	3,92E-03
1,2	0,044444	1,33E-02	0,010989	0,075472	0,0117	5,45E-03	0,105263	7,74E-03	8,17E-03
1,4	0,102985	2,40E-02	0,01734	0,197648	0,025	1,03E-02	0,292059	1,99E-02	1,55E-02
1,6	0,169481	3,93E-02	0,025759	0,336024	0,0476	1,81E-02	0,502796	4,41E-02	2,71E-02

ρ1	Вероятность отказа – P_{2m}								
	$N = 1$			$N = 2$			$N = 3$		
	$s = 2$	$s = 3$	$s = 4$	$s = 2$	$s = 3$	$s = 4$	$s = 2$	$s = 3$	$s = 4$
	$k = 20$	$k = 6$	$k = 3$	$k = 24$	$k = 8$	$k = 5$	$k = 26$	$k = 10$	$k = 5$
1,8	0,231407	5,94E-02	0,036367	0,461984	0,0815	2,96E-02	0,692703	8,61E-02	4,44E-02
1,9	0,285864	8,41E-02	0,049169	0,571506	0,127	4,55E-02	0,857202	1,49E-01	6,83E-02

Из таблицы видно, что для обеспечения требуемого значения QoS необходимо обеспечить требуемое количество параллельных каналов между конкретными узлами сети, а также определить оптимальное количество мест ожидания (емкость накопителя) в ее соответствующих узлах коммутации. Анализы численных расчетов вероятности отказов в многоканальных и многоузловых сетях с ограниченной очередью и двухприоритетным обслуживанием показывают, что увеличение нагрузки первого приоритета более 0,8 Эрланга приводит к значительному увеличению вероятности отказов требований второго приоритета.

Список используемых источников

1. Кучеряевый А. Е., Кучеряевый Е. А., Харью Я. Качество обслуживания в сети Интернет // Электросвязь. 2002. № 1. С. 9–14.

2. Гасанов А. Н., Мурадов П. Д. Анализ телекоммуникационных сетей с современной технологией // Ученые записки. 2010. С. 11–16.

3. Теория телетрафика; пер. с нем. / Под ред. Г. П. Бошарина. М. : Связь, 1971. 320 с.

УДК 004.77

ПОДХОД К РАЗРАБОТКЕ И ОЦЕНКЕ ПРОТОКОЛА УДАЛЕННОЙ АТТЕСТАЦИИ JAVA-ПРОГРАММ

В. А Десницкий[1, 2], П. И. Думенко[1]

[1]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
[2]Санкт-Петербургский институт информатики и автоматизации Российской академии наук

В работе предложен подход к разработке и оценке протокола удаленной аттестации на примере программы, реализующей заданный вычислительный процесс с использованием языка программирования Java. Предлагаемая защита основывается

на организации двух методах: методе проверки контрольных точек и методе контрольных сумм критически важных структур данных, которые задействованы в определенных местах кода нашей Java-программы.

удаленная аттестация, контрольная точка, контрольная сумма, критически важная структура данных.

Современный информационно-телекоммуникационные системы состоят из разнообразных вычислительных устройств, телекоммуникационных технологий, кибер-физических устройств, компонентов обработки информации и программного обеспечения (ПО). Для обеспечения безопасности таких систем применяют комплексы мер для их защиты от актуальных угроз [1]

Проблема защиты программного обеспечения (ПО) от несанкционированной модификации является чрезвычайно актуальной, вследствие высоких потерь нелегитимного распространения программного кода и рисков внесения в него несанкционированных изменений.

В работе анализируются методы защиты программного кода и данных информационно-телекоммуникационных систем информации с использованием протокола удаленной аттестации [2]. Действенность предлагаемых решений подтверждается на примере задачи защиты программного кода на языке Java.

Удаленная аттестация используется для контроля целостности программы. При этом пользователь может отследить появление несанкционированных модификаций, преследующих цель взлома программного обеспечения (ПО), либо снятия определенных ограничений на использование продукта. Данный метод предполагает, что в программу встраиваются определенные функции, которые непрерывно или время от времени отсылают на сторону контролирующего доверенного сервера небольшие фрагменты данных, именуемые впоследствии «подписями» [3]. На серверной стороне, в свою очередь, происходит проверка корректности полученных подписей и делается вывод о том, поступила ли несанкционированная модификация этой программы со стороны некоторого злоумышленника или нет.

В тестовое программное приложение на языке Java, состоящее из нескольких важных конструкций `if-else` и циклов, а также некоторой структуры данных – в простейшем случае простой целочисленной переменной, встраивается разработанный компонент клиент-серверной защиты. При этом реализуются следующие два программных метода:

– метод проверки контрольных точек;

– метод контрольных сумм критически важных структур данных программы.

Метод контрольных точек основывается на распределении специализированных меток в определенных местах исходного кода Java-программы.

Таким образом, при достижении потока управления программы такой точки – срабатывает команда по отправке определенного маркера на серверную сторону. Серверная часть разработанного механизма защиты Java-программы собирает последовательность таких точек для работающего каждого экземпляра клиентской программы и проверяет ее корректность по заранее подготовленному шаблону [3]. При этом сервер обладает информацией о получении с клиентской стороны маркеров и формирует тестирующий граф. В конечном итоге, если программа была несанкционированно модифицирована злоумышленником, последовательность пройденных контрольный точек будет отличаться от ожидаемой, и сервер сможет это установить. Ниже приведен фрагмент программного кода целевого приложения, в который встраиваются операции метода проверки контрольных точек.

```
public class Client {

public static void main(String[] args) throws IOException {
try(ServerSocket serverSocket = new ServerSocket(8189);
Socket socket = serverSocket.accept();
Scanner scanner = new Scanner(socket.getInputStream())){
Scanner in = new Scanner(System.in);
double a, b, c, D;
double x, x0, x1, x2;
String str;
PrintWriter printWriter = new
 PrintWriter(socket.getOutputStream(),true);
```

Для организации сетевого соединения между серверной и клиентской частью механизма защиты по протоколу удаленной аттестации и передачи на серверную сторону программных маркеров были использованы Java-сокеты [4]. Сокеты – это программный интерфейс для обеспечения обмена данными между процессами, располагающимися на хостах. При этом запускается программное обеспечение сервера, которое осуществляет прослушивание указанного в коде порта, а клиентская программа производит подключение к данному порту. После установления соединения происходит обмен данными между клиентом и сервером. Сокет в Java-программе выступает в роли «розетки» и может быть инициированным, как на клиентской, так и на серверной стороне, инициализируясь по определенному числовому порту. Ниже приведен фрагмент программного кода защищаемого Java-приложения со встроенными операциями отправки программных маркеров.

```
while (true) {
//Посылаем A
printWriter.println("A");
try {
System.out.println("Введите ваше уравнение: ");
```

```
str=in.next();
//Посылаем B
printWriter.println("B");
System.out.print("Введите значение переменной a: ");
a = in.nextDouble();
//Посылаем C
printWriter.println("C");
System.out.print("Введите значение переменной b: ");
b = in.nextDouble();
//Посылаем D
printWriter.println("D");
System.out.print("Введите значение переменной c: ");
c = in.nextDouble();
//Посылаем E
printWriter.println("E");
```

Серверная сторона принимает данную последовательность и осуществляет проверку ее корректности путем обхода графа (рис.). Как только программа начала свое выполнение, клиент посылает первую подпись в виде маркера «A», затем программа обращается к следующему фрагменту кода и посылает второй маркер «B». После того, как все необходимые переменные были введены пользователем с клавиатуры, на серверной стороне образовывается следующая последовательность из подписей «A», «B», «C», «D» и «E». Внедренные в защищаемое приложение программные маркеры позволяют проверить корректность программного управления и передачи управления в рамках конструкций `if-else`. Получение маркера «J» свидетельствует об окончании выполнения программы и выхода из цикла `while(true)`. Таким образом, если последовательность маркеров изменяется или принимает ложный характер, то компонент защиты на серверной стороне способен сделать вывод о несанкционированном изменении кода Java-программы.

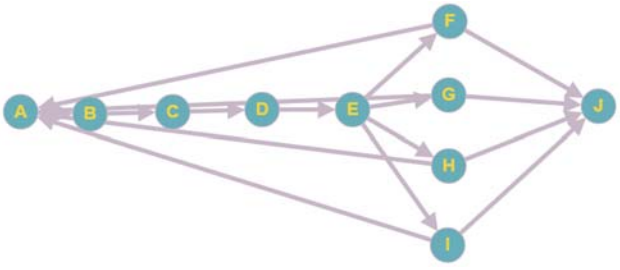


Рисунок. Модель ориентированного графа на стороне сервера

На сервере за формирование графа отвечает специальный класс DirectedGraph, который хранит информации о заранее подготовленном шаблоне.

Второй из предложенных методов основывается на проверке контрольных суммах критически важных структур данных Java-программы [5]. Параллельно с основным потоком (*thread*) программы, выполняющим его основную бизнес-логику, запускается дополнительный поток, который периодически отсылает результат хеш-функции, примененной к некоторой структуре данных или нескольким таким структурам.

Хеш-код определяет целое число фиксированной длины, которое, можно допускать, является уникальным идентификатором содержимого объекта. В результате выполнения целевой программы в консоли отобразится конкретное число, именно оно и является нашим хеш-значением. В терминологии Java хеш-код – это целочисленный результат работы метода, которому в качестве параметра передан объект и представлен в виде числа примитивного типа int, который равен 4-м байтам и помещается в диапазоне от –2 147 483 648 до 2 147 483 647.

В рамках Java-программы на клиентской стороне формируется массив определенной длины, для которого вычисляется его хеш-значение. В последствие сервер принимает все необходимые данные на проверку и сравнивает полученные хеш-коды [6]. Для одного и того же объекта значения хеш-функций будут всегда одинаковыми. Если в какой-то момент на сервере обнаружено, что хеш-значение стало отличаться от ожидаемого, то это свидетельствует о возможной несанкционированной модификации этих данных.

В Java-программе за вычисление хеш-значения отвечает метод `hash.Code()`, который переопределенный в наследниках Object. Если говорить о хешировании более простым языком, то это способ преобразования любой переменной или объекта в уникальный код после применения определенного алгоритма к их свойствам. Хеш-функция должна возвращать неизменный хеш-код всякий раз, когда она применена к одному и тому же или идентичным объектам.

Проведенные в рамках разработанного программного прототипа механизма защиты эксперименты показали выполнимость предложенных и реализованных методов защиты Java-программ от модификаций.

В качестве направлений дальнейших исследований предполагаются построение классификации существующих методов защиты программного обеспечения от несанкционированных модификаций, оценка уровня их защищенности и исследование механизмов автоматизированного встраивания в защищаемое программное обеспечение компонентов его защиты.

Работа выполнена в СПИИРАН при поддержке Гранта президента Российской Федерации № МК-5848.2018.9.

Список используемых источников

1. Казарин О. В. Безопасность программного обеспечения компьютерных систем: монография. М. : МГУЛ, 2003. 212с.
2. Воскресенский Г. А., Чаплыгин А. М. Способы защиты от компьютерных атак на сетевую карту [Электронный ресурс] // Вопросы кибербезопасности: электрон. науч. журнал 2013. N 3. С. 12–15.
3. Десницкий В. А., Котенко И. В. Модель защиты программного обеспечения на основе механизма «удаленного доверия» // Известия высших учебных заведений. Приборостроение. 2008. Т. 51. № 11. С. 26–31.
4. Дубаков А. А. Сетевое программирование: учебное пособие. СПб. : НИУ ИТМО, 2013. 248 с.
5. Десницкий В. А., Чечулин А. А., Котенко И. В., Левшун Д. С., Коломеец М. В. Комбинированная методика проектирования защищенных встроенных устройств на примере системы охраны периметра // ТРУДЫ СПИИРАН. 2016. № 5 (48). С. 5–31.
6. Разбираемся с hashCode() и equals() [Электронный ресурс] // Хабрахабр. URL: https://habrahabr.ru/post/168195/ (дата обращения 29.03.2018).

УДК 004.056

ИССЛЕДОВАНИЕ ВНЕДРЕНИЯ ШИФРОВАНАНИЯ И АУТЕНТИФИКАЦИИ НА ФУНКЦИОНИРОВАНИЕ КРИПТОВАЛЮТ

В. В. Добрянский, Д. В. Кушнир

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

Обеспечение конфиденциальности информации является частью подавляющего большинства информационных систем. Однако только в настоящее время начинают внедряться методы обеспечения шифрованного аутентифицированного канала в криптовалютах. Без обозначенной защиты мониторинг сети и анализ незашифрованных данных способны поставить конфиденциальность информации под угрозу.

В работе рассматриваются особенности внедрения BIP 151 – предложения по созданию защищенного соединения при использовании неполных узлов, что позволяет избежать целого ряда атак на систему.

биткоин, криптовалюта, SPV, шифрование, аутентификация, безопасность.

Широкое распространение в последнее время целого спектра криптовалют привлеко внимание к ним большого количества новых пользователей, которые уверены в криптографической защищённости используемых меха-

низмов. Такие пользователи полагают наличие защищённости функционирования всех аспектов работы, выбранной криптовалюты, например, Биткоина. Однако, в настоящее время, сеть Биткоин не создаёт защищенного соединения между пользователями, таким образом, транзакции и блоки передаются от узла к узлу в открытом виде. Это создаёт проблемы в безопасности системы, так как позволяет третьим лицам манипулировать трафиком, отслеживать действия пользователей и проводить анализ перехваченных данных. В основном, данная угроза может оказать значительное влияние на конфиденциальность лишь для кошельков пользователей с упрощенной проверкой платежей (SPV – *Simplified Payment Verification*), поскольку они полагаются на подключение к «доверенному» узлу [1].

Очевидно, что многие пользователи не осведомлены о тех мерах безопасности, которые действительно важны и эффективны. Возможно, они предприняли попытки по сохранению закрытого ключа в тайне при помощи аппаратного кошелька, но на данный момент для таких устройств еще не установлены единые стандарты, а это означает, что нельзя полагаться на них полностью. К тому же они не способны обеспечить защищенное подключение к полным узлам. Многие пользователи одновременно разворачивают полный узел и используют SPV клиент на мобильном устройстве, но при этом у них нет возможности связать их между собой. Это означает, что пользователи проверили блокчейн, но не могут пользоваться им с мобильного устройства в полной мере.

Для провайдера или любого другого «человека посередине» сбор сведений и идентификация пользователя является простой задачей. К примеру, при совершении какой-либо покупки в магазине с использованием SPV кошелька необходимо подключиться к интернету, и, тем самым, оставить информацию о своём устройстве, и, как следствие, о себе.

SVP кошельки для проверки существования той или иной транзакции используют фильтр Блума [2], который представляет собой вероятностный фильтр поиска. Шаблон поиска создается SVP узлом и включает в себя все адреса из кошелька клиента и pay-to-public-key-hash сценарий [2], который будет ожидать закрывающий сценарий scriptPubKey [2]. Полученные шаблоны добавляются в фильтр Блума, который далее, в виде компактного пакета данных, отправляется полному узлу для фильтрации и поиска транзакций. Эти пакеты могут быть использованы для определения того, какие биткоин-адреса принадлежат пользователю.

Установление защищенного соединения между узлами одноранговой сети возможно с помощью таких механизмов как: VPN, NAT, stunnel или Tor, но данные решения не практичны в использовании применительно к SPV, поскольку уязвимы к атакам направленным на деанонимизацию пользователей путем связывания их публичного адреса кошелька с IP-

адресом. Кроме того, следует учесть, что задействование упомянутых механизмов требует привлечения дополнительного программного обеспечения и обеспечения соответствующих требований к их безопасности на своём уровне, что в общем случае может быть трудно реализуемым. Поэтому для обеспечения унифицированного подхода к безопасности для каждого пользователя в равной степени шифрование должно быть реализовано непосредственно в самом протоколе биткоина.

Важным шагом в решении данной проблемы может являться внедрение подходов, предложенных в BIP 151 (*Bitcoin Improvement Proposal*) [3], в котором описывается метод обеспечения шифрования данных между конечными узлами.

BIP 151 предлагает вместо распространенных криптографических стандартов TLS/SSL использовать «Chacha20/Poly1305@openssh» [4], чтобы избежать потенциальных угроз безопасности.

«Chacha20» – это потоковый шифр семейства «Salsa». Он состоит из 20-ти раундов и принимает на входе 96-битное значение nonce и 256-битный ключ, сформированные при помощи криптографически стойкого генератора псевдослучайных чисел, а также значение для 32-битного счетчика блоков [4].

«Poly1305» – одноразовый аутентификатор. Он вычисляет 128-битный аутентификатор сообщения (тег) любой длины, используя 16-байтовый nonce (уникальный номер сообщения) и одноразовый 32-байтовый секретный ключ, который получается при помощи блочной функции ChaCha20 [4].

«Chacha20/Poly1305@openssh» объединяет два этих механизма в режим аутентифицированного шифрования с присоединенными данными (AEAD – *Authenticated Encryption with Associated Data*) [5].

Процесс установления защищенного соединения будет происходить следующим образом [3]:

1) Узел, запрашивающий шифрованное соединение, генерирует сеансовую пару ключей на основе эллиптических кривых и отправляет инициирующее сообщение принимающему узлу, после чего дожидается подтверждающего сообщения.

2) Ответный узел выполнят аналогичные действия.

3) Параллельно с этим происходит формирование симметричного ключа шифрования по протоколу Диффи-Хеллмана на эллиптический кривых.

4) После успешного взаимодействия, инициирующего и подтверждающего сообщений стороны должны передавать зашифрованные сообщения. Передача незашифрованных сообщений приведет к завершению сеанса.

5) Оба узла вычисляют 256-битный идентификатор сеанса, который может быть использован для идентификации текущего защищенного сеанса.

6) После установления шифрованного соединения может быть выполнена аутентификация узлов. Для этого обмен открытыми ключами идентификации (такие ключи создаются отдельно для каждого сетевого интерфейса до момента установления шифрованного соединения), должен быть произведен по другому каналу связи [6].

Внедрение описанных механизмов в процесс взаимодействия узлов сети усложняет противнику выполнение атаки «человек посередине». Узлы устанавливают шифрованное соединение друг с другом без аутентификации. Злоумышленник по-прежнему может заменить ключи в обоих направлениях и прослушивать проходящую через него информацию. Однако, теперь шанс его обнаружения очень велик, поскольку противник не знает, будут ли узлы проводить аутентификацию друг с другом. Если же нарушитель контролирует всю сеть, то шанс его обнаружения становится еще больше, поскольку какой-нибудь из узлов определенно выполнит аутентификацию.

Во время аутентификации узлы обмениваются сообщениями, содержащими хеш от идентификатора их защищенного сеанса и открытого ключа идентификации, который каждый из них ожидает, а также подписями идентификатора защищенного соединения, выполненными на основе их закрытых ключей идентификации. Узлы производят проверку полученный данных, и если один из узлов окажется невалидным, то ему будет направлено ответное сообщение, содержащее 64 байта нулей.

За счет своей компактной реализации, требующей малого количества ресурсов, «ChaCha20/Poly1305» обладает высокой степенью производительности при низких вычислительных затратах, благодаря чему подходит для использования в мобильных устройствах. Так, согласно тестам, проведенным компанией Google скорость шифрования данных на мобильных устройствах при помощи «ChaCha20/Poly1305» в три раза быстрее скорости шифрования AES-GCM [7]. Результаты тестирования приведены в таблице.

ТАБЛИЦА. Скорость шифрования на распространенных мобильных ЦПУ

Процессор	AES-GCM	ChaCha20/Poly1305
OMAP 4460	24,1 Мб/с	75,3 Мб/с
Snapdragon S4 Pro	41,5 Мб/с	130,9 Мб/с

Также данный механизм шифрования призван минимизировать утечку информации при таком типе атаки по побочным каналам, как атака по времени, поскольку в реализации ChaCha используется алгоритм ARX, основанный на постоянных во времени операциях: ADD, битовый сдвиг и XOR.

Этапы внедрения BIP 151:

1. Одобрение предложения сообществом Bitcoin Core.

2. Тщательная проверка кода предложенного механизма.

3. Внедрение кода в ветку релиза Bitcoin Core, которая, в дальнейшем, станет новой версией этого ПО.

4. Процесс голосования для активации BIP 151 в Bitcoin Core (требуется поддержка не менее 95 % вычислительной мощности сети – майнеров [2]).

Поскольку предложенный в BIP 151 механизм создания защищенного соединения не затрагивает уровень консенсуса, который является важным в сети Биткоин, то любой пользователь, в случае успешного проведения процесса голосования, может активировать его в своем Bitcoin Core кошельке по собственному желанию. Очевидно, что если, к примеру, один из двух узлов не активировал поддержку данного механизма, то данные продолжат передаваться в открытом виде.

Подобного рода изменения в исходном коде Биткоин называются софтфорками. Для софтфорка характерно временное разделение сети на две части – происходит разветвление цепи блокчейн. Это означает, что одна половина пользователей будет видеть набор транзакций отличный от транзакций для другой половины. В результате может возникнуть ситуация, при которой одна цепь перестанет быть валидной, и пользователи, использовавшие её, потеряют все свои средства. По этой причине внедрение BIP 151 все еще не было осуществлено. Большинство пользователей сомневаются в эффективности этого механизма из-за его процесса аутентификации, который осуществляется в ручном режиме и требует наличия отдельного, надежного канала связи между пользователями, из-за чего процесс эксплуатации данного предложения усложняется. В настоящее время использование такого метода аутентификации эффективно лишь в ситуации, когда у каждого пользователя есть свой полный узел, на котором они производят настройку защищенного соединения со своим SPV клиентом, с которым и осуществляют аутентификацию. Поэтому необходимо продолжить поиски метода аутентификации, который будет не только оптимальным для всех пользователей, но и будет соответствовать децентрализованной модели сети Биткоин.

Список используемых источников

1. Nakamoto S. Bitcoin: A Peer-To-Peer Electronic Cash System [Электронный ресурс] // bitcoin.org. URL: https://bitcoin.org/bitcoin.pdf (дата обращения 22.11.2017).

2. Antonopoulos A. M. Mastering Bitcoin. 1th ed. Sebastopol, CA: O`Reilly Media, 2014. pp. 259.

3. Schnelli J. Peer-to-Peer Communication Encryption [Электронный ресурс] // github.com. URL: https://github.com/bitcoin/bips/blob/master/bip-0151.mediawiki (дата обращения 17.11.2017).

4. Nir Y., Langley A. ChaCha20 and Poly1305 for IETF Protocols [Электронный ресурс] // rfc-editor.org. URL: https://www.rfc-editor.org/rfc/rfc7539.txt (дата обращения 09.12.2017).

5. Википедия – сводная энциклопедия, AEAD-режим блочного шифрования [Электронный ресурс] // ru.wikipedia.org. URL: https://en.wikipedia.org/wiki/Authenticated_encryption (дата обращения 09.12.2017).

6. Schnelli J. Peer Authentication [Электронный ресурс] // github.com. URL: https://github.com/bitcoin/bips/blob/master/bip-0150.mediawiki (дата обращения 13.12.2017.

7. Bursztein E. Speeding up and strengthening HTTPS connections for Chrome on Android [Электронный ресурс] // security.googleblog.com. URL: https://security.googleblog.com/2014/04/speeding-up-and-strengthening-https.html (дата обращения 22.12.2017).

УДК 004.056

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СЕТЕЙ ИМПЛАНТИРУЕМЫХ УСТРОЙСТВ: ОСНОВНЫЕ ТЕНДЕНЦИИ

Е. В. Дойникова[1,2], С. В. Савков[1,2], Е. А. Чумак[2]

[1]Санкт-Петербургский институт информатики и автоматизации Российской академии наук
[2]Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

В работе рассматриваются основные направления исследований в области информационной безопасности сетей имплантируемых устройств. Их актуальность объясняется тем, что данные системы непосредственно связаны с телом человека, и атаки на них могут нанести непоправимый ущерб здоровью. Приводятся ключевые особенности таких сетей и самих имплантируемых устройств, определяющие основные требования к их безопасности. Выделяются и классифицируются слабые места таких систем и характерные угрозы безопасности. Анализируются существующие методики оценки защищенности и средства защиты, их достоинства и недостатки. В дальнейшей работе планируется разработать методику оценки и обеспечения защищенности сетей имплантируемых устройств с учетом недостатков существующих систем.

сети имплантируемых устройств, имплантируемые устройства, защищенность, оценка защищенности, средства защиты, эффективность.

В настоящее время человечество неразрывно связано с информационными технологиями. Одной из важнейших областей человеческой жизни, на которую сильно повлияло их развитие, является здравоохранение. Информатизация затронула как процессы регистрации и обработки данных

о пациентах, так и различное медицинское оборудование. В последние годы наблюдается существенный рост рынка носимой электроники в здравоохранении (по данным ABI Research в 2016 г. их поставки в мире составили 8 млн шт. [1]). К ней относятся терапевтические медицинские устройства, носимые устройства мониторинга и диагностики и устройства для фитнеса и спорта. Ее преимуществом является возможность постоянного удаленного наблюдения за состоянием пациента. Также развивается сфера имплантируемых устройств (ИУ), способных выполнять как схожие с носимой электроникой функции сбора данных (к ним относятся измеритель кровяного давления, датчик движения, пульсометр, датчик положения в пространстве, датчик температуры, устройства, снимающие ЭКГ и ЭЭГ), так и функции профилактики и лечения заболеваний (к ним относятся имплантируемые кардиостимуляторы, инсулиновые помпы, инъекторы глюкозы, стимуляторы спинного мозга). Преимущества ИУ в том, что нет необходимости их постоянно заряжать, их невозможно потерять и ненужно носить с собой. Таким образом формируется медицинская инфраструктура, позволяющая удаленно следить за здоровьем человека и при необходимости поддерживать его. Так, в России, в рамках национальной технологической инициативы HealthNet [2], к 2035 г. планируется подключение большинства граждан к системе круглосуточного мониторинга, что позволит как предупредить различные проблемы со здоровьем пациентов, так и обеспечит возможность оперативной экстренной помощи.

Однако, элементы данной инфраструктуры, в том числе ИУ могут быть использованы в злонамеренных целях. В силу того, что все предписанные им задачи так или иначе связаны со здоровьем человека, эти устройства требуют повышенного внимания с точки зрения обеспечения безопасности. Данное исследование показало, что этим вопросам в нашей стране в настоящее время уделяется недостаточное внимание.

Данная работа посвящена существующим тенденциям в области обеспечения информационной безопасности сетей имплантируемых устройств (СИУ). Ее вклад состоит в систематизации известных слабых мест СИУ и характерных для них угроз безопасности, а также анализе достоинств и недостатков существующих методик оценки их защищенности и средств защиты.

В последнее время в медицине стали активно использоваться устройства, наблюдающие за состоянием здоровья человека и собирающие соответствующую информацию без участия персонала. Часть этих устройств устанавливаются непосредственно в тело человека. Такие устройства могут снимать сердечный ритм, ЭКГ, данные об уровне сахара в крови и т. д. Для дальнейшей обработки полученных данных все эти устройства объединяются в одну сеть – СИУ. Обобщенная схема представлена на рис. В состав

сети входит наружная коммуникация (НК) и внутренняя коммуникация (ВК).

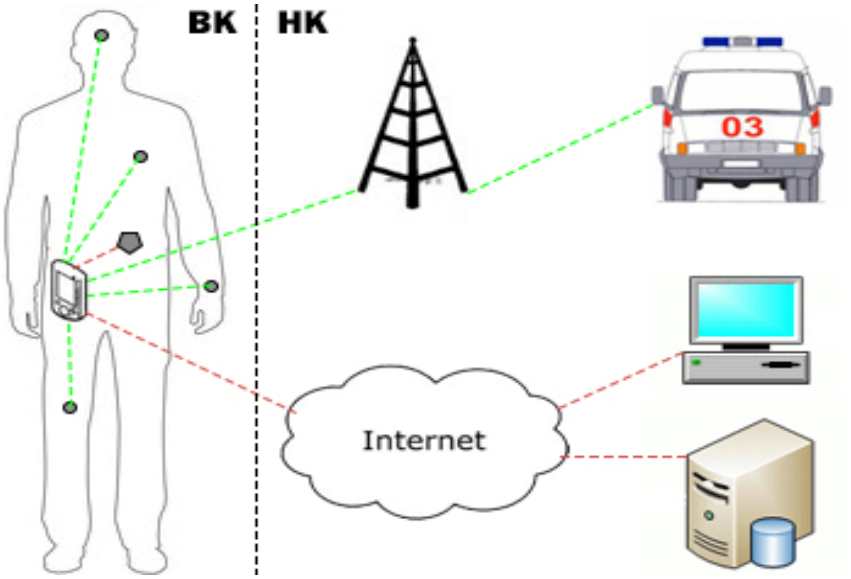


Рисунок. Обобщенная схема СИУ

Под НК понимается обычная компьютерная сеть или мобильная сеть за пределами человеческого тела. Элементами НК являются сервера и телефоны служб экстренной медицинской помощи, сервера медицинских учреждений, в которых наблюдается пациент, а также компьютеры лечащих врачей. Доступ к серверам и компьютерам осуществляется через глобальную сеть Интернет, а к телефонам – посредством мобильной связи.

Под ВК понимается сеть устройств, находящихся в теле человека. ВК отличается небольшой зоной охвата сигнала, подаваемого ИУ.

Сеть ВК объединяется одним головным устройством (ГУ), собирающим и передающим информацию далее в необходимые инстанции (в НК). В качестве ГУ должно выступать устройство, способное принимать радиосигналы с ИУ и передавать их дальше через сеть Интернет, а также иметь возможность совершить экстренный вызов медицинских спецслужб при обнаружении критического состояния здоровья человека. С подобными задачами может справиться почти любой современный смартфон.

ИУ можно разделить на пассивные – те, что собирают информацию и передают ее на ГУ, и активные – те, которые при получении сигнала для активации (например, снимаемые пассивными ИУ характеристики или команда, задаваемая врачом), могут быть использованы, к примеру, для введения инъекции.

Основой ИУ служат микроконтроллеры: 8-битный Atmel-AVR или 16-битный TI MSP430. Эти микроконтроллеры обладают малым энергопотреблением, что является одним из самых важных для ИУ параметров. Общение внутри СИУ также должно быть, как можно менее затратным с точки зрения

энергопотребления. Для общения большая часть существующих ИУ используют протокол IEEE 802.15.4 или протокол ZigBee [3, 4]. Также существует протокол BSN-MAC [5], позволяющий уменьшить затраты энергии и, при этом, обеспечить достаточный для приемника уровень сигнала.

На основе анализа существующих работ и архитектуры СИУ можно выделить их слабые места. Одним из наиболее уязвимых мест в СИУ является канал открытой радиосвязи между ИУ и ГУ. В связи с открытостью канала, существует опасность для конфиденциальности и достоверности данных: злоумышленник имеет возможность перехвата сигнала с ИУ, а также подачи ложного сигнала на ГУ. Помимо этого, злоумышленник может провести DOS-атаку на ГУ (или медицинские сервера), что приведёт к повышенной загруженности или недоступности вышеупомянутых элементов СИУ. Также злоумышленник имеет возможность повлиять на активные ИУ и вызвать их ложное срабатывание, что может нанести вред здоровью или жизни носителя ИУ. Реализовать эти угрозы можно также через различные уязвимости используемого программного обеспечения. Помимо этого, СИУ имеет ряд слабых мест, характерных для обычных компьютерных сетей, касающихся целостности, доступности и конфиденциальности информации [6]. Например, они могут пострадать от перебоев энергоснабжения, ошибок оператора при пользовании БД или различных снифферов.

Подробная информация по слабым местам СИУ и соответствующим угрозам безопасности сведена в таблицу.

ТАБЛИЦА 1. Слабые места СИУ

Проблема	Причина	Описание
Конфиденциальность данных	Открытый радиоканал, уязвимости ПО на серверах с БД	Возможность съема информации путем перехвата сигнала связи между ИУ и ГУ, или получение доступа к БД
Достоверность данных	Открытый радиоканал, уязвимость ПО ГУ	Возможность передачи на ГУ данных, не соответствующих реальным, посредством стороннего источника сигнала
Доступность ГУ	Открытый радиоканал, уязвимость ПО ГУ	Возможность DoS-атаки на ГУ путем передачи большого количества ложных данных, глушение сигнала
Доступность данных на серверах медицинских структур	Отсутствие фильтрации трафика	Возможность выведения из строя БД, что повлечет за собой отсутствие доступа к данным для медицинского персонала
Подмена данных	Открытый радиоканал, уязвимости в ПО медицинских структур	Возможность вызвать ложное срабатывание активных ИУ
Истощение ресурсов	Открытый радиоканал, уязвимость ПО ГУ	Возможность влиять на энергопотребление устройств в системе

Исходя из обозначенных ранее причин возникновения угроз можно сделать вывод о необходимости защиты радиоканала передачи данных между ИУ и ГУ. Криптография является одним из методов защиты открытых каналов связи, но ее использование связано с решением задачи по управлению ключами. Использование заранее заданных ключей или сложных криптографических алгоритмов приведет к низкой эффективности и гибкости применяемого метода. Поскольку задача генерации ключей является вычислительно сложной, это накладывает требования на использование памяти и энергопотребление. Однако, как уже описывалось, для СИУ это ключевые ресурсы, которые необходимо минимизировать. Это и есть основное ограничение. Для решения этой задачи, в СИУ предлагается использовать характеристики передающего радиосигнала [7] или биометрические показатели, для обеспечения целостности, конфиденциальности и достоверности данных [8]. Эти методы предполагают использование параметров, получаемых устройствами в ходе выполнения своей задачи, для генерации ключей. Эти параметры могут обеспечить необходимый уровень безопасности в силу того, что являются объемными, случайными и изменяются со временем.

Остальные слабые места СИУ можно приравнять к слабым местам обычной компьютерной сети, одним из методов защиты которой является усовершенствование используемого программного обеспечения [9].

В статье была рассмотрена проблема защиты СИУ. Выявлены их слабые места. На данном этапе развития СИУ, используемых мер по защите этих сетей недостаточно. Это направление активно развивается и с каждым днем предлагается все больше новых решений. Однако, эффективность этих решений остается под вопросом. В дальнейшей работе планируется определить наиболее эффективные средства обеспечения безопасности СИУ исходя из существующих угроз и влияния контрмер на эти угрозы, используя авторскую разработку [10].

Работа выполнена при поддержке РФФИ (16-29-09482, 18-07-01488), гранта президента РФ (МК-314.2017.9), стипендии президента РФ (СП-751.2018.5), при частичной поддержке бюджетных тем (№ АААА-А16-116033110102-5), и при государственной финансовой поддержке ведущих университетов РФ (субсидия 074-U01).

Список используемых источников

1. mHealth Wearables Boost Patient Healthcare Both Inside and Outside the Hospital [Электронный ресурс]. Режим доступа: https://www.abiresearch.com/press/mhealth-wearables-boost-patient-healthcare-both-in

2. Национальная технологическая инициатива. HealthNet [Электронный ресурс]. Режим доступа: http://www.nti2035.ru/markets/healthnet

3. IEEE 802.15.4-2003: IEEE Standard for Information Technology–Part 15.4: Wireless medium access control and physical layer specifications for low rate wireless personal area networks. NY: IEEE, Inc., 2003 679 c.

4. Официальный сайт ZigBee Alliance. Режим доступа: http://www.zigbee.org.

5. Li H. & Tan J. An ultra-low-power medium access control protocol for body sensor network // 27th Annual international conference of the engineering in medicine and biology society, 2005. IEEE-EMBS, Shanghai, 2005. C. 2451–2454.

6. Мусина В. Ф. Байесовские сети доверия как вероятностная графическая модель для оценки медицинских рисков // Труды СПИИРАН. 2013. Вып. 24. С. 135–151.

7. Singele´e D. Latre´ B., Braem B., De Soete M., De Cleyn P., Preneel B. et al. A secure cross-layer protocol for multi hop wireless body area networks // 7th International conference on ad-hoc networks & wireless (ADHOCNOW 2008), Vol. LNCS 5198, France, Sep 11–13, 2008. PP. 94–107.

8. Poon C. C. Y., Zhang Y.-T., Bao S.-D. A novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health // IEEE Communications Magazine, 2006. PP. 73–81.

9. Дойникова Е. В. Показатели и методики оценки защищенности компьютерных сетей на основе графов атак и графов зависимостей сервисов // Труды СПИИРАН. Вып. 3 (26). СПб. : Наука, 2013. С. 54–68.

10. Чумак Е. А. Разработка подсистемы оценки эффективности средств защиты информации для автоматизированной системы стохастического риск-анализа : дис. бакалавра. ИТМО, 2017. 71 с.

УДК 654.739

ИССЛЕДОВАНИЕ ИНТЕЛЛЕКТУАЛЬНЫХ СИСТЕМ ХРАНЕНИЯ ДАННЫХ

В. О. Долгун, В. Л. Литвинов

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

В статье рассмотрены современные системы архивации данных в АСУТП. Описан принцип построения многоуровневых и распределенных систем сбора и архивации данных, а также агрегации и горячего резервирования. Приведены требования, предъявляемые к интеллектуальным системам хранения данных. Подчеркнута востребованность и необходимость изучения данного направления.

система хранения данных, автоматизированная система управления, интеллектуальная система.

На сегодняшний день, для повышения конкурентоспособности компании на рынке, во всех отраслях промышленности необходимо уметь произ-

водить системы диспетчерского управления, сбора данных, систем хранения данных и проектировать их таким образом, чтобы программное обеспечение, которое в них применяется позволяло бы осуществлять визуализацию всей системы в целом в режиме реального времени. Существующие технологии позволяют операторам редактировать настройки технологических процессов с целью достижения наилучшего состояния независимо от применяемого программного продукта в системе. Не стоит забывать про оптимизацию производственных процессов в режиме реального времени, которая невозможна без анализа событий и статистики за предыдущие дни, которые показывали бы хорошие и плохие события в системе. Оперативно предоставленные данные об изменении одной или нескольких переменных смогут своевременно помочь в решении проблем еще на начальном этапе.

Для осуществления анализа данных требуется несколько циклов, чтобы можно было увидеть закономерность происходящих тех или иных событий и судить об оптимальности тех или иных параметров.

Производя анализ систем хранения данных в автоматизированных системах управления, необходимо производить анализ всех процессов и иметь полное понимание о состоянии системы и работе всех исполнительных процессов в момент производства.

При выборе систем хранения данных необходимо принимать во внимание следующие факторы [1]:

– максимальный возможный объем хранимой информации;

– максимальное число пользователей, одновременно обращающихся к базе;

– аппаратные компоненты сервера;

– серверная операционная система;

– уровень квалификации персонала обслуживающий систему хранения данных.

Система хранения данных (СХД) представляет собой совокупность программного обеспечения и специализированного оборудования, предназначенного для хранения и передачи информации больших объемов. Особенностью каждой СХД является оптимальное распределение ресурсов при хранении информации на дисковых площадках. Необходимость в СХД появляется тогда, когда массивы хранимой и передаваемой информации из года в год вырастают на определенный процент от ее первоначального объема.

Применение СХД в настоящее время происходит повсеместно: от простой системы видеонаблюдения до создания резервных копий файлового хранилища организации. СХД должна быть масштабируемой, то есть гибкой, отказоустойчивой и, в определенных случаях, катастрофоустойчивой (рис. 1).

Рис. 1. Требования к СХД

Современные серверные платформы для центров обработки данных становятся также все более экономичными и энергоэффективными. Благодаря последнему поколению процессоров они стали привлекательнее как для традиционного использования, так и для виртуальных и облачных сред.

Серверные решения удовлетворяют потребность рынка в высокомасштабируемых энергосберегающих системах для разного типа нагрузок. Среди тенденций можно выделить рост числа ядер, повышение производительности и энергоэффективности процессоров, а также усовершенствованную поддержку виртуализации.

Все больше компаний используют серверы архитектуры x86 для решения критически важных для бизнеса задач. Подходы к построению центров обработки данных постоянно меняются, и это влечет за собой потребность в широком спектре серверных решений.

Например, компания Dell EMC выпустила 14-е поколение серверов Dell EMC PowerEdge. Они были анонсированы на конференции Dell EMC World 2017 в Лас-Вегасе и представлены на осеннем форуме Dell EMC Forum 2017 в Москве [2].

Новинки построены на базе процессоров Intel Xeon Scalable, оптимизированы под NVMe и предназначены для:

- традиционных и облачных приложений,
- программно-определяемых хранилищ данных,
- конвергентных и гиперконвергентных инфраструктур.

NVM Express (или NVMe) представляет собой стандартизированный высокопроизводительный программный интерфейс для твердотельных дисков (SSD), подключенных по шине PCI Express, которые используют энер-

гонезависимую память (NVM). NVMe предоставляет эффективный и масштабируемый набор простых протоколов и команд, обеспечивая высокую пропускную способность и низкую задержку.

Эти системы оптимизированы для самых разных нагрузок, снабжены автоматизированными средствами управления и встроенными функциями обеспечения безопасности.

Новое поколение серверов Dell EMC PowerEdge – это очередной рост вычислительных мощностей, большая емкость, низкое энергопотребление, высокая плотность памяти для модульных решений, масштабируемая подсистема хранения данных с широким выбором дисков и накопителей, в том числе All-flash и NVMe во всех форм-факторах.

У серверов нового поколения выросла энергоэффективность: благодаря технологии Dell Fresh Air оборудование можно эксплуатировать при температурах до 40°C, а это существенно уменьшает расход электричества. На рис. 2 показано превосходство СХД нового поколения над серверами PowerEdge предыдущего поколения.

Высокоплотные конфигурации с флеш-памятью позволяют перемещать данные как можно ближе к процессорам, повышая производительность серверов, особенно для транзакционных нагрузок. Возможность комбинировать емкие диски и SSD-накопители в одной серверной платформе, а также поддержка кеширования значительно уменьшают время доступа к данным. Сверхпроизводительные SSD-накопители NVMe с прямым подключением к шине PCIe ускоряют работу приложений. Расширена и поддержка графических ускорителей.

Высокая производительность	Показатель IOPS увеличился в 12 раз, на 98% сократилось время ожидания выполнения запросов в кластере VMware vSAN.
Ускоренная миграция виртуальных машин	При использовании сети 25GbE с дистанционным прямым доступом к памяти (Remote Direct Memory Access, RDMA) миграция стала на 58% быстрее и при этом требует на 75% меньше ресурсов ЦП.
Высокая скорость и емкость подсистемы хранения данных	Использование накопителей NVMe повышает производительность приложений. Общая емкость флеш-памяти увеличилась в пять раз, плотность выросла на 25%, а количество слотов ввода-вывода — на 30%.
Процессоры Intel Xeon Scalable	Число ядер процессоров выросло на 27%, пропускная способность памяти — на 50%, что способствует ускорению работы критически важных приложений.

Рис. 2. Преимущества новых СХД Dell EMC

Простые и мощные средства администрирования (набор инструментов *Dell OpenManage*) позволяют быстрее внедрять новые сервисы и управлять оборудованием из любого места.

Новая консоль управления OpenManage Enterprise с API RESTful предлагает инструменты для автоматизации развертывания, обновлений, мониторинга и обслуживания серверов.

Подводя итоги нужно отметить, что системы хранения данных все больше и больше переходят в облачные хранилища. В настоящий момент большинство пользователей тратят большую часть бюджета на построение и дальнейшую поддержку работоспособности систем хранения данных.

На больших предприятиях все больше требуется общий доступ к архивным копиям данных. Отсюда появляется вопрос о необходимости создания облачных ресурсов для организации вычислений, хранения и обмена информации. В таких системах требуется оплачивать только используемые на текущий момент ресурсы. При этом стоит отметить и недостатки данных систем. Так, например, остро встает вопрос безопасности передачи данных, задержки при передачи данных. Тем не менее, в ближайшее время популярность облачных систем хранения данных и виртуализации приложений будет расти.

Список используемых источников

1. Кудрявцев В., Гасанов Э. Интеллектуальные системы. Теория хранения и поиска информации // Юрайт. 2017. С. 45–91.

2. Moscow DELL EMC FORUM 2017. URL: https://www.dellemc.com/ru-ru/events/dellemc-forum/post-event.htm (дата обращения 27.03.2018).

УДК 004.735

РАЗРАБОТКА МОДЕЛЕЙ И МЕТОДОВ ТЕСТИРОВАНИЯ УСТРОЙСТВ И ПРИЛОЖЕНИЙ ИНТЕРНЕТА ВЕЩЕЙ НА БАЗЕ МОДЕЛЬНОЙ СЕТИ

Р. А. Долгушев, Р. В. Киричек

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

Статья посвящена обзору основных этапов тестирования устройств и приложений Интернета Вещей на базе модельной сети. В качестве исследования приводится анализ существующих подходов к тестированию, которые применяются в сетях связи в настоящее время. Описываются платформы, позволяющие автоматизировать процесс тестирования в зависимости от используемой системы/архитектуры.

Интернет Вещей, ИВ, IoT, тестирование, модельная сеть.

Быстрое развитие и разнообразие различных IoT-продуктов, представленных на рынке, привело к ряду проблем, которые затрагивают как вопросы взаимодействия Интернет Вещей между собой, так и вопросы безопасности. Возможные уязвимости в IoT-продуктах позволяют злоумышленникам получить доступ не только к личным данным пользователя, но и организовать наблюдение за ним. Также стоит отметить тот факт, что не всегда при разработке тех или иных приложений/устройств Интернета Вещей рационально используется выбранная архитектура и технологии. Поэтому, на данный момент вопрос тестирования и сертификации устройств и приложений Интернета Вещей является наиболее обсуждаемым, чтобы в дальнейшем избежать этих проблем. Классический подход к тестированию не вписывается в модель IoT. Нужно выработать новые стратегии, которые помогут добиться стабильной работы всех компонентов Интернета Вещей.

Стоит отметить, что в дальнейшем Интернет Вещей будет генерировать большие объемы данных (*Big Data*), которые к тому же, обладают другими характеристиками, нежели таковые в традиционной модели связи (аудио, видео, данные), что заставляет серьезно задуматься о модернизации уже существующих телекоммуникационных систем, систем обработки и хранения. Важно то, что на передачу данных от IoT-устройств до конечного сервера (рис. 1) влияет не только качество соединения, но также и такие параметры, как автономность Вещей, особые протоколы маршрутизации и методы сжатия информации. Наличие этих особенностей влечет за собой новые промежуточные этапы для обработки данных.

Рис. 1. Принцип коммуникации в Интернете Вещей

С ростом числа устройств Интернета Вещей и программных проектов потребность в тестировщиках и особых подходах к тестированию также возрастет. Специалисты в этой области столкнутся со множеством различных

проблем и возможных ошибок. Им придется сосредоточиться на проверках эргономичности устройств, моделируя среду (рис. 2), в которой они будут использоваться, для того, чтобы убедиться, что обмен информацией между ними происходит должным образом, и достигаются необходимые показатели качества обслуживания [1].

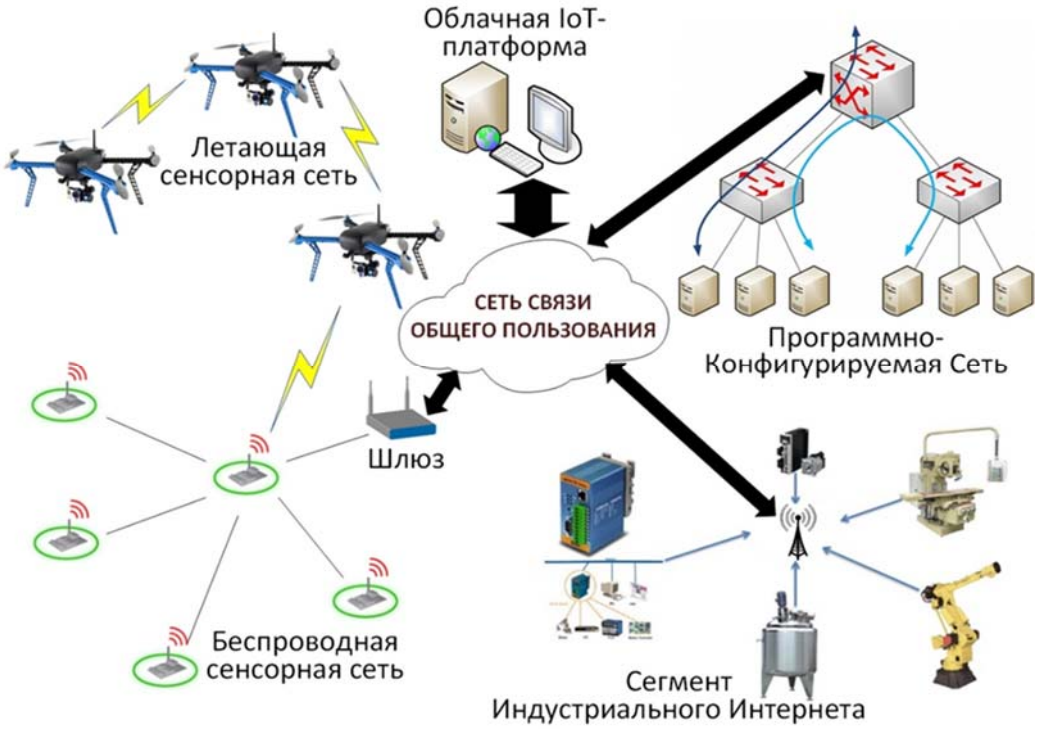


Рис. 2. Структура модельной сети

Чтобы получить как можно более информативные результаты по тестированию, необходимо мыслить не по шаблону, а искать нестандартные сценарии использования приложений и объектов IoT.

При разработке IoT-системы, процесс тестирования включает в себя тестирование используемого оборудования, программного обеспечения, анализ интерфейсов для взаимодействия с потоками данных в режиме реального времени [2]. Тестирование необходимо начинать с описания архитектуры, конкретных задач, которые стоят перед той или иной Интернет Вещью, методов их решения, и продолжать этот процесс в ходе эксплуатации системы. Это важно, как для оценки возможных рисков при введении новых компонентов и сервисов, так и для оптимизации работы уже функционирующей системы.

Модель тестирования IoT-системы, которая позволит обеспечить должное качество разрабатываемого продукта, его безопасность и сократит время разработки до выхода готового приложения или устройства, состоит из нескольких этапов:

– этап моделирования;
– этап сборки;
– этап развертывания;
– этап нагрузочного тестирования.

На этапе моделирования наибольшее внимание уделяется функциональному тестированию, а именно, модульным и интеграционным тестам.

На этапе сборки акцент делается на создании простейших компонентов, из комбинации которых в дальнейшем можно определить конечный продукт и его основные цели применения.

Этап развертывания, как правило, подразумевает собой ввод в эксплуатацию ряда сервисов для того, чтобы оценить их успешность. Для этого нужно тестировать разрабатываемый продукт на наличие несоответствий, противоречий и дублирования. Также необходимо убедиться в том, что развернутые сервисы смогут предоставлять услуги с заявленным качеством обслуживания.

И, наконец, этап нагрузочного тестирования. Он заключается в проведении стрессового тестирования. Крайне важно оценить поведение системы в случае возможных перегрузок, а также определить максимальную емкость отдельных компонентов IoT-системы.

В представленной модели тестирования устройств и приложений Интернета Вещей главную роль играет уровень автоматизации тестирования. Прежде всего, это связано с необходимостью проведения большого объема работ, и с воспроизведением реальных ситуаций, которые могут быть связаны с риском для используемого оборудования. Для того, чтобы имитировать такие ситуации, используются виртуальные эмуляторы, которые будут описаны в дальнейшем. Еще один немаловажный момент – это выбор средств мониторинга за элементами инфраструктуры Интернета Вещей. Перед тем, как выбрать такой инструмент, нужно проанализировать, насколько сильно влияет работа самих систем мониторинга на работу контроллеров.

Средства тестирования

Как было сказано ранее, автоматизация тестирования крайне важна в сфере Интернета Вещей. Такие подходы, как UML 2.0 Testing Profile (U2TP), предоставляют возможность для проектирования и разработки тестов методом черного ящика, но не поясняют, как именно использовать данный профиль. Абстрактный U2TP предлагает только план действий, который в дальнейшем должен быть реализован на соответствующем языке программирования [3].

Для тестирования сервисов в этом случае используются Testing and Test Control Notation version 3 (TTCN-3) или JUnit (библиотека для модульного тестирования программного обеспечения на языке *Java*). TTCN-3 является

строго типизированным скриптовым языком, используемым в тестировании коммуникационных систем, а также спецификацией интерфейсов тестовой инфраструктуры, позволяющих связать абстрактные тестовые скрипты с конкретным коммуникационным оборудованием. Взаимодействие же непосредственно с контроллерами осуществляется средствами языков программирования C/C++ и Python.

Рассмотренные инструменты тестирования достаточно сложны, и поэтому не каждый инженер тестирования обладает необходимыми навыками для их использования. Однако, существуют более простые, но не менее функциональные, средства тестирования.

Одним из таких средств является платформа EuWIn Platform [4]. Она предоставляет возможность работы с различными реализациями физического уровня модели OSI.

Для моделирования и тестирования физического расположения IoT-устройств может быть использован эмулятор EEBuildingSim (рис. 3). Он позволяет эмулировать работу устройств в зависимости от того, как они расположены на местности.

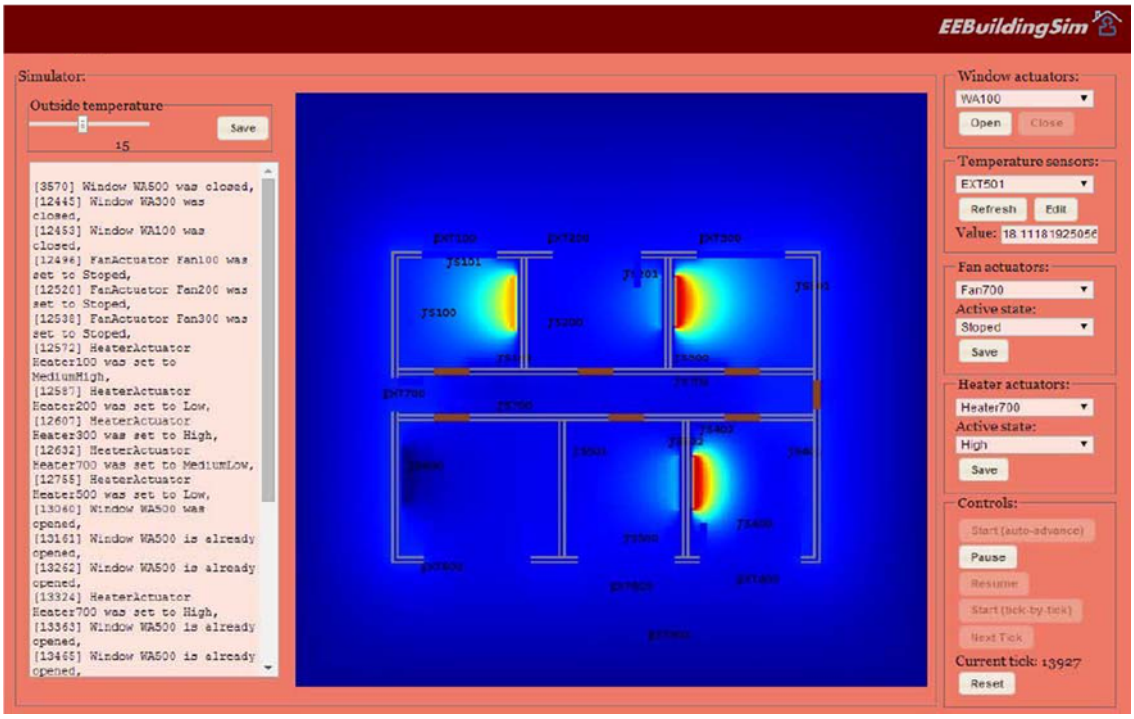


Рис. 3. Эмулятор EEBuildingSim

При тестировании самих IoT-сервисов могут быть использованы решения, позволяющие создавать различные тесты в графическом виде. Одним из таких решений является платформа Service Composition Environments (SCE) [5]. Данная платформа предоставляет графический интерфейс редактирования бизнес процессов и связанных с ними услуг.

Выводы

В итоге Интернет Вещей и рост популярности «умных» устройств несомненно потребует развития различных методов тестирования. Грамотное планирование и проектирование при разработке различных IoT-продуктов будет по-прежнему иметь решающее значение, а тестирование будет неотъемлемой частью данного процесса. При этом подход к тестированию IoT может отличаться в зависимости от конкретной системы/архитектуры. Тестировать сферу IoT сложно, но вместе с тем она открывает перед тестировщиками ряд интересных и нестандартных задач, ведь существует большое количество различных устройств, протоколов и операционных систем.

Список используемых источников

1. Интернет Вещей – это глобальный тренд в мире телекома, который будет трудно затмить в ближайшие 10–15 лет [Электронный ресурс] / Режим доступа: https://clck.ru/CJwfm.
2. Сложности тестирования IoT-устройств [Электронный ресурс] / Режим доступа: https://goo.gl/yMFyT9.
3. Пирмагомедов Р. Я., Худоев И. В. Особенности тестирования приложений Интернета Вещей // 2-я международная научно-техническая конференция студентов, аспирантов и молодых ученых «Интернет Вещей и 5G (INTHITEN 2016)». С. 31–37.
4. Internet of Things Environment for Service Creation and Testing [Электронный ресурс] / Режим доступа: htpps://goo.gl/61d8fX.
5. Test-Enabled Architecture for IoT Service Creation [Электронный ресурс] / Режим доступа: https://goo.gl/NSspS5.

УДК 004.492.2

АНАЛИЗ ЗАЩИЩЕННОСТИ ВИРТУАЛЬНЫХ ИНФРАСТРУКТУР С ИСПОЛЬЗОВАНИЕМ ПО VGATE

Е. А. Донсков, И. А. Ушаков

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

В статье сравниваются предложения от российских производителей по вопросу защиты виртуальных инфраструктур. Также более подробно рассматривается решение от компании «Код Безопасности» по обеспечению защищенности виртуальных машин – ПО vGate. В рамках статьи была поставлена задача рассмотреть ПО vGate с функциональной и практической точек зрения, развернув виртуальную инфраструктуру и установив на нее данное ПО. Также в работе представлены результаты тестирования основного заявленного функционала ПО vGate.

виртуализация, защита виртуальных машин, vGate.

Технология виртуализации позволяет более эффективно и рационально использовать вычислительные ресурсы. При этом сохраняется привычная функциональность устройств и появляются преимущества по сравнению с традиционной физической средой.

Современные технологии виртуализации в своем составе содержат компоненты защиты, но они неспособны нейтрализовать весь спектр современных угроз, в частности, несанкционированный доступ к информации при ее передаче по недоверенным каналам связи, а также не могут полностью выполнить требования законодательства в области обеспечения информационной безопасности.

Решить задачу защиты виртуальной инфраструктуры компании и безопасного доступа к ней можно, используя традиционные программно-аппаратные комплексы (ПАК). Это проверенное временем аппаратное решение, подходящее для защиты физических компонентов, применимо и к обеспечению безопасности виртуальных систем.

Альтернативой являются специальные средства защиты, предназначенные для работы в виртуальной среде. Такой способ позволяет в полной мере использовать основные преимущества технологии виртуализации: экономичность, масштабируемость, отказоустойчивость. Средства защиты, выполненные в виде виртуальных программных комплексов, имеют аналогичную функциональность, не уступающую традиционным программно-аппаратным решениям, при этом повышая удобство пользования сетевыми сервисами и упрощая администрирование средств защиты информации [1].

Предложений сертифицированных продуктов на рынке большое множество, поэтому необходимо разобраться в функциональных возможностях основных лидеров.

Проведя исследование в области виртуальных инфраструктур, были выявлены основные рыночные предложения по их защите. Актуальными версиями таковых являются:

– СЗИ vGate R2 (vGate 4.0) [2];
– СЗИ ВИ Dallas Lock [3];
– ПАК Аккорд-В (Версия 1.3) [4];
– С-Терра Виртуальный Шлюз (Версия 4.1) [5].

Для объективной оценки данных решений были отобраны критерии в соответствии с основными угрозами для виртуальных инфраструктур.

Главным критерием для российского рынка является уровень сертификации ФСТЭК предлагаемого продукта. (Ввиду наличия закона Российской Федерации № 5485-I «О государственной тайне».)

Для защиты информации, значимость которой определяется градацией «секретность/конфиденциальность», установлены следующие классы защищенности:

– четвертый класс защищенности (1Г) – является достаточным для защиты конфиденциальной информации;

– третий класс защищенности (1В) – используется для защиты информации с грифом «Секретно»;

– второй класс (1Б) – с грифом «Совершенно секретно»;

– первый класс (1А) – используется для защиты информации с грифом «Особой важности».

Результаты анализа показали, что ни один из продуктов не обладает первым классом защищенности – «Особой важности», однако есть 2 продукта с вторым классом (табл. 1).

ТАБЛИЦА 1. Классы защищенности

vGate R2	Dallas Lock	Аккорд-В	С-Терра ВШ
До 1Б	До 1Г	До 1Б	До 1В

Следующим критерием необходимым к рассмотрению является поддержка различных платформ виртуализации. Данный критерий является одним из важнейших, так как показывает величину покрытия продуктом рыночного спроса.

Результаты анализа показали, что ни один из продуктов не удовлетворяет спросу в полном объеме (табл. 2).

ТАБЛИЦА 2. Поддержка платформ виртуализации

Платформы	vGate R2	Dallas Lock	Аккорд-В	С-Терра ВШ
VMware vSphere	5.5/6.0/6.5	5.5	5/5.1/5.5/6.0	5.0/5.1/5.5/6.0
Microsoft Hyper-V	2012/ 2012 (R2)/ 2016	–	–	–
KVM	–	–	–	1.1.2

Оставшиеся критерии нет необходимости рассматривать более подробно, поэтому они все сведены в общую таблицу (табл. 3).

Безусловного лидера выявить не удалось, однако, основываясь на результатах сравнительного анализа, наиболее выигрышным вариантом на российском рынке для большинства платформ виртуализации будет являться СЗИ vGate R2.

ТАБЛИЦА 3. Общее сравнение продуктов по важным критериям

Критерии	vGate R2	Dallas Lock	Аккорд-В	С-Терра ВШ
Централизованное управление	+	+	+	+
Аутентификация администраторов и пользователей	+	+	+	Только администраторы
Контроль целостности виртуальной инфраструктуры/ трафика	+/+	+/–	+/+	–/+
Отказоустойчивость	+	–	–	+
Поддержка сетевых хранилищ	+	–	–	–
Разграничение доступа к VM	+	–	–	+
Поддержка кластеризации VM	+	–	–	–
Поддержка доверенной загрузки	+	+	+	–
Интеграция с Active Directory	+	+	+	+
Регистрация событий использования серверов (аудит)	+	+	+	–

СЗИ vGate R2 – это программное обеспечение, которое ставится на серверную версию операционной системы Windows. Такой сервер становится сервером авторизации и является центром управления виртуальной инфраструктуры.

Он изолирует определенный участок сети от внешней незащищенной, делая его защищенным. Теперь, посредством пропускания через себя всего трафика, появляется возможность отбрасывать весь несанкционированный.

Санкционированность трафика помогает определять Authentication Header (идентификационный заголовок), один из заголовков IPsec-протокола, делая трафик подписанным, а также политики доступа на сервере авторизации (рис. 1).

Если же рассматривать СЗИ vGate R2 с более подробной точки зрения, необходимо знать насколько сложен процесс внедрения в готовую виртуальную инфраструктуру. Поэтому было принято решение о развертывании тестового стенда на платформе гипервизора компании Microsoft – Hyper-V, с последующей установкой на него ПО vGate 4.0.

В качестве основы для тестового стенда были установлены:

– Microsoft Windows Server 2016 с ролью Hyper-V;
– Microsoft Windows Server 2012 R2 с ролью Hyper-V;

– Microsoft Windows Server 2012 R2;
– Microsoft Windows 10.

Рис. 1. Архитектура сети и размещение компонентов

После установки vGate 4.0 тестовый стенд стал удовлетворять требованиям, приведенным в документации (рис. 2) [2].

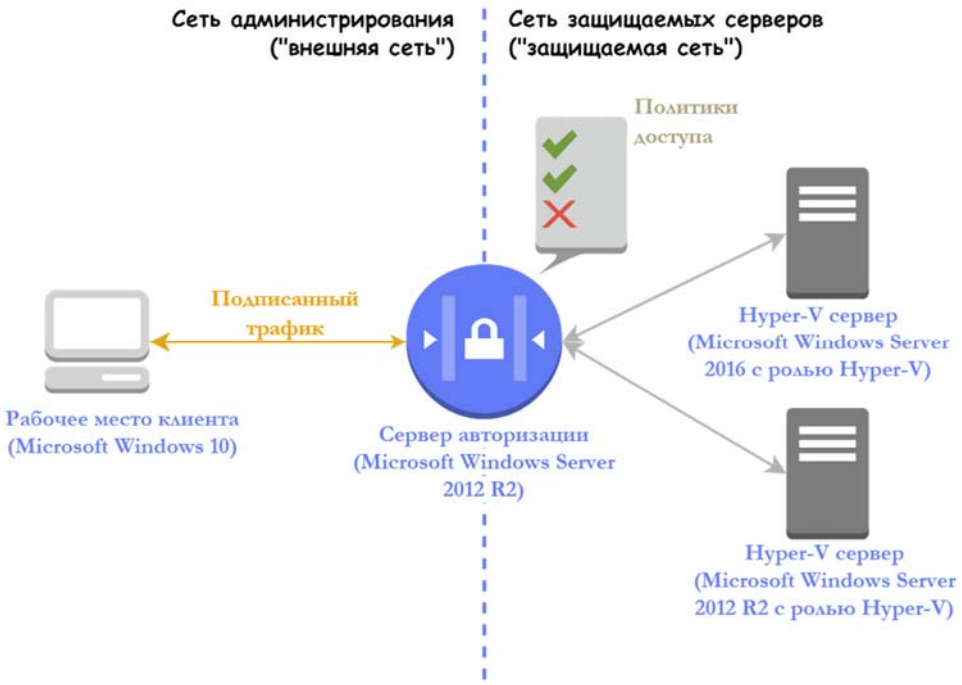


Рис. 2. Архитектура сети и размещение компонентов после инсталляции vGate 4.0

Были рассмотрены три основных тестовых сценария:

1. Подключение не аутентифицированным в СЗИ клиентом к виртуальной машине, находящейся на Hyper-V сервере. (Ожидаемый результат – Ошибка подключения).

2. Подключение аутентифицированным в СЗИ клиентом к виртуальной машине, находящейся на Hyper-V сервере, с не настроенными/запрещающими доступ политиками безопасности. (Ожидаемый результат – Ошибка подключения).

3. Подключение аутентифицированным в СЗИ клиентом к виртуальной машине, находящейся на Hyper-V сервере, с разрешающими доступ политиками безопасности. (Ожидаемый результат – Успешное подключение).

По итогам выполнения тестовых сценариев ожидаемые результаты полностью подтвердились фактическими (рис. 3–5).

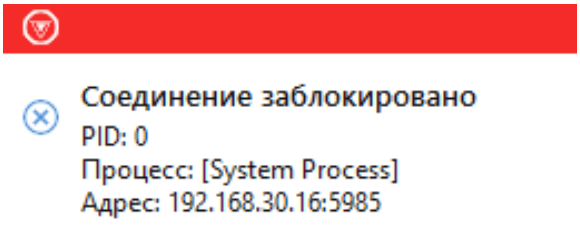


Рис. 3. Результат 1-го сценария

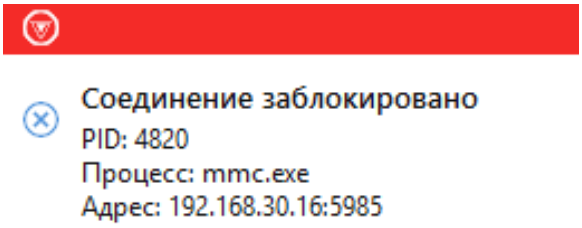


Рис. 4. Результат 2-го сценария

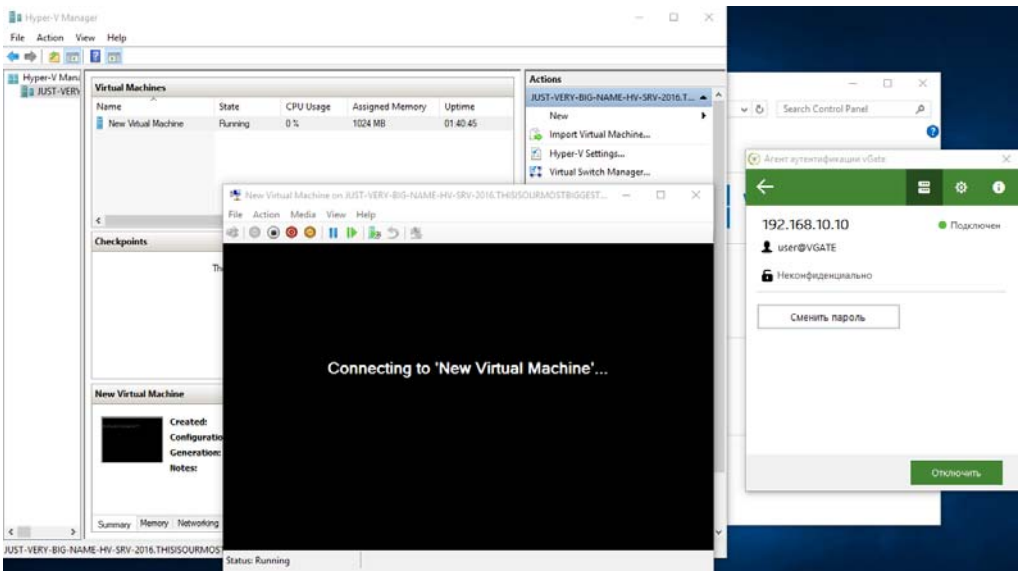


Рис. 5. Результат 3-го сценария

В результате работы с ПО vGate 4.0 никаких серьезных проблем не возникало. Однако для создания требуемой конфигурации сети при установке и работе продукта требовалось наличие основной теоретической базы знаний по сетям передачи данных.

Список используемых источников

1. Котенко И. В., Ушаков И. А. Технологии больших данных для мониторинга компьютерной безопасности // Защита информации. Инсайд. 2017. № 3 (75). С. 23–33.
2. Документация СЗИ vGate R2 (vGate 4.0). URL:https://www.securitycode.ru/products/vgate/documentation/ (дата обращения: 27.02.2018).
3. Документация СЗИ ВИ Dallas Lock. URL:https://dallaslock.ru/products/szvi/ (дата обращения: 27.02.2018).
4. Документация ПАК Аккорд-В (Версия 1.3). URL:http://www.accord.ru/accord-v.html (дата обращения: 27.02.2018).
5. Документация С-Терра Виртуальный Шлюз (Версия 4.1). URL:https://www.s-terra.ru/resheniya/industry_solutions/zashchita-virtualnoy-infrastruktury/ (дата обращения: 27.02.2018).

Статья представлена научным руководителем, кандидатом технических наук, доцентом А. В. Красовым.

УДК 004.056.53

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ И ЧЕЛОВЕЧЕСКИЙ ФАКТОР В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Д. М. Донской, А. С. Карев, Д. В. Сахаров

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

Информация может составлять коммерческую тайну компании, т.е. при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке. Социальная инженерия – это комплекс мер и методов получения несанкционированного доступа к информации. Комплекс основан на использовании слабостей человеческого фактора и является очень эффективным. В своей работе авторы исследуют существующие методы социальной инженерии, а также влияние человеческого фактора на вопросы информационной безопасности.

социальная инженерия, человеческий фактор, нарушитель, информационная безопасность.

Введение

Информация – это один из важнейших ресурсов любой компании. Зачастую, довольно большой объем информации, который находится во владении организации, представляет собой коммерческую тайну, т. е. данный ресурс при определенных обстоятельствах позволяет увеличить доходы, из-

бавиться от неоправданных растрат, утвердить свое положение на рынке товаров и услуг, а также обеспечить другое коммерческое преимущество компании. Следовательно, такую информацию целесообразно защищать.

Так как в любой организации работают люди, то на многие процессы, протекающие в данной компании, неизбежно сказывается влияние человеческого фактора. В том числе и на процесс защиты конфиденциальной информации.

Человеческий фактор – это устойчивое выражение, обозначающее психическую составляющую человека как предполагаемый и актуальный источник проблем при использовании им современных технологий [1].

Действия сотрудника организации, связанные с нарушением режима безопасности, разделяют на две категории: умышленные и неумышленные действия.

Умышленные действия подразумевают под собой: кражу корпоративной информации, ее модификация, либо ее уничтожение (диверсия).

К неумышленным действиям можно отнести утрату носителя информации, искажение данных либо полное уничтожение информации по неосторожности.

Также, к неумышленным действиям относится оказание «услуги» сторонним лицам, к примеру, в том случае, когда человек не осознаёт, что его действия направлены на нарушение целостности и безопасности коммерческой тайны, но при этом лицо, которое просило об оказании «услуги», отчетливо понимает к чему приведут подобные действия. Это явный пример социальной инженерии.

Анализ

Социальная инженерия — это метод получения несанкционированного доступа к информации или месту хранения информации без использования технических средств. Метод основан на использовании уязвимостей человеческой психологии и является крайне эффективным в настоящее время. Злоумышленник может добыть нужную информацию, к примеру, путем сбора данных о работниках объекта атаки, используя обычный телефонный звонок либо непосредственное проникновение в организацию под видом сотрудника [2].

Социальный инженер может совершить звонок сотруднику организации (под видом службы технической поддержки) и узнать пароль, сославшись на необходимость решения проблемы в компьютерной системе. Самое сильное влияние в этом случае оказывают приятный голос и актёрские способности злоумышленника. Узнать имена сотрудников удается после нескольких звонков и изучения имён руководителей на сайте организации,

также существует большинство других источников открытой информации (отчёты, реклама и т. п.). Используя реальные имена в диалоге со службой технической поддержки, злоумышленник выдает за правду выдуманную историю, к примеру, что он не может попасть на важное совещание на сайте и ему срочно необходимо учетная запись удаленного доступа.

Также в качестве методов достижения цели являются исследование мусорных контейнеров компании, виртуальных мусорных корзин, кража портативного компьютера и прочих носителей информации. Эти методы используется, в том случае, когда злоумышленник выбрал в качестве жертвы конкретную организацию.

1. Обобщенная модель социальной инженерии

Подразумевается, что каждый работник имеет определенный уровень компетентности в вопросах безопасности и свой уровень доступа к корпоративной системе. Линейные сотрудники не обладают правами доступа к критичной информации, то есть даже кража их аккаунтов и получение всей известной им информации не нанесёт организации серьёзного ущерба. Но тем не менее, их данные могут использоваться для перехода на следующую ступень уже внутри защищаемой зоны.

Смоделируем ситуацию, когда злоумышленник звонит в организацию пару раз в неделю на протяжении месяца. Он представляется сотрудником, общается, расспрашивает о каких-то мало значимых вещах, иногда просит оказать небольшую помощь. Авторизацию заменяет тот факт, что человек звонит часто. До тех пор, пока не становится одним из «своих». Он свой, так как он в курсе разных особенностей работы компании и звонит регулярно. Далее, в определенный момент атакующий просит оказать небольшую услугу, но на этот раз касающуюся важных данных. И если надо, приводит логичное и правдоподобное объяснение, почему это требуется. Вероятность того, что ему помогут в таком случае крайне высока.

Проблема заключается в том, что таким атакам подвержены не только некомпетентные сотрудники. К. Д. Митник в книге «Искусство обмана» описывал случай, когда нарушитель представился ведущим разработчиком проекта и заставил системного администратора дать привилегированный доступ к системе. Социальный инженер принудил профессионала, который прекрасно понимал, что именно он делает [3].

2. Основные методы социальной инженерии

2.1. Несуществующие ссылки

Данный вид атаки заключается в отправке письма с важной причиной перейти на определенный сайт и прямой ссылкой на него, которая имеет лишь визуальное сходство с ожидаемым сайтом, например,

www.PayPai.com. Выглядит это, как ссылка на PayPal, мало кто заметит, что буква «*l*» заменена на «*i*». Таким образом, при переходе по ссылке жертва попадает на сайт, максимально похожий на оригинальный, вводит там данные своей кредитной карты, после чего, эта информация сразу попадает в руки к злоумышленнику.

Одним из самых известных примеров массовой фишинговой рассылки может служить афера 2003 г., во время которой более 1000 пользователей eBay получили электронные письма, в которых их уведомляли о том, что их учетная запись была заблокирована, и для её разблокировки необходимо обновить данные о кредитных картах. Во всех этих письмах была ссылка на фишинговую web-страницу, в точности напоминающую официальную [4].

2.2. Мошенничество с использованием брендов известных корпораций

В фишинговых схемах такого рода используются поддельные сообщения с электронной почты или web-сайты, содержащие названия либо упоминание крупных или известных компаний. Также фишинговое сообщение может содержать поздравление с победой в каком-либо конкурсе, проводимом известной компанией, либо упоминание о том, что получателя взломали в связи с чем, срочно требуется изменить учетные данные или пароль, перейдя по прикрепленной к сообщению ссылке. Подобные мошеннические схемы от лица службы технической поддержки могут осуществляться и по телефону.

2.3. Ложные письма с предложениями чего-либо бесплатного/интересного

Жертва может получить электронное сообщение с крайне выгодным либо инересным для нее предложением, например:

2.3.1 Поддельные антивирусы, более известные как «scareware» (программное обеспечение, которое выглядит как антивирус, хотя, на самом деле, является непосредственно самим вирусом.)

Подобный программный продукт генерирует ложные оповещения о различных угрозах, а также зачастую вынуждает пользователя осуществлять денежные транзакции в пользу злоумышленника. Столкнуться с подобного рода программами пользователь может через электронную почту, онлайн объявления и так далее.

2.3.2 Пользователь может получить электронное сообщение, в котором сообщается, что он выиграл в лотерею, которая проводилась известной организацией. По внешнему виду данные сообщения могут напоминать официальные письма, направленные от лица одного из высокопоставленных работников корпорации.

2.4 IVR или телефонный фишинг

Телефонный фишинг — это один из методов мошенничества социальной инженерии, который заключается в том, что злоумышленники, используя телефонную связь и примеряя на себя определенную роль (сотрудник банка, покупатель, продавец и т.д.), выманивают у держателя банковской карты конфиденциальную информацию либо мотивируют жертву к совершению определенных действий со своим банковским счетом/платежной картой.

IVR (англ. *Interactive Voice Response*) — система заранее записанных голосовых сообщений, которая создана для маршрутизации звонков внутри организации опираясь на вводимую клиентом на клавиатуре телефона последовательность чисел, используя режим тонального набора.

IVR фишинг – это техника, которая основана на использовании системы заранее записанных голосовых сообщений, с целью воссоздать «официальные звонки» от банковских работников либо от других официальных структур и учреждений.

Чаще всего, объекту атаки на электронную почту поступает письмо о необходимости связаться с банком и подтвердить или обновить какую-либо информацию по указанному номеру. Система требует аутентификации пользователя, посредством ввода PIN-кода или пароля. Поэтому, заранее записав ключевую фразу, можно выведать всю нужную информацию. К примеру, практически любой человек может записать типичную команду: «Нажмите 1, для смены пароля. Нажмите 2, чтобы получить ответ оператора» и воспроизвести её вручную в нужный момент времени, создав впечатление работающей в данный момент системы предварительно записанных голосовых сообщений.

2.5. Претекстинг

Претекстинг (англ. *pretexting*) – атака, при которой мошенник представляется другим человеком и по заранее спланированному сценарию выпытывает конфиденциальную информацию у атакуемого лица. Данный тип атаки невозможен без должной подготовки и сценария, к примеру, полезной информацией считается: дата рождения, ИНН, паспортные данные либо последние цифры счета. Все это необходимо для того, чтобы не вызвать подозрений у жертвы.

2.6. Квид про кво

Квид про кво (от лат. *Quid pro quo* – «то за это») – в английском языке данное выражение используют в значении «услуга за услугу». Атака подобного рода подразумевает обращение злоумышленника в организацию по корпоративному телефону (используя актерское мастерство и смекалку)

либо по электронной почте. Часто злоумышленник представляется сотрудником технической поддержки, который сообщает о обнаружении технических проблем на рабочем месте сотрудника и предлагает свою помощь в их устранении. В процессе «решения» технических проблем, мошенник вынуждает жертву совершать действия, позволяющие атакующему запускать команды или устанавливать различного рода программные продукты на компьютер жертвы.

2.7. Дорожное яблоко

Дорожное яблоко – это метод атаки представляет собой подбрасывание «инфицированных» физических носителей информации в местах общего доступа, где эти носители могут быть легко найдены. Местами для «подбрасывания» могут служить туалеты, парковки, столовые, или рабочее место атакуемого сотрудника. Внешний вид физического носителя маскируется как принадлежащий атакуемой организации, либо просто на носитель ставится отметка, которая призванна вызвать любопытство у сотрудников организации.

2.8. Сбор информации из открытых источников

На данный момент один из самых популярных методов получения информации о человеке, является ее сбор из открытых источников, в большинстве случаев из социальных сетей. К примеру, такие сайты как «livejournal», «Одноклассники», «ВКонтакте», «Instagram», «Facebook» содержат огромное количество информации, которую люди и не пытаются скрыть. Зачастую, пользователи социальных сетей не уделяют должного внимания вопросам безопасности, оставляя в свободном доступе информацию и сведения, которые вполне могут быть использованы мошенником для совершения очередной атаки.

В качестве показательного примера может служить история о похищении сына Евгения Касперского. В ходе следствия было выявлено, что злоумышленники узнали расписание дня и маршруты следования подростка из его записей на странице в социальной сети [5].

Несмотря на то, что зачастую пользователь имеет возможность ограничивать доступ к информации на своей странице в социальной сети, это все равно не дает гарантии того, что она никогда не попадет в руки злоумышленников [6].

Выводы

Технические средства меняются, а вот психология людей – остается прежней. Если выработать у сотрудников привычку всякий раз, заметив отклонения в повседневной работе, звонить в службу безопасности,

то это, безусловно, добавит определенных хлопот, однако это все же лучше, чем думать, что все в порядке, и продолжать игнорировать предпосылки для нарушения целостности и безопасности системы. Один проигнорированный случай нарушения может лишить организацию всего. В своей работе авторы исследуют существующие методы социальной инженерии, а также влияние человеческого фактора на вопросы информационной безопасности.

Список используемых источников

1. Андрианов В. И., Красов А. В., Липатников В. А. Внновационное управление рисками информационной безопасности: учебное пособие. Федеральное агентство связи, Федеральное гос. образовательное бюджетное учреждение высш. проф. образования «Санкт-Петербургский гос. ун-т телекоммуникаций им. проф. М. А. Бонч-Бруевича». Санкт-Петербург, 2012.

2. Краткое введение в социальную инженерию [Электронный ресурс] // Режим электронного: https://habrahabr.ru/post/83415/ (дата обращения 22.09.2017).

3. Кевин Д. Митник; Вильям Л. Саймон. Искусство обмана. АйТи, 2004. 360 с.

4. Социальная инженерия [Электронный ресурс] // Режим доступа: http://www.hg.org/article.asp?id=5778 (дата обращения 22.09.2017).

5. Дело о похищении Ивана Касперского [Электронный ресурс] // Режим доступа: https://rg.ru/sujet/4383/ (дата обращения 22.09.2017).

6. Социальная инженерия [Электронный ресурс] // Режим доступа: https://ru.wikipedia.org/wiki/социальная инженерия (дата обращения 22.09.2017).

УДК 371.687:621.3.037.37

АНАЛИЗ МЕТОДОВ ОЦЕНКИ ПРОПУСКНОЙ СПОСОБНОСТИ МУЛЬТИСЕРВИСНОЙ СЕТИ

П. А. Дунаев, С. Ю. Рябцунов

Казахский агротехнический университет им. С. Сейфуллина

Рассматриваются методы моделирования пропускной способности мультисервисеной сети с учетом времени задержки IP-пакетов. Реализована программа DelayProg для расчета пропускной способности канала при заданной вероятности безотказной работы (св. РК № 1105), что подтверждает научную новизну данной работы.

методы моделирования, время задержки, пропускная способность, IP-пакет.

В рамках исследований, проводимых по теме «Разработка и исследование методов оценки качества изображения в цифровом телевидении», одним из рассматриваемых факторов является оценка пропускной способности мультисервисной сети.

На мультисервисной IP-сети важными элементами транспортной инфраструктуры являются компрессоры, маршрутизаторы и серверы с цифровой обработкой сигналов вносящие основные задержки в сеть.

Построим простейшую модель сети с задержкой, вносимой одним компрессором, одним сервером цифровой обработки сигнала и одним маршрутизатором. Обозначим соответственно задержки: t_C, t_S, t_R.

В условиях реальной эксплуатации сети при смене IP-пакетов будет затрачиваться дополнительное время на его обработку, т. е. время ожидания их в очередях промежуточных маршрутизаторов и коммутаторов сети. Обозначим его $t_{обр}$.

Тогда пропускную способность сети можно вычислить как:

$$B_n = \frac{1}{t_C + t_S + t_R + t_{обр}}$$

Так как мультисервисные сети являются системами массового обслуживания и имеют параллельную схему функционирования, следовательно, пропускная способность сети возрастет в N раз в результате увеличения числа каналов обслуживания.

В данном случае пропускная способность будет равна:

$$B_n = \frac{1}{t_C + t_S + t_R + t_{обр}} \times N$$

Учитывая разные варианты обслуживания IP-пакетов [1], можем записать:

$$B_n = \frac{1}{max\left(t_{IP1}, t_{IP2}\right) + t_{обр}} \times N$$

Согласно проведенным исследованиям [2], время обслуживания IP-пакетов подчиняется нормальному закону распределения.

Поэтому:

$$B_n = \frac{1}{\sqrt{\frac{1}{N^2}\sum_{i=1}^{N} d_{xi}^2} + t_{обр}} \times N$$

Ориентировочно вносимое время задержки составляет: компрессорами – 15…50 мс, маршрутизаторами – 10…20 мс, серверами с цифровой обработкой сигналов – 80…150 мс [3].

Для формирования нормальной случайной величины (СВ) *Y* исходными данными являются границы равномерно распределенных СВ *X,* т. е. 105 и 220 мс соответственно.

Чтобы оценить степень разброса значений времени обслуживания относительно среднеквадратичного отклонения сгенерируем 10000 СВ с нормальной плотностью распределения вероятности, полученные результаты представлены на рис. 1.

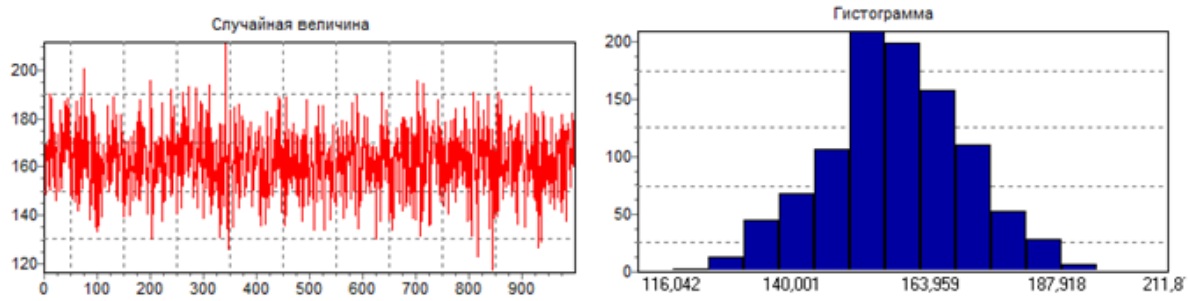


Рис. 1. График и гистограмма распределения СВ

На рис. 2. показана графическая зависимость времени обслуживания IP-пакетов от среднеквадратичного отклонения, с учетом результатов моделирования (рис. 1).

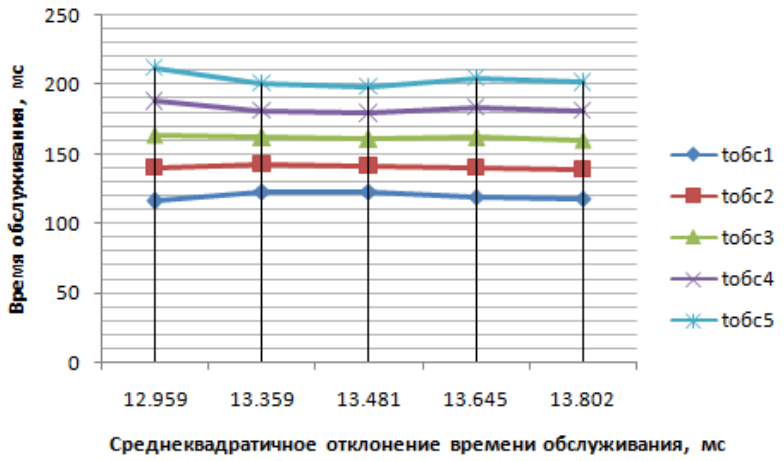


Рис. 2. Степень разброса значений времени обслуживания относительно среднеквадратичного отклонения

Из приведенного выше графика видно, что не наблюдается определенной функциональной зависимости, с помощью которой можно было судить о пропускной способности сети.

Вследствие этого было решено воспользоваться методом статистического моделирования, а именно метода Монте-Карло [4].

Алгоритм работы модели сети IP, представлен на рис. 3 [5].

Моделирование задержек IP-пакетов и соответственно расчет пропускной способности канала осуществлялось в разработанной программе DelayProg [6].

Изменяя значения вероятности безотказной работы согласно [7, 8, 9, 10], в результате моделирования получаем данные, по которым строятся графические зависимости от вероятности безотказной работы компрессора, сервера, маршрутизатора [5].

В DelayProg реализована возможность задавать размер информационного IP-пакета.

Поскольку стратегическим преимуществом, на сегодняшний день, обладает технология FTTH, в этом случае, можно использовать любой из способов передачи данных: SDH, ATM, Ethernet. Однако предпочтение в основном отдается Ethernet-протоколам [3].

При минимальном размере Ethernet-кадра в 64 байта изменение пропускной способности канала представлено на рис. 4 (см. ниже).

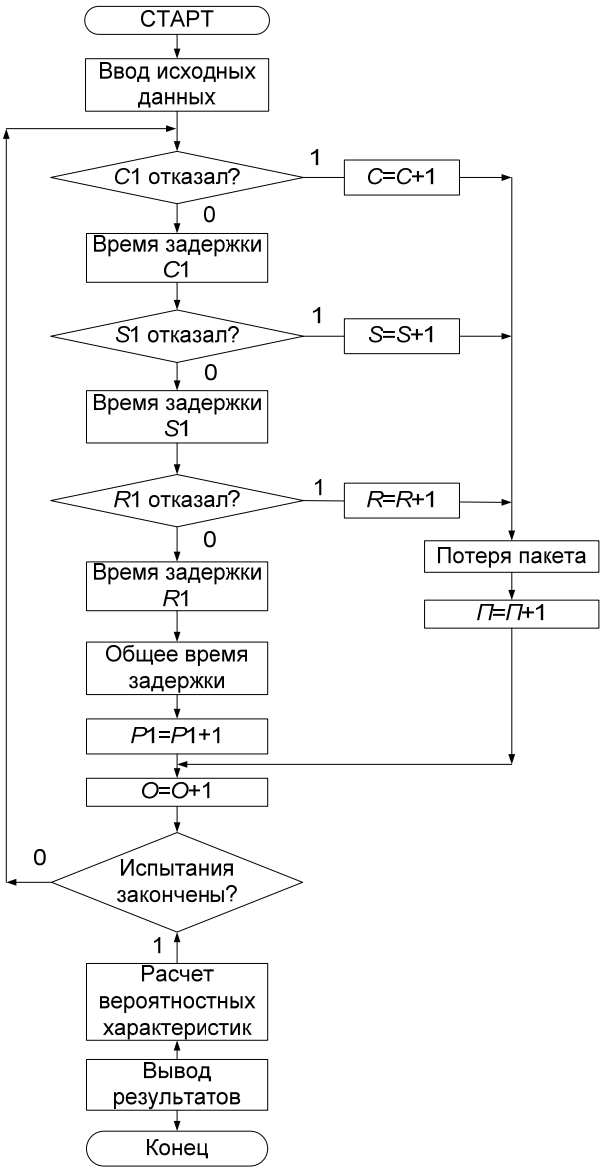


Рис. 3. Алгоритм работы модели сети IP

Выводы

Разработан алгоритм работы модели IP-сети для оценки пропускной способности канала в зависимости от времени обслуживания IP-пакетов.

При заданных задержках компрессора, сервера, маршрутизатора и заданных вероятностях безотказной работы оборудования от 0,98 до 1 определено, что при размере Ethernet-кадра в 64 байта пропускная способность изменяется от 30,9 до 37,3 Мб/с.

Рис. 4. Графическая зависимость пропускной способности от вероятности безотказной работы

Список используемых источников

1. Дунаев П. А., Наурыз К. Ж. Влияние времени обслуживания IP-пакетов на пропускную способность мультисервисной сети // Молодой исследователь: вызовы и перспективы: сб. ст. по материалам L междунар. науч.-практ. конф. № 25 (50). М. : Интернаука, 2017. 299 с.

2. Вентцель Е. С. Исследование операций. М. : Сов. радио, 1972. 552 с.

3. Мамчев Г. В. Использование в телевизионном вещании интернет – протокола. Новосибирск : СибГУТИ, 2009. 156 с.

4. Михайлов Г. А., Войтишек А. В. Численное статистическое моделирование. Методы Монте-Карло: учеб. пособие для студ. вузов. М. : Академия, 2006. 368 с.

5. Дунаев П. А., Рябцунов С. Ю. Статистическое моделирование IPTV-сети для оценки пропускной способности канала с учетом времени обслуживания пакетов // Доклады ТУСУР. Томск : Издательство ТУСУР, 2017. № 3 (20). С. 172–176.

6. Дунаев П. А., Рябцунов С. Ю. Свидетельство о государственной регистрации прав на объект авторского права 008473 РК. DelayProg (программа для ЭВМ). – № 1105; заявл. 07.04.2017; Опубл. 23.05.2017. – Министерство Юстиции Республики Казахстан.

7. ГОСТ Р 27.002-2009. Надежность в технике. Термины и определения. М. : Стандартинформ, 2011. 26 с.

8. ГОСТ Р 27.403-2009. Надежность в технике. Планы испытаний для контроля вероятности безотказной работы. М. : Стандартинформ, 2011. 10 с.

9. ГОСТ Р 27.607-2013. Надежность в технике. Управление надежностью. Условия проведения испытаний на безотказность и статистические критерии и методы оценки их результатов. М. : Стандартинформ, 2015. 46 с.

10. ГОСТ Р 51901.16-2017. Повышение надежности. Статистические критерии и методы оценки. М. : Стандартинформ, 2017. 39 с.

УДК 004.732

АНАЛИЗ МЕТОДОВ ПОСТРОЕНИЯ СЕТЕЙ WI-FI ВЫСОКОЙ ПЛОТНОСТИ

Р. А. Дунайцев, А. А. Егорова

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

В статье рассматриваются особенности работы сетей Wi-Fi при большом числе пользователей и клиентских устройств в ограниченном пространстве. Проводится анализ и сравнение рекомендаций производителей беспроводного сетевого оборудования по построению сетей Wi-Fi высокой плотности.

Wi-Fi, IEEE 802.11, сеть высокой плотности, радиопланирование, точка доступа.

В настоящее время сети Wi-Fi есть практически везде, включая аудитории, конференц-залы, стадионы и тому подобные места с большим скоплением людей. Поэтому планирование сетей Wi-Fi с учетом высокой плотности пользователей является актуальной задачей.

Факторы, которые необходимо учитывать при проектировании подобных сетей Wi-Fi, включают: тип объекта, планировка этажа и высота потолка, используемые строительные материалы и наличие препятствий, количество этажей, число пользователей в конкретной области, обслуживаемой одной точкой доступа, среднее число мобильных устройств с поддержкой Wi-Fi на одного пользователя, доля активных пользователей, типы запускаемых приложений и необходимая для их работы скорость передачи, а также используемые частотные диапазоны (2,4 ГГц и 5 ГГц).

Чтобы теоретически определить пропускную способность, обеспечиваемую точкой доступа каждому пользователя, нужно поделить пропускную способность точки доступа на количество активных пользователей, подключенных к ней. Например, теоретическая скорость передачи точки доступа, которую она может поддерживать, составляет 600 Мбит/с. Если предположить, что 25 пользователей будут одновременно пользоваться Wi-Fi в этой области, можно ошибочно посчитать, что такая точка доступа сможет обеспечить 24 Мбит/с для каждого из них. Но на практике, как показано на рис. 1, это значение оказывается гораздо ниже. Существует ряд факторов, которые существенно снижают реальную пропускную способность по сравнению с теоретическим максимумом точки доступа. К таким факторам относятся накладные расходов протоколов и алгоритмов (уменьшают пропускную способность на 40–50 %), низкоскоростные или удаленные

клиенты (клиенты, которые находятся в зоне слабого сигнала, могут привести к дополнительному снижению пропускной способности), неравномерное распределение клиентов и др. [1].

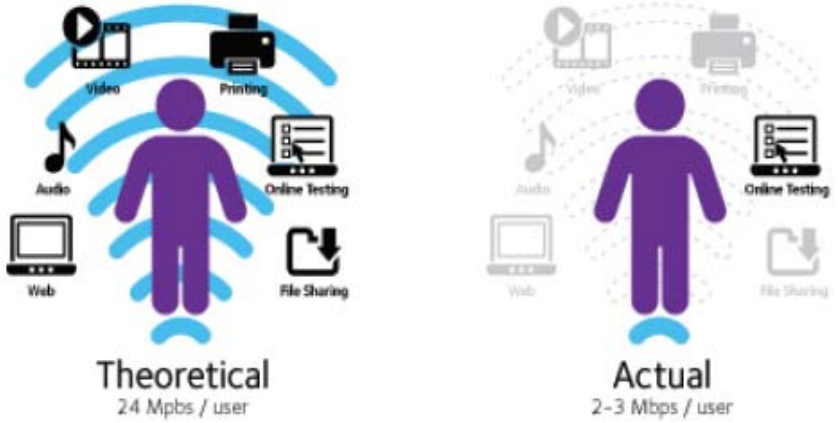


Рис. 1. Теоретическая и реальная пропускная способность на клиента

При проектировании беспроводных сетей высокой плотности очень важно понять, какие приложения будут использоваться и сколько полосы пропускания будет потребляться каждым пользователем. В таблице приведены некоторые общие рекомендации о том, сколько пропускной способности необходимо для обычных приложений, таких как передача аудио и видео, отправка документов на печать, обмен файлами и резервное копирование [2].

ТАБЛИЦА Необходимая полоса пропускания для различных приложений

Приложение	Пропускная способность, Мбит/с
Аудио	0,1–0,5
Резервное копирование	10–50
Обмен файлами	1–10
Печать	1–2
Видео (480)	2–3
Видео (720)	4–6
Видео (1080)	10–12
Web	0,5–1

Следующие рекомендации основаны на многих успешных внедрениях и могут служить в качестве руководства для проектирования, планирования и развертывания беспроводной сети в среде с высокой плотностью пользователей и мобильных устройств.

1) Следует использовать преимущественно двухдиапазонные точки доступа (2,4 ГГц и 5 ГГц) для обеспечения максимальной пропускной способности.

2) Точки доступа следует располагать так, чтобы каждый клиент всегда «слышал» две или три соседние точки доступа. Если одна точка доступа оказывается перегружена, клиент может быть подключен к другой точке доступа без какого-либо ухудшения качества обслуживания.

3) Использовать балансировку трафика для равномерного распределения клиентов между точками доступа. По результатам тестирования, Netgear рекомендует устанавливать максимальное количество клиентов от 25 до 30 на один радиомодуль [1].

4) Снизить выходную мощность передатчика точки доступа до уровня типового клиентского устройства.

5) Ограничить количество используемых SSID, так как использование более пяти SSID ведет к неэффективному использованию эфирного времени.

6) Отказаться от объединения каналов. Например, IEEE 802.11n разрешает использовать канал шириной 40 МГц путем объединения двух каналов по 20 МГц, что значительно увеличивает скорость передачи. Но это практично только для каналов в диапазоне 5 ГГц, поскольку диапазон 2,4 ГГц крайне ограничен в количестве непересекающихся каналов.

7) Технология Aruba для выбора канала использует распределенный алгоритм, где каждая точка доступа самостоятельно принимает решение путем измерения радиоэфира. Каждый узел доступа периодически сканирует все разрешенные каналы, клиентов, фоновый шум и помехи. Таким образом получают два показателя: «индекс помех» и «индекс покрытия». Эти показатели используются для выбора оптимального канала и мощности передатчика [3].

8) Динамическое планирование эфирного времени (рис. 2) повышает производительность сети для высокоскоростных клиентов за счет уменьшения эфирного времени клиентами с низкой скоростью [4]. В традиционной сети Wi-Fi обеспечиваются равные возможности доступа к среде передачи для всех клиентов. Более медленные клиенты используют значительно больше эфирного времени для передачи того же объема данных по сравнению с высокоскоростными клиентами. Для решения этой проблемы точки доступа компании Aerohive выделяют эфирное время на каждого клиента индивидуально, путем динамического расчета потребления эфирного времени. Это приводит к более высокой пропускной способности для более быстрых клиентов без отрицательного воздействия на медленных клиентов.

9) Компания Ruckus предлагает применять в точках доступа активные антенные решетки, способные формировать диаграмму направленности в нужном направлении [5]. Это позволяет задействовать передатчик точки

доступа на полную мощность, чтобы обмениваться данными с клиентом на максимально возможных скоростях. В результате удается добиться более высокой емкости беспроводной сети. Разработанные Ruckus антенные решетки BeamFlex обеспечивают формирование точкой доступа до нескольких тысяч уникальных диаграмм направленности для каждого отдельного клиента и даже для каждого передаваемого кадра в соответствии с особенностями радиоэфира (рис. 3).

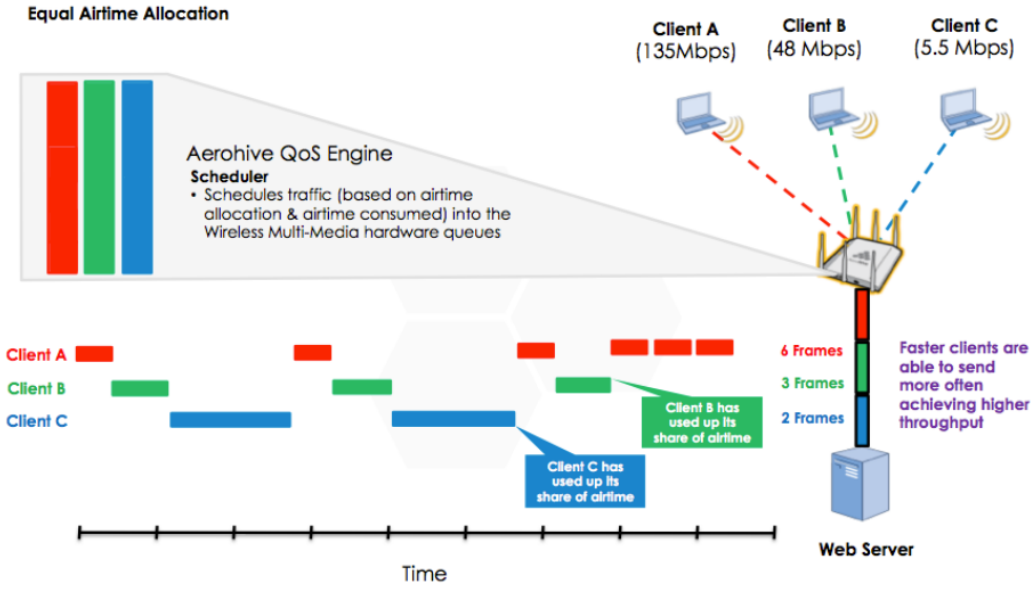


Рис. 2. Динамическое планирование эфирного времени

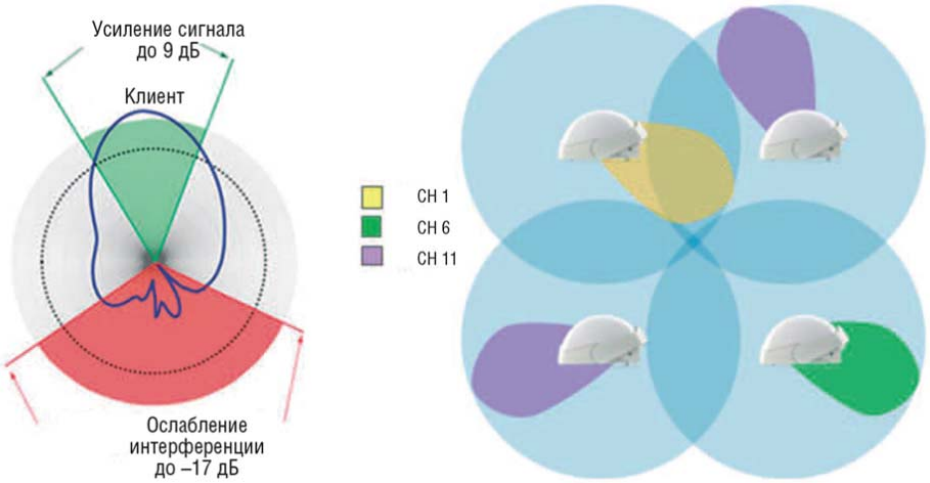


Рис. 3. Диаграмма направленности антенной решетки BeamFlex

Список используемых источников

1. Best practices for high-density wireless network design in education and small-medium businesses: 2013 NETGEAR Inc. 8 с.

2. Wireless LAN design guide for high-density client environments in higher education: 2011. CISCO. 40 с.

3. High-density wireless networks for auditoriums – validated reference design. ARUBA. 179 с.

4. High-density Wi-Fi design principles. AEROHIVE. 113 с.

5. Deploying high density Wi-Fi – design and configuration guide for enterprise. RUCKUS. 36 с.

УДК 519.218

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ХАРАКТЕРИСТИК ТРАФИКА РЕАЛЬНОГО ВРЕМЕНИ НА СТОРОНЕ ОТПРАВИТЕЛЯ И СТОРОНЕ ПОЛУЧАТЕЛЯ

Р. А. Дунайцев, О. Р. Кулебякина

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

При передаче трафика по сетям связи, его статистические характеристики могут подвергаться изменениям. Это обусловлено задержками, коллизиями, потерями пакетов, различными ошибками при передаче и другими факторами. В проведенном эксперименте трафик изменился с антиперсистентного на самоподобный.

трафик, самоподобие, антиперсистентность, параметр Херста.

Эксперимент проводится для трафика, переданного через сеть Интернет. Сравниваются результаты расчета значения параметра Херста до и после прохождения трафика по сетям связи. Цель эксперимента состоит в наблюдении изменения свойства самоподобия трафика после передачи по сетям связи. Знание характеристик трафика, например, наличия самоподобия или антиперсистентности, позволит лучше спрогнозировать нагрузку на сеть связи.

Для проведения эксперимента был произведена передача потокового видео, для чего использовался ресурс. Видео закодировано кодеком G.711. Для захвата трафика использовалось ПО Wireshark, затем трафик фильтровался по нужному протоколу. На рис. 1 и 2 показана нагрузка на сеть для трафика отправителя и получателя.

На рис. 1 видно, что нагрузка на сеть равномерна и количество пакетов составляет 143294. На рис. 2 наблюдается менее равномерная нагрузка на сеть, появились более заметные пики и спады. Количество пакетов увеличилось и составляет 152974.

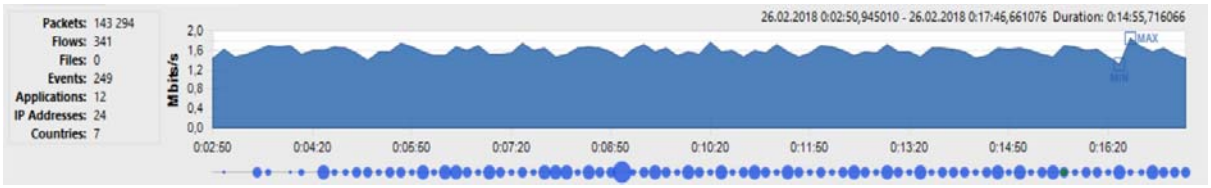


Рис. 1. Трафик на стороне отправителя

Рис. 2. Трафик на стороне получателя

Рассмотрим круговую диаграмму распределения пакетов по размеру. На рис. 3 видно, что размер большинства передаваемых пакетов составляет от 1024 до 1517 байт. Из рис. 4 следует, что количество пакетов меньшего размера значительно увеличилось, что говорит о том, что многие пакеты подверглись фрагментации при прохождении по сетям связи. Отсюда можно сделать вывод о том, что трафик значительно видоизменялся при прохождении сети связи.

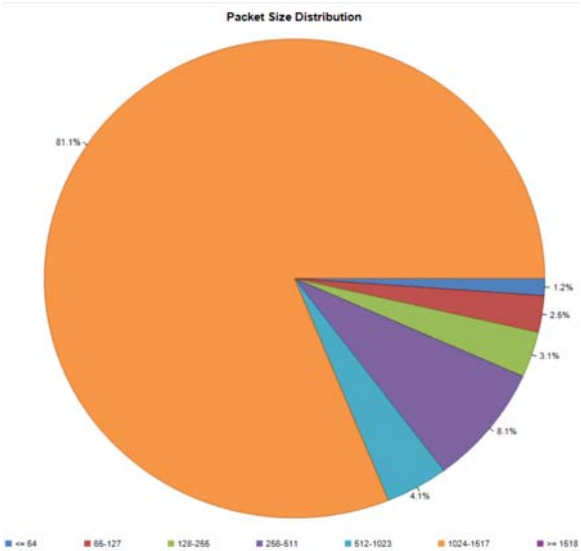


Рис. 3. Размер пакетов на стороне отправителя

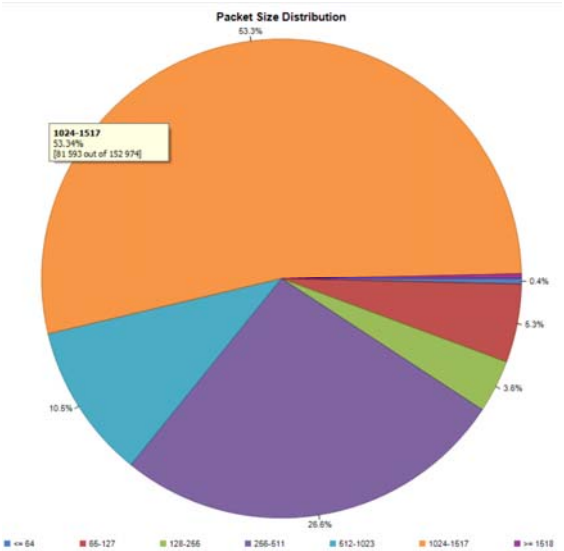


Рис. 4. Размер пакетов на стороне получателя

Далее был рассчитан параметр Херста с помощью ПО MATLAB. Для передающей стороны график R/S функции представлен на рис. 5. На рис. 6 представлен график R/S функции для принимающей стороны.

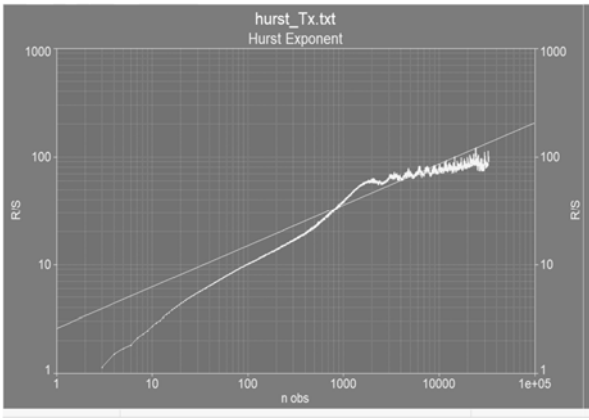


Рис. 5 График R/S функции для стороны передачи

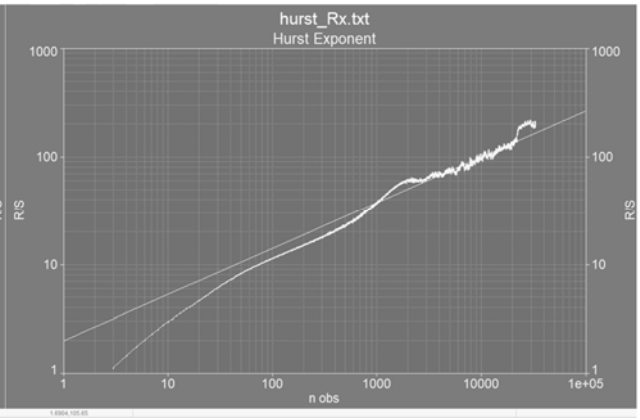


Рис. 6. График R/S функции для стороны приема

В результате расчетов получили следующие значения параметра Херста: для передающей стороны H = 0,4186, а для принимающей стороны H = 0,5328. Следовательно, можно сделать вывод о том, что трафик после передачи по сетям связи в нашем эксперименте изменился с антиперсистентного на самоподобный [1]. Далее мы уменьшили количество отсчетов – разницу во времени между приходом каждого пакета, чтобы получились равные промежутки между расчетами H. На рис. 7 показан график зависимости параметр Херста от количества отсчетов в диапазоне от 1 до 140000-го отсчета. На этом графике видно, что трафик передающей стороны стремится к антиперсистентности большую часть времени.

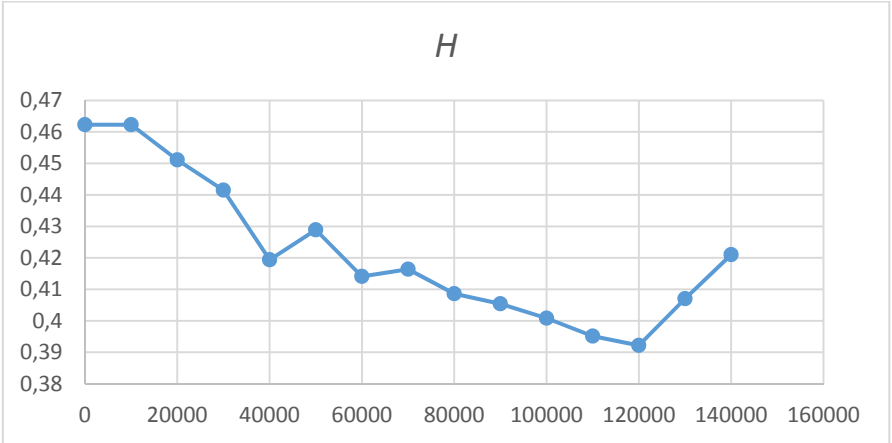


Рис. 7. Зависимость значения параметра Херста от количества отсчетов для передающей стороны

Из полученных результатов можно сделать вывод о том, что характеристики трафика заметно видоизменяются после передачи по сетям связи. В проведенном эксперименте трафик на передающей стороне был антиперсистентным, а на принимающей стороне уже демонстрирует свойство самоподобия.

Список используемых источников

1. Карпухин А. В., Кириченко Л. О., Грицив Д. И., Ткаченко А. А. Применение методов нелинейной динамики и фрактального анализа для оценивания работы инфокоммуникационных систем с протоколом TCP // Cloud of Science: электронный журнал. 2014. Т. 1. № 2. С. 258–271.

2. Едемская Е. Н., Бельков Д. В. Исследование сетевого трафика с помощью функции Херста // Информатика и кибернетика. 2015. № 2. С. 39–46.

УДК 519.218

АНАЛИЗ ХАРАКТЕРИСТИК АГРЕГИРОВАННОГО ТРАФИКА

Р. А. Дунайцев, А. А. Москалюк

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

Одним из важных свойств сетевого трафика является его свойство самоподобия. Зная, насколько самоподобен трафик, можно прогнозировать его поведение в будущем. В данной статье предлагается сравнить результаты расчетов параметра Херста для трассировки трафика, полученного от множества пользователей, и трассировки трафика, полученного от одного из этих пользователей, но сложенного с собой несколько раз так, чтобы сымитировать работу того же количества пользователей, что и в исходном агрегированном трафике.

трафик, самоподобие, антиперсистентность, параметр Херста.

В данной статье рассматривается возможность оценки параметра Херста агрегированного трафика множества пользователей по потоку одного из них. Для проведения эксперимента использовалась корпоративная сеть с тридцати тремя пользователями, у каждого из которых имеется канал со скоростью 1 Гбит/с для подключения к файловому серверу. Сбор общего трафика осуществляется на стороне файлового сервера, затем из общего потока выделялся трафик одного пользователя и складывался сам с собой *n* раз. Для исследования был выбран исходящий с сервера трафик, так как именно он создает основную нагрузку на сеть.

Путем сложения трафика пользователя с самим собой n раз, в зависимости от его доли в агрегированном трафике, получим имитацию трафика от n пользователей. Пользователи для проведения эксперимента были выбраны в соответствии их активностью в сети. Для сбора трафика применен следующий фильтр Wireshark: port 445 и ip.src 192.168.10.1. Таким образом

собирается только исходящий от сервера трафик по протоколу SMB2. Также было установлено ограничение на захват не более чем 200000 пакетов. На момент захвата трафика в сети находилось и вело обмен с сервером 33 пользователя. Чтобы выбрать пользователей для участия в эксперименте, использовалось ПО Savvius Omnipeek. На рис. 1 представлен трафик 5 пользователей, которые вели самый активный обмен с сервером.

Node	Country	Total Bytes %	Total Bytes	Packets Sent	Packets Received
192.168.10.128	Private Network	12,211%	58 561 438	0	68 637
192.168.10.30	Private Network	1,820%	8 729 954	0	42 060
192.168.10.118	Private Network	47,598%	228 756 149	0	12 945
192.168.10.125	Private Network	6,434%	30 857 870	0	7 816
192.168.10.106	Private Network	1,871%	8 971 260	0	7 302

Рис. 1. Самые активные пользователи

Обозначим пользователей как П1 (192.168.10.128), П2 (192.168.10.30), П3 (192.168.10.118), П4 (192.168.10.125), П5 (192.168.10.106). После фильтрации трафика в ПО Wireshark оказалось, что трафик этих пользователей составляет 69,4 % от общего трафика или 138760 пакетов (рис. 2).

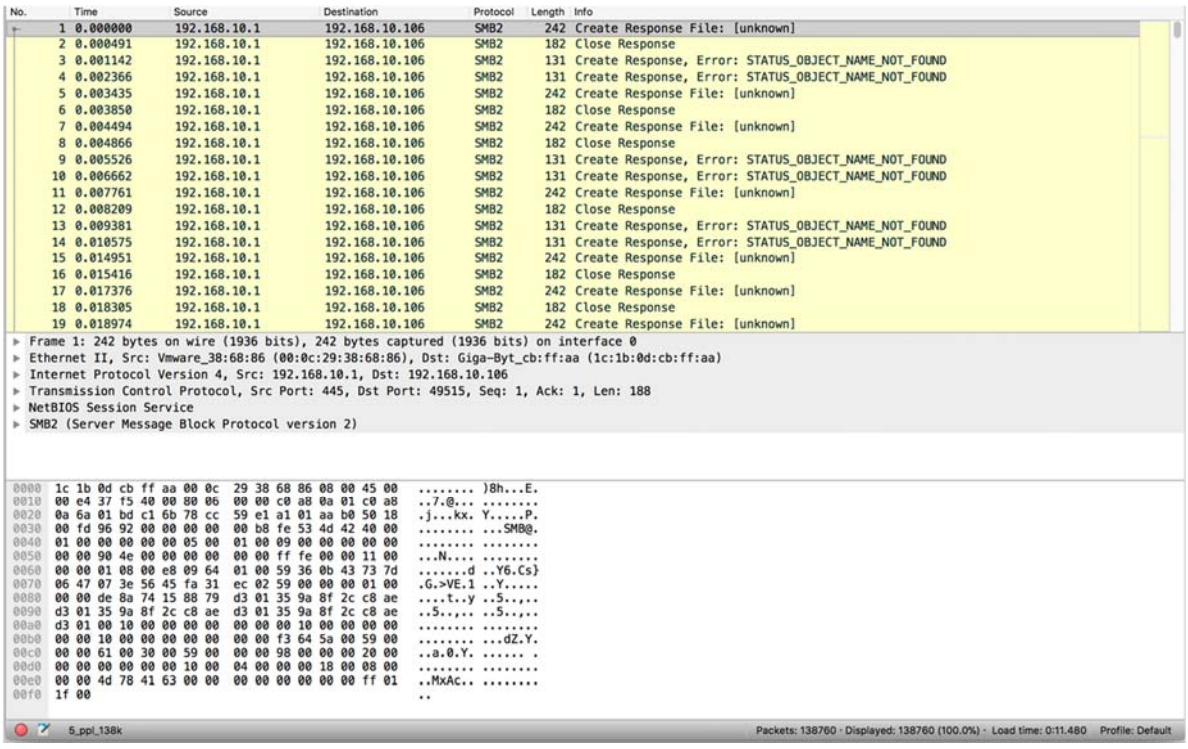


Рис. 2. Трафик выбранных пользователей

Из 5-ти представленных выше пользователей необходимо выбрать одного. Для проведения эксперимента был выбран пользователь П1. Трафик пользователя суммируется с временным сдвигом, равным одной секунде. При первом проведении эксперимента суммирование выполняется таким образом, чтобы количество пакетов было максимально близко к количеству

пакетов в исходном трафике 5 пользователей, а затем так, чтобы количество переданных байт было примерно равно количеству байт информации в исходном трафике. Далее предлагается сравнить характеристики общего и суммированного трафика.

На рис. 3–5 представлены графики нагрузки на сеть. Хорошо заметно изменение максимальной и средней нагрузки для разных видов трафика. Из рис. 5 видно, что нагрузка на сеть приблизилась к исходной нагрузке на сеть от 5 пользователей.

Далее переходим к расчету параметра Херста. Для расчета параметра Херста будем использовать ПО MATLAB. При значении параметра Херста более 0,5 трафик можно считать самоподобным. Тенденция его изменения может быть спрогнозирована [1].

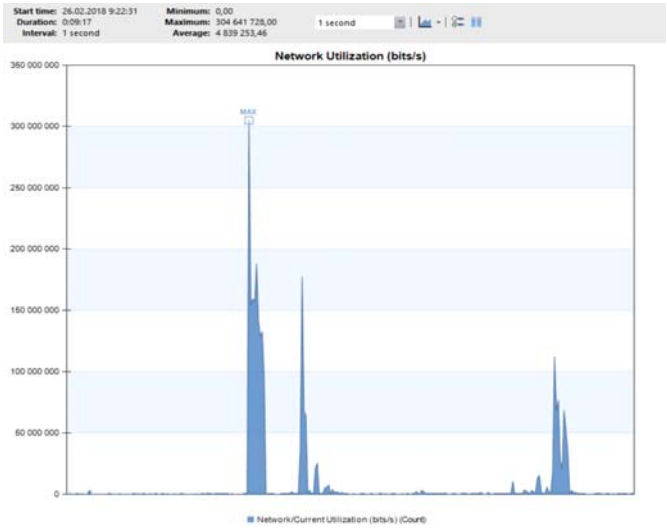


Рис. 3. Нагрузка на сеть исходного трафика

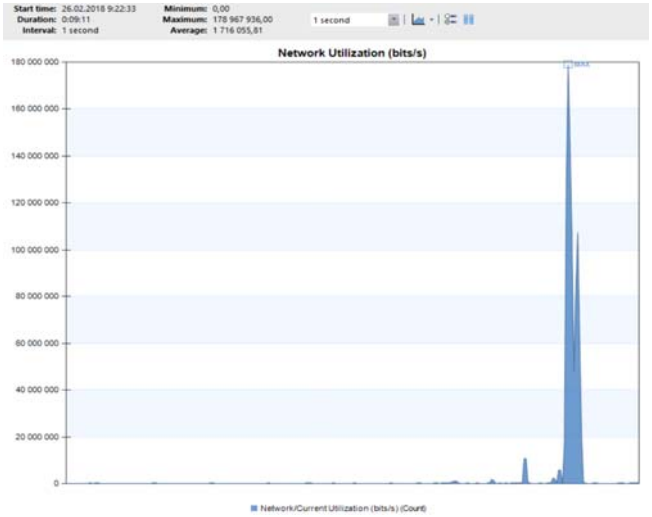


Рис. 4. Нагрузка на сеть суммированного по количеству пакетов трафика

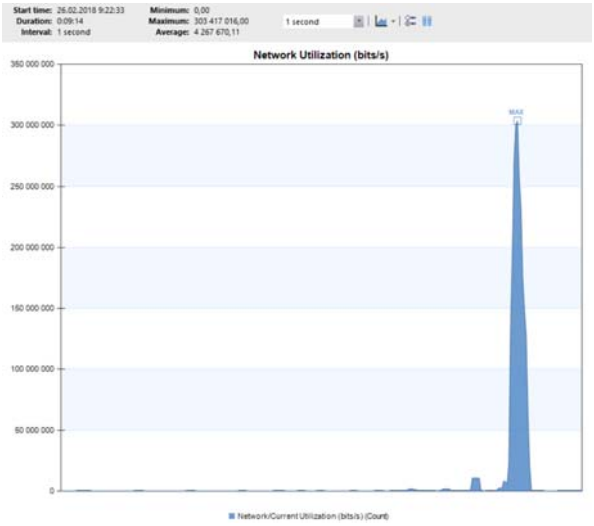


Рис. 5. Нагрузка на сеть суммированного по количеству байт трафика

Обозначим исходный трафик 5 пользователей как H1, трафик пользователя П1 как H2. Трафик, суммированный по количеству пакетов и по количеству переданных байт, как H3 и H4 соответственно. Результаты расчетов приведены в таблице.

ТАБЛИЦА. Результаты расчетов

H1	H2	H3	H4
0,6670	0,6444	0,6574	0,6520

На рис. 6 и 7 представлены графики R/S функции для каждого трафика.

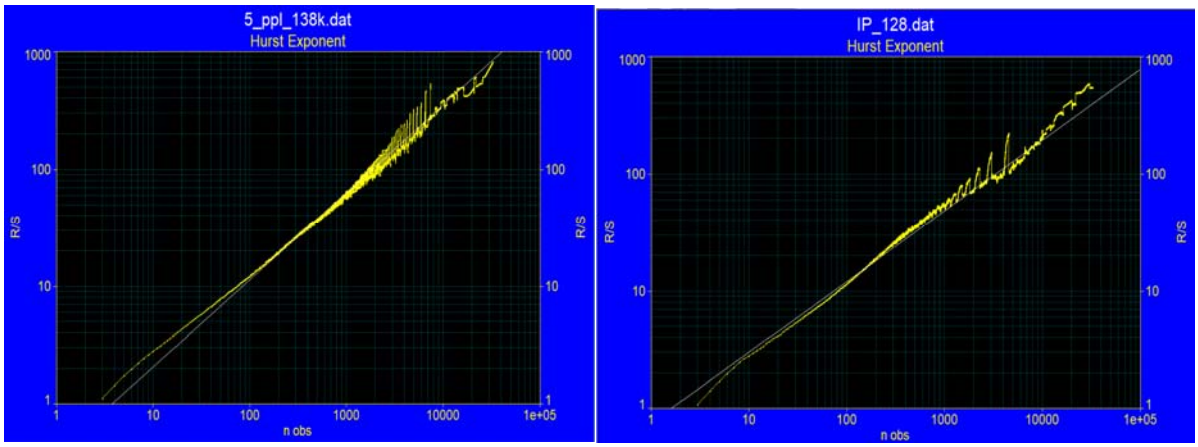


Рис. 6. График R/S функции H1 и H2

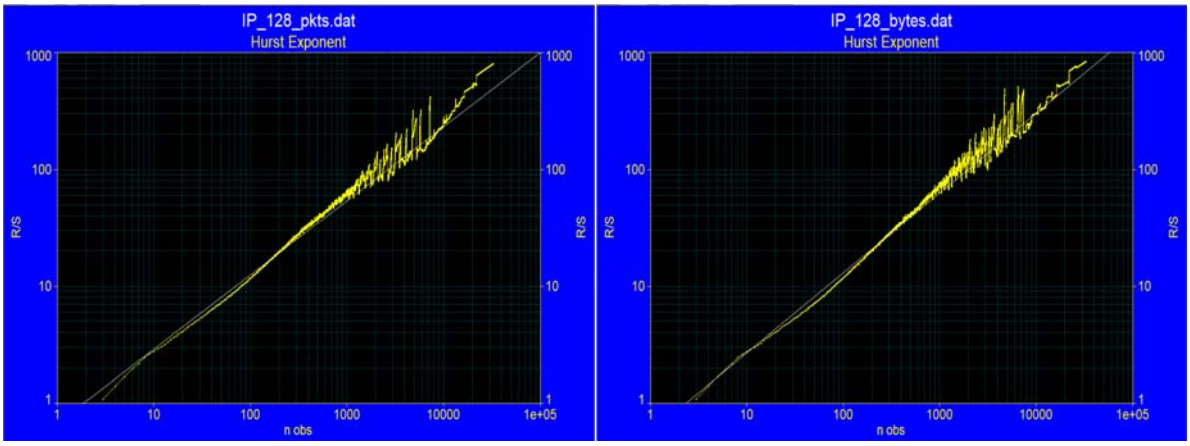


Рис. 7. График R/S функции H3 и H4

На основании полученных после расчетов данных можно сделать следующие выводы. Во-первых, оценка степени самоподобия агрегированного трафика по одному пользователю является возможной, хотя и с небольшой погрешностью. Чем больше совпадает количество переданных пакетов в агрегированном трафике и трафике одного пользователя, тем точнее значение параметра Херста. Во-вторых, после суммирования трафик сохранил свойство самоподобия.

Список используемых источников

1. Амосов О. С., Муллер Н. В. Исследование временных рядов с применением методов фрактального и вейвлет анализа [Электронный ресурс]. URL: https://naukovedenie.ru/PDF/147TVN314.pdf (дата обращения 28.03.2018).

УДК 004.732

ИССЛЕДОВАНИЕ ХАРАКТЕРИСТИК СЕТИ WI-FI ПЕТЕРБУРГСКОГО МЕТРОПОЛИТЕНА

Р. А. Дунайцев, П. А. Овчинникова, А. С. Петренко

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

В статье представлены результаты радиообследования поездов Петербургского метрополитена. В ходе работы с помощью специализированного ПО были собраны данные по расположению точек доступа в вагонах поезда, используемым частотным диапазонам и задействованным каналам в подвижном составе.

Wi-Fi, радиообследование, беспроводная локальная сеть, точка доступа.

Сейчас все популярнее становятся системы беспроводного доступа. На современном этапе развития сетевых технологий, технология Wi-Fi является наиболее удобной в условиях, требующих мобильности, простоты установки и использования. Так, например, по результатам статистики, в жилье, сдаваемом для отдыха в России, более 90 % (в совокупном представлении) оснащено беспроводными точками доступа (ТД) и среди самых оснащенных городов Санкт-Петербург занимает третье место – 93,8 % [1], что свидетельствует о высоком пользовательском спросе на доступность подключения к сети. Также следует отметить, что идея создания и внедрения муниципальных сетей в Санкт-Петербурге уже частично реализована: на территории площадью 3,5 квадратных километров были размещены 320 хот-спотов, покрывающие Центральный, Василеостровский и Петроградский районы города [2], а в 2017 г. Wi-Fi появился и в метро. Следует отметить, что в Петербургском метро Wi-Fi тестировали еще в 2007 г. Но в итоге проект не получил продолжения. Представители «большой тройки» сотовых операторов (Мегафон, МТС и Вымпелком) заявили, что не имеют планов по созданию сетей Wi-Fi в Петербургском метрополитене [3]. Однако в октябре 2016 г. конкурс на создание и обслуживание Wi-Fi в метро состоялся, и выиграла его телекоммуникационная компания «МаксимаТелеком». На сегодняшний день все станции московского и питерского метрополитена оснащены ТД, обеспечивающими доступ в Интернет для жителей и гостей города.

Целью работы был анализ характеристик сети Wi-Fi и радиоразведка в вагонах метрополитена. Для этого использовалась программа Ekahau Site Survey 9.0.3 [4], установленная на ноутбуке. В качестве карты мы использовали планы вагонов метрополитена, задав необходимый масштаб. Радиообследование проходило в пошаговом режиме: напротив каждой двери вагона запускалось сканирование каналов Wi-Fi. После этого мы перемещались к следующей двери и повторяли процедуру. Таким образом в каждом вагоне проводилось по 4 сканирования (рис. 1).

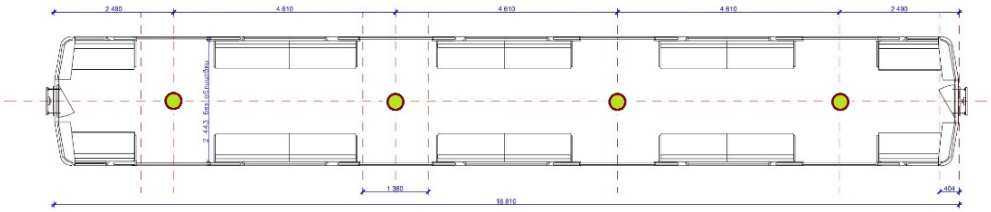


Рис. 1. Радиообследование в вагоне поезда

Так как встроенный в ноутбук беспроводный адаптер поддерживал лишь диапазон 2,4 ГГц, для сканирования каналов в обоих диапазонах было принято решение использовать внешний USB-адаптер ASUS USB-AC53 Nano.

В результате измерений было установлено, что в каждом вагоне находится по одной двухдиапазонной ТД «MT_FREE». Как правило, ТД расположены в конце вагона по ходу движения поезда (за исключением тех случаев, когда в ходе перестановки отдельных вагонов состава они оказывались в «развернутом» положении). Помимо этого, соседние ТД используют чередование непересекающихся частотных каналов. Для диапазона 2,4 ГГц применяются каналы 1, 6 и 11 шириной 20 МГц каждый (рис. 2) с поддержкой стандартов 802.11 g/n.

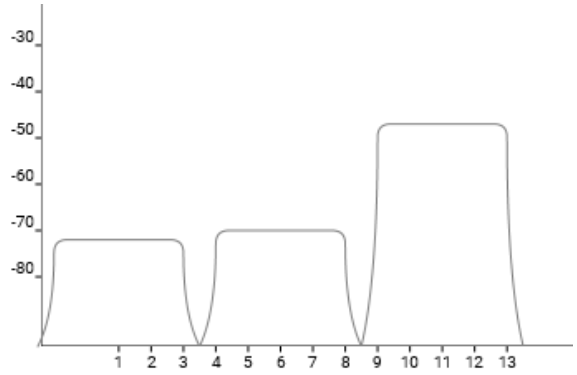


Рис. 2. Используемые каналы для диапазона 2,4 ГГц

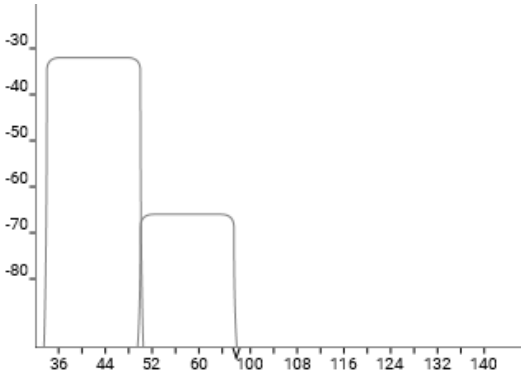


Рис. 3. Используемые каналы для диапазона 5 ГГц

В диапазоне 5 ГГц используются 3 канала шириной 80 МГц, а именно 36@80 (36/40/44/48), 56@80 (52/56/60/64) и 64@80 (52/56/60/64) (рис. 3). Использование таких широких частотных каналов призвано увеличить скорость передачи данных. Поддерживаемые стандарты в данном диапазоне – 802.11 a/n/ac.

Следует заметить, что по уровню сигнала ТД, находящиеся в соседних вагонах, обладают хорошим радиусом покрытия: «слышимость» ТД одного вагона в середине другого вагона по результатам измерения достигает относительно приемлемого уровня сигнала около –65 дБм, что дает потенциальную возможность части пассажиров подключаться к ТД, находящейся в другом вагоне, при перегрузке или выходе из строя ближайшей ТД.

Визуально предполагаемое расположение ТД получилось обнаружить только в некоторых типах вагонов под панелями, изображенными на рис. 4.

В ходе наших исследований мы также задались вопросом «А так ли востребована сеть Wi-Fi в метро?». За ответом мы обратились к популярному сайту отзывов otzovik.com [5]. Статистика оказалась неутешительной – большинство отзывов были отрицательными (рис. 5). Однако это может быть обусловлено тем, что многие отзывы были оставлены в период, когда сеть только начали запускать и покрытие оставляло желать лучшего (рис. 6).

Кроме того, низкий рейтинг объясняется тем, что из-за желания быстро окупить затраты на строительство сети пользователю показывают слишком большое количество рекламы (рис. 7).

Рис. 4. Предполагаемое расположение ТД в вагоне

Таким образом, в результате проведенного радиообследования было выявлено, что сеть Петербургского метрополитена удовлетворяет требованиям территориально-частотного планирования, а именно близлежащие ТД в обоих диапазонах 2,4 ГГц и 5 ГГц используют чередование непересекающихся каналов. Также в ходе работы мы определили предполагаемое расположение ТД. Однако при изучении вопроса о востребованности Wi-Fi в метро, мы столкнулись с множеством негативных отзывов, что требует дальнейшего исследования и выработки рекомендаций по улучшению сети.

Рис. 5. Общая статистика отзывов

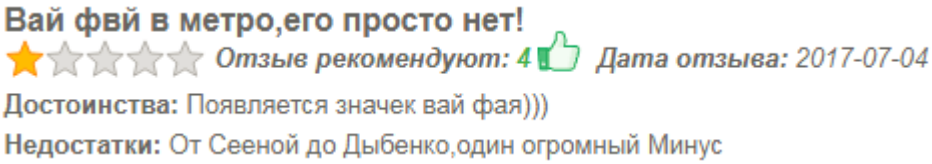


Рис. 6. Один из первых отзывов с сайта otzovik.com

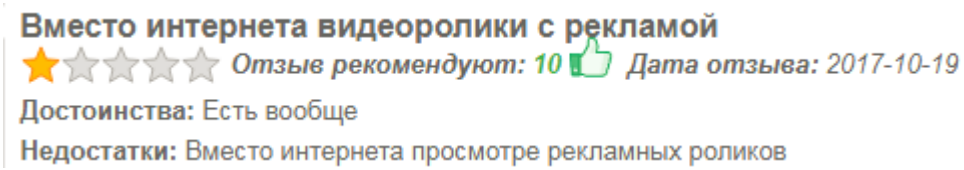


Рис. 7. Отзыв о большом количестве рекламы

Список используемых источников

1. Где Wi-Fi лучше? [Электронный ресурс]. URL: https://www.hometogo.ru/media/internet/ (дата обращения 28.03.2018).
2. Бесплатный городской Wi-Fi заработал в трех районах Петербурга [Электронный ресурс]. URL: https://www.spbdnevnik.ru/news/2017-01-23/besplatny-gorodskoy-Wi-Fi-zarabotal-v-trekh-rayonakh-peterburga/ (дата обращения 28.03.2018).
3. Метро Петербурга не хочет запускать Wi-Fi из соображений безопасности [Электронный ресурс]. URL: https://www.dp.ru/a/2012/01/20/Metro_Peterburga_ne_hochet (дата обращения 26.03.2018).
4. Ekahau Wi-Fi Design Solutions [Электронный ресурс]. URL: https://www.ekahau.com/ (дата обращения 26.03.2018).
5. Бесплатный Wi-Fi в метрополитене Санкт-Петербурга [Электронный ресурс]. URL: http://otzovik.com/reviews/besplatniy_wi-fi_v_metropolitene_sankt-peterburga_russia_sankt-peterburg/ (дата обращения 26.03.2018).

УДК 004.942, 621.39

КОМПЬЮТЕРНОЕ МОДЕЛИРОВАНИЕ РАБОТЫ AWG МУЛЬТИПЛЕКСОРА ДЛИН ВОЛН

А. С. Дюбов, М. Ю. Мокрецова

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

Рассмотрена конструкция и принцип действия мультиплексора длин волн AWG. Мультиплексоры AWG строятся на основе дифракционной решетке, сформированной массивом волноводов. Мультиплексоры типа AWG получили широкое распространение в сетях плотного спектрального уплотнения DWDM. В статье рассмотрена программа для расчета и компьютерного моделирования работы мультиплексоров, построенных на технологиях AWG. Приводятся описание и функциональные возможности программы, приводятся результаты моделирования работы мультиплексора. Рассмотрена перспектива использования данного программного обеспечения в учебном процессе при изучении технологии спектрального мультиплексирования.

мультиплексор длин волн, плотное спектральное уплотнение, массив волноводов, волоконно-оптические системы связи, компьютерное моделирование.

Мультиплексоры и демультиплексоры длин волн служат для объединения и разделения спектральных каналов при организации связи в системах со спектральным уплотнением. В настоящее время разработано несколько методов для реализации мультиплексоров и демультиплексоров, однако при построении сетей DWDM (*dense wavelength-division multiplexing*) наибольшее распространение получили устройства на основе технологии

AWG (*Arrayed Waveguide Grating*). Одно и то же устройство может выполнять функции мультиплексирования и демультиплексирования длин волн в зависимости от схемы включения. На рис. 1. приведена схема конструкции мультиплексора/демультиплексора AWG. Конструкцию мультиплекса составляют: входной и выходные волноводы (порты ввода-вывода), две области свободного распространения (волновод-пластина), дифракционная структура, образованная массивом волноводов.

На рис. 1. показана работа устройства в режиме демультиплексирования на примере четырех длин волн. Входной сигнал, содержащий четыре длины волны, через входной волновод поступает в область свободного распространения и распределяется по массиву волноводов. Попадая во вторую область свободного распространения сигналы интерферируют и на плоскости, сопряженной с массивом выходных волноводов, формируются максимумы и минимумы интенсивности сигнала. Подбирая разность длин волноводов массива и геометрию областей свободного распространения можно добиться пространственного разделения максимумов разных длин волн, таким образом, разделяя сигналы по выходным волокнам. Аналогичным образом, но в противоположном направлении происходит мультиплексирование сигналов разных длин волн [1].

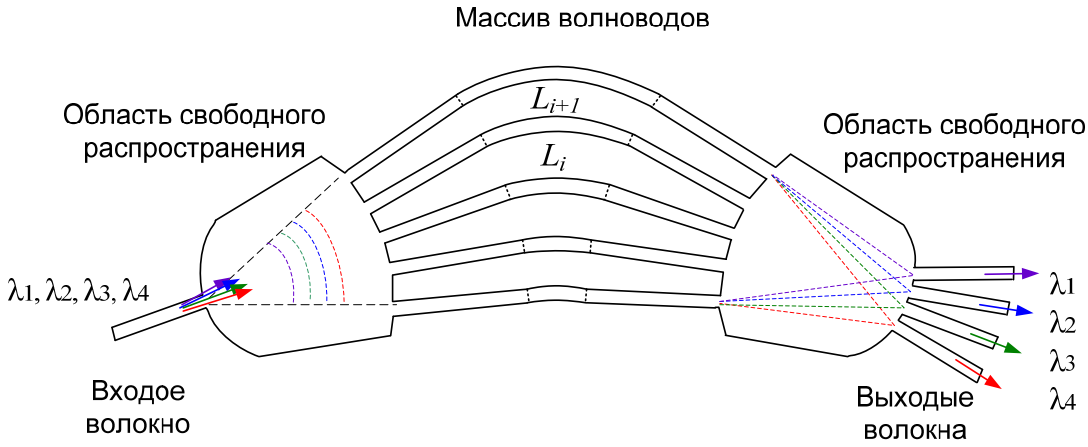


Рис. 1. Конструкция мультиплексора (демультиплексора) AWG

Мультиплексоры AWG выполняются по интегральной технологии, могут применяться для мультиплексирования и демультиплексирования нескольких десятков спектральных каналов, имеют хорошие характеристики по вносимым потерям, неравномерности и защищенности между каналами.

Сложность проектирования и анализа подобных устройств обусловлена множеством варьируемых параметров, таких как: число спектральных каналов, шаг между каналами, ширина спектрального канала. Дополнительно задачу усложняют требования к максимальному допустимому вно-

симому затуханию и уровню переходных помех, приемлемой поляризационной зависимостью. Возможно множество геометрических конфигураций массива волноводов и областей свободного распространения. Поэтому применение компьютерного моделирования для анализа и изучения работы устройств AWG кажется обоснованным и актуальным.

В данной работе рассматривается программное обеспечение WDM Phasar компании Optiwave. Программа WDM Phasar предназначена для расчета и моделирования работы оптических устройств, включающих решетки на массивах фазированных волноводов (*Phased Arrays* или PHASARs), таких как оптические мультиплексоры и демультиплексоры. Программа доступна для бесплатного скачивания с сайта разработчика, что можно считать серьезным преимуществом перед имеющимися аналогами [2].

В описании разработчика указано, что программа использует численные методы для анализа устройств AWG и оптимизации их параметров. Программа сопровождается описанием применяемых методов расчета, руководством пользователя с указаниями по работе с интерфейсом, уроками и примерами с демонстрацией основных возможностей программы и этапов моделирования [3].

Моделировать AWG мультиплексора на компьютере, начинается с задания его конструктивных параметров: геометрическая конфигурация волноводов и областей свободного распространения, расстояние между волноводами в массиве, число волноводов в массиве, фокусное расстояние, пространственно частотный фактор, дифракционный порядок и другие. Необходимо задать рабочие длины волн, ширину канального интервала, эффективные показатели преломления волновода и подложки, радиусы модовых полей входных и выходных волноводов.

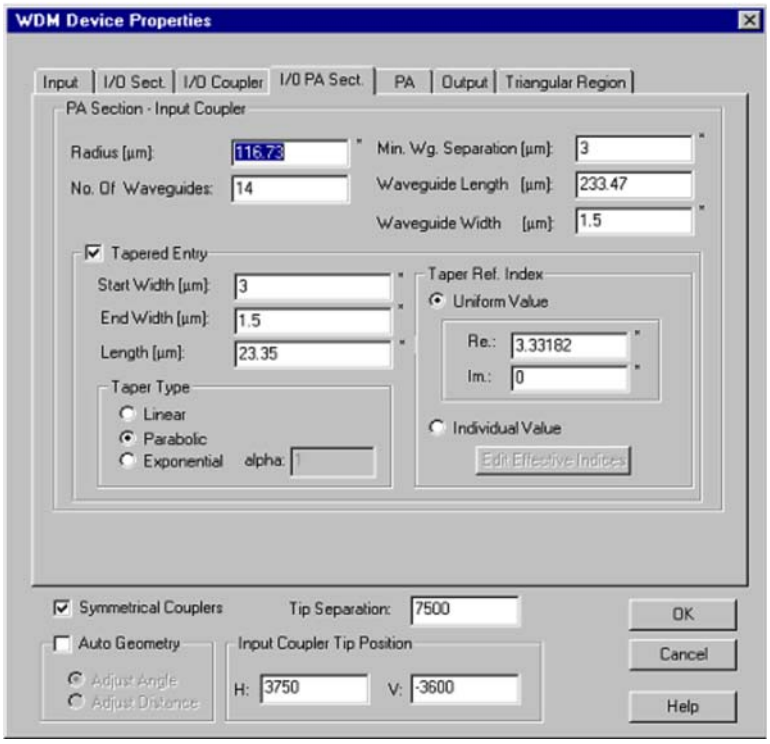


Рис. 2.Параметры WDM устройства

На рис. 2. приведена одна из вкладок «I/O PA Sect.» окна WDM Device Properties, в котором задаются настройки свойств устройства.

С использованием программы WDM Phasar демонстрируется, что изменением фазы и амплитуды в массиве волноводов можно направлять сигнал спектрального канала в определенный выходной волновод. На рис 3 приведены исходные значения фазы в массиве волноводов и график распределения оптического сигнала.

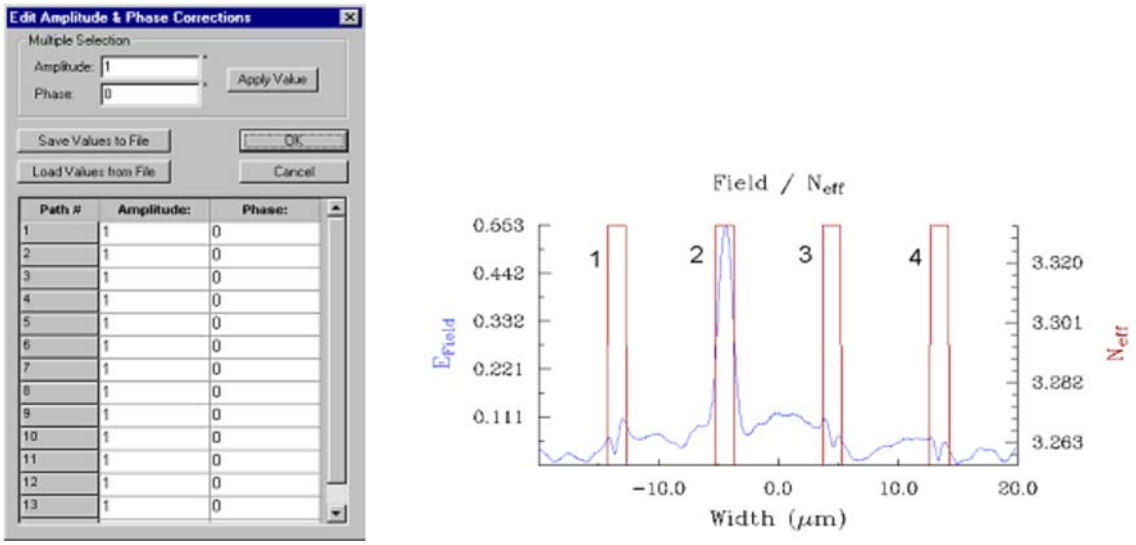


Рис.3. Исходные значения

При добавлении правильного опережения по фазе для каждого из 14 волноводов в фазированной решетке, мощность спектрального канала со входа может быть направлена со 2 в 4 выходной волновод. На рис. 4. приведены скорректированные значения фазы и результирующее изменение распределения оптического сигнала.

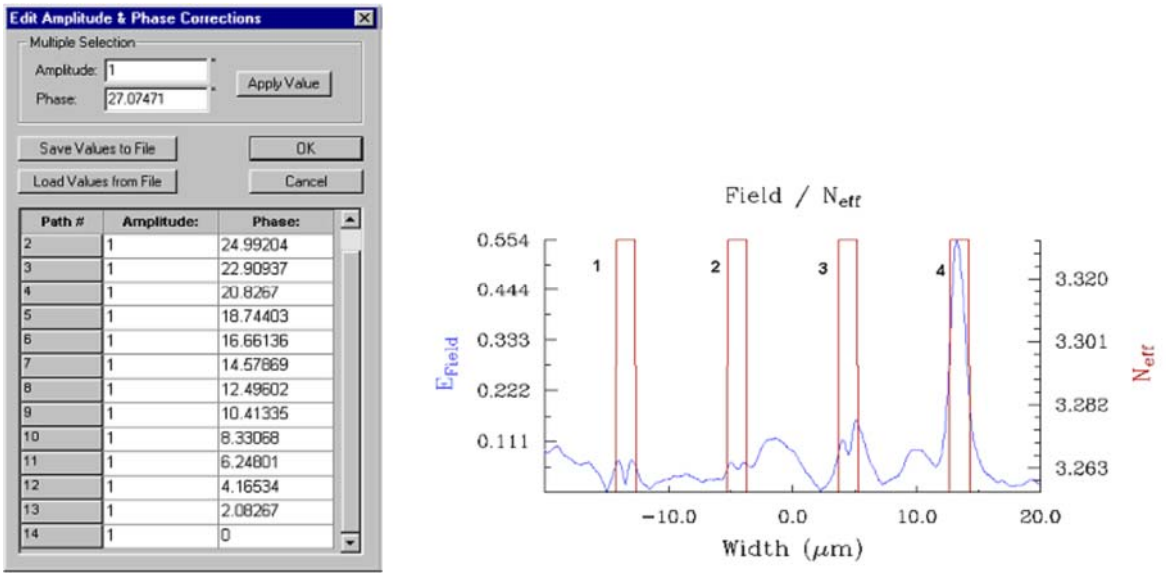


Рис.4. Скорректированные значения

Из сравнения рис. 3 и рис. 4 видно, что мощность перенаправлена из 4 канала в выходной канал 4. В документации разработчика приведены и другие примеры использования программы, например, трехмерные графики распределения энергии при ее распространении по устройству от входных до выходных волноводов [4].

Можно считать привлекательным применение программы WDM Phasar в демонстрационных и учебных целях при изучении работы мультиплексоров и демультиплексоров AWG.

Список используемых источников

1. Meint K. Smit, Cor van Dam. PHASAR-Based WDM-Devices: Principles, Design and Applications. // IEEE Journal of selected topics in quantum electronics, vol. 2, No. 2, June 1996.

2. WDM Phasar Freeware [Электронный ресурс] // Optiwave Systems Inc. URL: https://optiwave.com/resources/academia/wdm-phasar-download/ (дата обращения: 10.02.18).

3. WDM_Phasar User's Guide Phased Array WDM Device Design Software // Optiwave Systems Inc.

4. WDM Phasar Technical Background and Tutorials Phased Array WDM Device Design Software // Optiwave Systems Inc.

УДК 621.391

ПРИМЕНЕНИЕ СОЦИАЛЬНОГО ГРАФА ДЛЯ ПОСТОБРАБОТКИ ДАННЫХ ЗАКОННОГО ПЕРЕХВАТА

В. С. Елагин, А. А. Махура

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

В настоящее время в СОРМ существует проблема с визуализацией данных, поступающих с систем СОРМ, для их быстрого анализа конечным потребителем. В качестве одного из решения для анализа данных с систем законного перехвата может выступать социальный граф. Граф будет выступать в роли объекта программирования указывающего связи объектов в файле через ребра, а для простоты отображения и анализа, каждый объект в зависимости от идентификатора будет иметь отличительные свойства: форма, цвет, размер. Помимо самого графа будут использоваться и стандартные формы отчетов, такие как excel таблицы и возможность сохранять данные по графу через вкладку: File – Save all/Save IPDR object. В самом интерфейсе программы будет реализовано возможность ознакомиться с инструкцией по работе с данной программы через вкладку help – Instruction, которая откроется в виде web страницы в браузере по умолчанию.

граф, социальный граф, система СОРМ, СОРМ-2/3, IPDR, постобработка данных законного перехвата, метрика, ребра, вершины, матрица смежности, MATHLAB, biograph.

Сам социальный граф, в качестве примера, будет построен по данным полеченным с тестовой системы СОРМ-2/3. Сами данный представляют собой файл в виде IPDR – полей в закодированном виде, разделенных символами разделителями и имеющими свое определенное значение в зависимости от вида и названия файла, и местоположения в файле. В качестве решения будет использоваться программа, написанная на языке программирования MATHLAB. Основной функцией для построения самого графа, будет выступать встроенная функция biograph, которая в свою очередь базируется на матрице смежности из теории графов [1, 2].

Исходные данные для программы: социальный граф, который строится по данных с системы СОРМ-2/3. Граф будет строится по протоколу HTTP, в роли социальных объектов для данного графа будут выступать сайты и другие объекты с заданным IP адресом, посещающие сайты. Поиск будет осуществляться в сети с AAA архитектурой. Будет выводится логин объекта и связанный с ним в данный момент IP-адрес. Объект наблюдения и посещенные им сайты будут выделять графически, с помощью цвета [3].

Помимо идентификаторов, косвенно характеризующих конкретного абонента сети передачи данных, также в бушующем можно использовать привязку, скрывающегося в данный момент, IP-адреса и конкретного пользователя сети, через закрепленный за ни идентификатор, указанный в договоре между оператором и абонентом сети оператора [4].

Программа действует по следующему принципу: выбирается исходный файл с данными (IPDR), выбирается протокол, для которого будет строится граф, вводится один из идентификаторов для поиска по объекту наблюдения. (для HTTP IPDR идентификатор объекта будет IP-адрес объекта наблюдения.), строится граф по заданному IPDR файлу и объекту контроля. Ниже, на рис. 1 приведен графический интерфейс программы, а на рис. 2 сокращенный алгоритм работы программы.

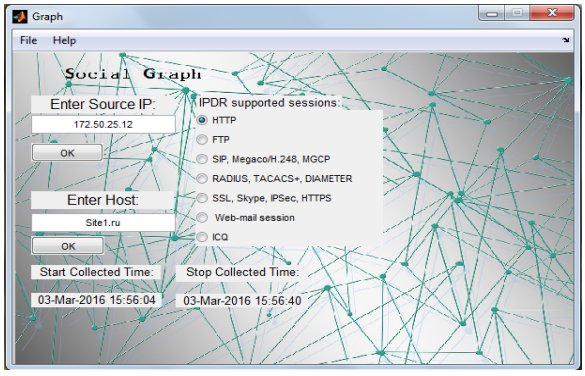


Рис. 1. Графический интерфейс программы

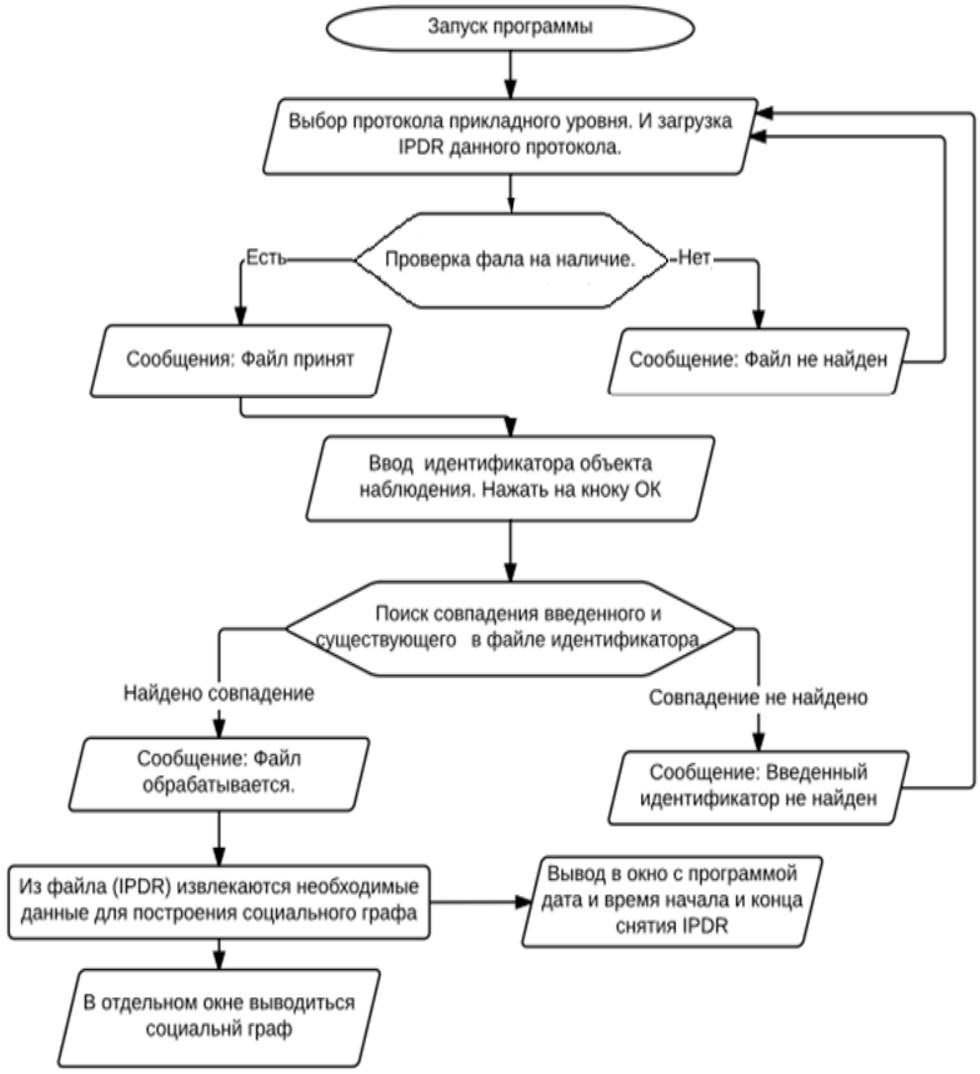


Рис. 2. Сокращенный пример алгоритма работы программы

Как ранее говорилось, социальный граф будет строится по встроенной в пакет прикладных программ MATHLAB функции biograph, которая базируется на матрице смежности. Стоит отметить, что построенный граф будет иметь ориентированные ребра. Для графа, построенного на HTTP IPDR матрица смежности будет иметь вид, приведенный на рис. 3.

Для данной матрице смежности основанная диагональ говорит о наличии у объекта петель, каждый столбец и строка указывает объект, который будет построен в графе. Количество столбцов и строк для матрицы смежности будет совпадать и указывает количество объектов, которые будут построены на графе. [5] Первый столбец – это введенный по идентификатору объект, со 2 по 5 идут адрес сайтов, которые посетил объект наблюдения, с 6 по 9 столбец идет взаимодействие объекта «напрямую» с другими IP-адресами, посетившими сайты, которые посетил объект наблюдения. Строки идут аналогичным образом, как и столбцы, разница заключалась

лишь в ориентации связей от кого к кому будут направлены ребра. На рис. 3 приведена матрица смежности для HTTP IPDR.

Рис. 3. Матрица смежности для HTTP IPDR.

В итоге получаем социальный граф по данным из HTTP IPDR, показанный на рис. 4. Как и говорились, граф ориентированный, т.е. показывает кто и куда заходил. Сам введенный объект контроля выделяется цветом, а также сами действия объекта контроля подсвечиваются цветом. Помимо этого, при наведении на любой из IP-адресов отображается логин, под которым заходил пользователь с данным IP. Заполняется данное поле, только при наличии в самой записи данных идентификаторов.

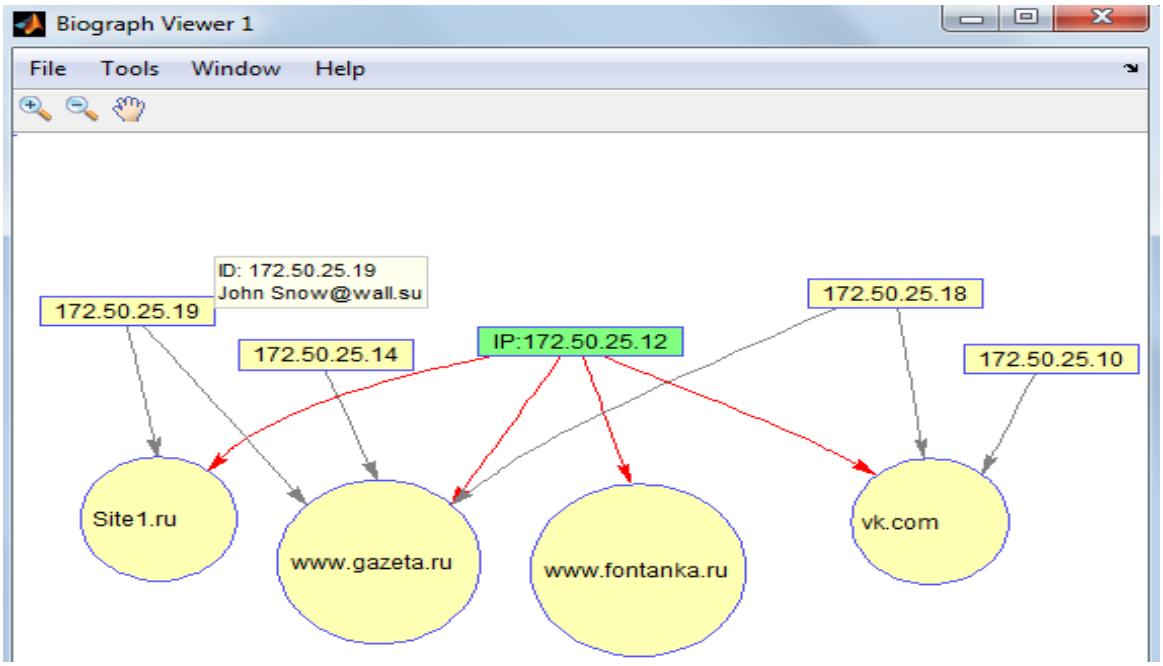


Рис. 4. Социальный граф для по HTTP IPDR

Также существует возможность передвигать объекты на самом рисунке как вам будет удобно в появившемся окне, сохранять файл в виде картинки и заходить в сами элементы социального графа, в них также можно сохранять какие-либо данные: такие как метрика или какие-либо дополнительные сведения. Все элементы являются объектами объектно- ориентированного программирования и обладают всеми свойствами, которые включены в функцию biograph: форма, цвет, толщина линий, действия при наведении на объект и прочее. Все это является примером встроенного функционала в функцию biograph пакета прикладных программ MATHLAB.

Помимо социального графа программа имеет стандартные средства диагностики данных из системы СОРМ-2/3, такие как отчеты в виде excel таблиц.

Социальный граф является одним из наиболее подходящих вариантов по сравнению с обычными средствами для отображения данных из систем СОРМ из-за огромного количества данных поступающих в системы СОРМ. Граф крайне удобен с точки зрения визуализации данных и упрощенной формы для их дальнейшего анализа. В программе, помимо графа, были реализованы стандартные способы представления данных в виде таблиц. Данная программа частично дублирует функционал ПУ и является программным дополнением к комплексу СОРМ. Программа ориентирована на помощь правоохранительным органам для проведения оперативно-розыскных мероприятий

Список используемых источников

1. Гольдштейн Б. С., Крюков Ю. С., Пинчук А. В., Хегай И. П., Шляпоберский В. Э. Интерфейсы СОРМ // Справочник по телекоммуникационным протоколам. СПб. : БХВ-Петербург, 2006. 160 с.

2. Гольдштейн Б. С., Крюков Ю. А., Полянцев В. И. Проблемы решения СОРМ-2 // Вестник связи. 2006. № 12.

3. Елагин В. С. Особенности развития и развертывания комплекса мероприятий законного перехвата СОРМ-2 // 61-я научно-техническая конференция профессорско-преподавательского состава, научных сотрудников и аспирантов СПбГУТ им. проф. М. А. Бонч-Бруевича: материалы, СПбГУТ. СПб., 2009. С. 20.

4. Гольдштейн Б. С., Крюков Ю. А., Хегай И. П. Инженерные аспекты СОРМ // Вестник связи. 2005. № 9.; Калигин А. С. СОРМ в кубе // СТАНДАРТ. Октябрь 2014. Специальный выпуск № 10.

5. Кристофидес Н. Теория графов. Алгоритмический подход. М. : Мир, 1978. 432 с.

УДК 004.72 (004.77)

ЭФФЕКТИВНОСТЬ DPI СИСТЕМЫ ДЛЯ ОПРЕДЕЛЕНИЯ ТРАФИКА И ОБЕСПЕЧЕНИЯ КАЧЕСТВА OTT-СЕРВИСОВ

В. С. Елагин, А. В. Онуфриенко

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

В статье авторы вводят определение термина OTT-сервиса, сравнивают его с традиционными услугами. Авторы идентифицируют проблемы, связанные с передачей данных через сети операторов связи. Для обеспечения необходимого качества обслуживания предлагается использовать DPI-технологию. В этой статье получены графики результатов эксперимента и оценили эффективность сигнатур, вывели формулы для оценки вероятности событий и применили их к соответствующему статистическому анализу.

Over The Top, OTT-service, DPI, Deep Packet Inspection, QoS, quality of service.

Телекоммуникационные услуги можно разделить на традиционные и на предоставляемые OTT-сервисами услуги. Провайдер имеет частичный контроль над контролируемыми услугами, такие услуги тесно связаны с базовой сетью.

OTT (OVER THE TOP) – это метод предоставления контента через Интернет для широкого круга пользователей через сети передачи данных без участия оператора в управлении и распространении контента. Таким образом, интернет-провайдер не несет ответственности за содержимое пакетов и не обязан гарантировать высококачественную доставку [1].

OTT-сервисы представляют зрителю значительный выбор, личный подбор услуг и позволяет получить доступ во всем мире и в любое время с подключением к Интернету.

Поскольку Интернет является неконтролируемой сетью, где пропускная способность не может контролироваться на всем пути передачи информации, предполагается, что пользователи справедливо разделяют доступные сетевые ресурсы. Когда появляется нехватка ресурсов, невозможно обеспечить необходимое качество для приложений реального времени [2].

В результате ухудшения потока приложение начинает обеспечивать низкое качество, что отрицательно сказывается на впечатлении пользователя о приложении.

Широкое использование служб OTT в настоящее время значительно изменяет параметры сети и устанавливает новые требования к работе оператора связи. В этой ситуации оператор может предложить настройку приоритетов трафика, что, в свою очередь, должно обеспечить максимальную гибкость для реализации услуг.

Чтобы у оператора была возможность идентифицировать OTT-сервисы, применять к ним уникальные надстройки и дальнейшей корректировки полосы пропускания и других сетевых характеристик, предлагаем рассмотреть использование DPI-системы в сети оператора связи.

Перспективно рассмотреть технологические особенности DPI-систем, по обеспечению QoS на сети провайдера для выделенныхOTT-сервисов.

Deep Packet Inspection (DPI) — совокупное название технологий, позволяющей проводить накопление, анализ, классификацию, контроль и модификацию сетевых пакетов в зависимости от их содержимого в реальном времени при которых оборудование реагирует не только на заголовки пакетов разного уровня, но и на содержимое (рис. 1).

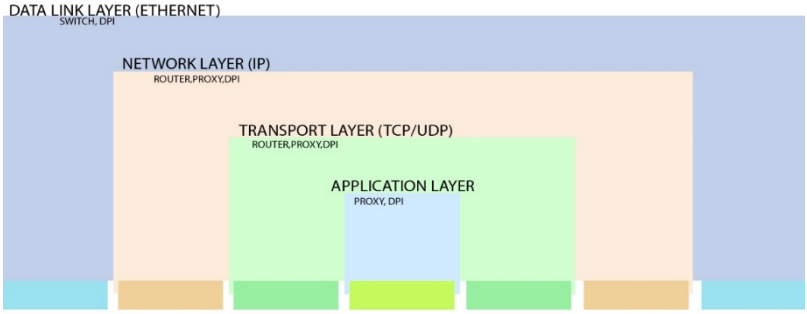


Рис. 1. Работа DPI на разных уровнях

При рассмотрении вопросов о качестве обслуживания трафика OTT-сервисов, необходимо чётко и однозначно дифференцировать различные типы OTT-сервисов. А также дать единое определение для разных типов OTT-сервисов и установить единообразное регулирование в указанной области с технической точки зрения [3].

Необходимо проверить достоверность идентификации OTT-сервисов существующими DPI-системами. Т. е. насколько точно мы можем распознавать разные приложения, используя эту систему.

Рассмотрим реакцию системы на три разных вида трафика трех различных OTT-сервиса (*Skype*, *KakaoTalk*, *Hangout*). Пример сигнатур, взятых для распознания трафика преобразованы в блок-схемы. В данной статье будут представлены результаты для сервиса Skype (рис. 2).

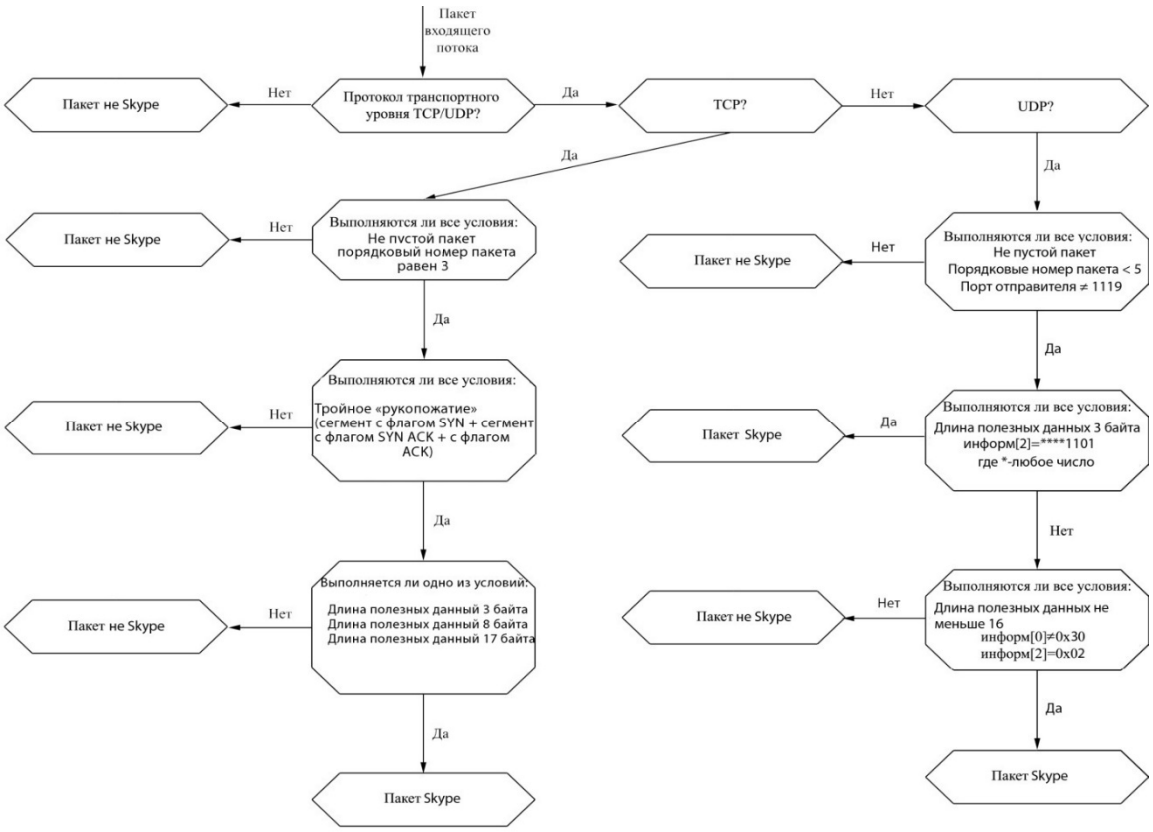


Рис. 2. Блок-схема для сигнатуры Skype

Проверим достоверность данных сигнатуры в ходе эксперимента.

Для проведения эксперимента была использована распространенная система DPI с открытым исходным кодом для анализа трафика и для проверки правильности и целостности, написанной сигнатуры, а также корректности работы DPI-системы был использован сниффер «Wireshark».

Полученные в ходе эксперимента результаты сведем в графики и проведем анализ работоспособности сигнатур (рис. 3).

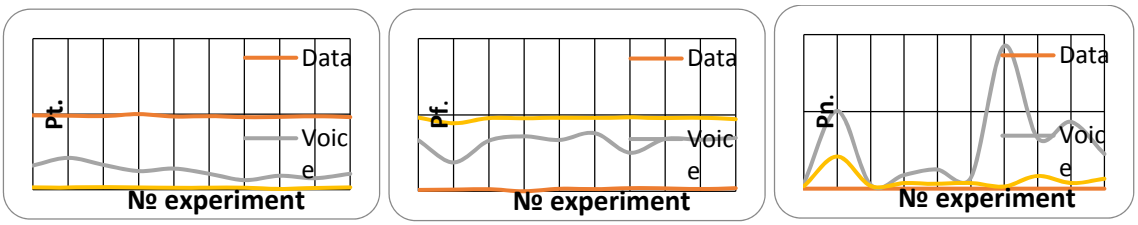


Рис. 3. Графики, отражающие вероятность срабатывания, несрабатывания, ложного срабатывания системы в результате эксперимента

Так как эксперимент неоднородный дальнейшие расчеты производились на основании основных понятий и определений теории вероятности с помощью следующих формул:

$$P_t = \begin{cases} \dfrac{DPI}{S}, если DPI \le S \\ \dfrac{S - |S - DPI|}{S}, если DPI \ge S \end{cases}, \quad (1)$$

$$P_f = \begin{cases} \dfrac{\sum_{i=0}^{k} \overline{DPI}\, i}{S}, если DPI \le S \\ \dfrac{S - \left|S - \overline{DPI}\right|}{S}, если DPI \ge S \end{cases}, \quad (2)$$

$$\mathrm{P}_n = \frac{S - \sum_{i=0}^{k} \overline{DPI} i - \sum_{i=0}^{k} DPIi + \sum_{i=0}^{k} \widetilde{\overline{DPI}}\, i}{S}, \quad (3)$$

где P_t – вероятность верного срабатывания системы – вероятность того, что трафик точно определен статистическим критерием (1); P_f – вероятность ложного срабатывания – вероятность того, что трафик неверно отвергнут статистическим критерием или что за исходный трафик принят ложный трафик (2); P_n – вероятность несрабатывания – вероятность того, что система не распознает, что в данном сеансе связи было использовано интересующее нас приложение (3); $\widetilde{\overline{DPI}}_i$ – объем трафика нераспознанного DPI-системой; $\overline{DPI}_i$ – объем трафика неверно распознанного DPI-системой; DPI_i – объем трафика верно распознанного DPI-системой; S – эталонный, переданный приложением трафик.

Полученные в ходе обработки данные были подвержены статистическому анализу (табл.).

ТАБЛИЦА. Рассчитанные значения для вероятности верного срабатывания

Приложение	Тип трафика	Средние значения	Дисперсия	Размах вариации	Относительное отклонение по модулю	Коэффициент вариации
Skype	Данные	0,9731	0,0002	0,0402	0,0092	0,0126
	Голос	0,2564	0,0096	0,3230	0,2769	0,3826
	Видео	0,0282	0,0000	0,0128	0,1776	0,1351

Приведенные расчеты отражают, что для вероятности верного срабатывания разброс средних значений для разных видов трафика крайне велик, что может говорить об отсутствии положительной системности в работе DPI-системы при распознавании различных видов трафика и приложений. Дисперсия показывает, что для одинаково вида трафика в пределах одного приложения приблизительно одинаковый результат обнаружения. Размах вариации, среднее линейного отклонение для разных видов трафика одного приложения различается из-за колебания значений в разных экспериментах. Коэффициент вариации позволяет судить об однородности совокупности для данных и видео, а для речи –недостаточной однородности.

Стоит отметить, что при одной и той же сигнатуре разные виды трафика имеют разную степень детектирования, что указывает на непроработанность сигнатур и невозможность использования одной сигнатуры для разных типов трафика в рамках одного приложения.

Предварительные итоги:

1) При анализе сигнатур разных OTT-сервисов можно заметить, что у Skype, как уже давно распространяемого, устоявшегося приложения сигнатура разработана гораздо лучше, чем у новых приложений, что негативно сказывается на применении DPI-системы для введения определенных политик для конкретного вида трафика.

2) Исследования показали, что для приложений со слабо разработанными сигнатурами использовать DPI для идентификации трафика OTT-сервисов нельзя, так как происходят несрабатывания и ложные срабатывания из-за близости или некорректности сигнатур.

Вариантами решения этих проблем могут стать следующие подходы:

1) Использование комбинированных методов для повышения распознаваемости трафика.

2) Дополнительная проработка сигнатур.

3) Четкая маркировка сервисов (со стороны производителя OTT-сервиса). Необходимо обеспечение взаимодействия не на уровне соглашения оператора связи и OTT-сервисов на идентификацию трафика в общем потоке с помощью маркировки трафика потребует от оператора связи большой объем надстроек на каждом пограничном узле, что легко решается в SDN, т.к. на контроллер можно указать правила.

Воздействие на сеть при помощи DPI-системы не ухудшает качество другим пользователям, однако выделяя «удобный» маршрут для транспортировки пакетов, можно гарантировать качество определенным пользователям на заданные виды сервисов, что не нарушает принцип сетевой нейтральности, принятый в Российской Федерации.

Список используемых источников

1. Godlovitch I., Kotterink B. and Markus D. Over-the-Top players (OTTs) // European Parliament's Committee. 2015. PP. 20–42.

2. Миранчиндани П. SDN/NFV – Is it the breakthrough CSPs need to help level the OTT playing field? // URL: http://www.oneaccess-net.com/easyblog/entry/sdn-nfv-is-it-the-breakthrough-csps-need-to-help-level-the-ott-playing-field (дата обращения: 17.11.2017).

3. Елагин В. С., Онуфриенко А. В. Как оператору заработать на OTT-сервисах и при чем тут SDN? // T-COMM: Телекоммуникации и транспорт. 2017. N 1. 2017. С. 17–21.

УДК 004.72

АНАЛИЗ ПРИМЕНЕНИЯ СИСТЕМЫ ENUM ПРИ РЕАЛИЗАЦИИ УСЛУГИ VOLTE

В. С. Елагин, П. А. Фрик

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

В статье рассмотрен пример сценария установления соединения VoLTE, а также вариант применения системы ENUM в данном сценарии.

ENUM, VoLTE, LTE, IMS.

Установление соединения VoLTE

Рассмотрим сценарий установления соединения между двумя абонентами, использующими услугу VoLTE и находящимися в одной сети (рис. 1).

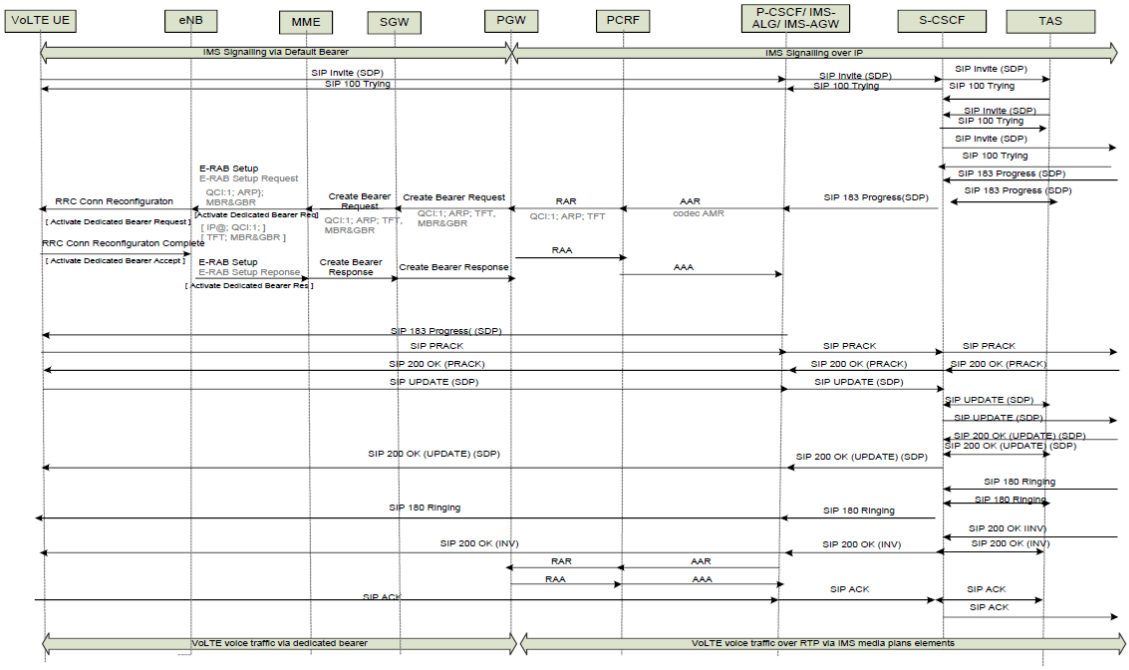


Рис. 1. Соединение между двумя абонентами с услугой VoLTE

Как видно из сценария, для установления соединения между абонентами используются сообщения протокола SIP, а также функциональные элементы IMS. Рассмотрим описание представленного выше сценария.

UE отправляет запрос SIP INVITE, содержащий SDP предложение сеанса. SDP предложение должно содержать узкополосный и рекомендуемый

широкополосный AMR кодеки, а также указывает требуемые условия QoS. Запрос отправляется в P-CSCF, который был обнаружен во время процедуры регистрации, и далее направляется к S-CSCF. S-CSCF принимает SIP INVITE, и вызывает те VoLTE услуги, которые были обнаружены внутри профиля абонента, полученного во время регистрации в IMS. После идентификации вызова как VoLTE, S-CSCF должен маршрутизировать SIP INVITE к TAS для вызова дополнительных услуг. TAS вызывает службу дополнительных услуг и возвращает SIP INVITE к S-CSCF. S-CSCF определяет, что вызываемая сторона находится в пределах домашней сети и направляет SIP INVITE к I-CSCF, чтобы определить завершающего S-CSCF от вызываемой стороны.

UE вызываемого абонента возвращает сообщение SIP 183 Progress, содержащее SDP ответ, который должен содержать только один кодек. Это сообщение получает S-CSCF, и направляется в P-CSCF. P-CSCF анализирует SDP ответ и посылает сообщение Authorize/Authenticate-Request к PCRF с информацией о связанной с ними услуге (IP-адрес, номера портов, информация медиа-типа). PCRF разрешает запрос и сопоставляет информацию об услуге с хранимой у себя. Далее на сетевых элементах LTE происходит выделение радиоресурсов для организации VoLTE соединения.

P-CSCF передает ответ SIP 183 Progress в UE. UE резервирует внутренние ресурсы и подтверждает это резервирование путем отправления сообщения SIP UPDATE с новым SDP предложением. Данное предложение содержит выбранный кодек и указывает, что на исходящей стороне был создан выделенный канал и что мультимедийный поток в настоящее время устанавливается в активное состояние. Сообщение UPDATE пересылается через P-CSCF и S-CSCF, к вызываемой стороне вызова.

После получения и обработки сообщения UPDATE вызываемая сторона отправляет ответ 200 OK UPDATE, в SDP ответе которого содержится единственный голосовой кодек и подтверждение, что предварительные условия также получены и что мультимедийный поток активен. Это сообщение пересылается на вызывающий UE через S-CSCF и P-CSCF.

Когда предварительные условия были выполнены, вызываемое UE зазвонило, вызывающей стороне отправляется ответ SIP 180 Ringing. При ответе вызываемой стороной на вызов вызывающей стороне посылается ответ 200 OK. Его получает S-CSCF и направляется в P-CSCF. P-CSCF вызывает PCRF, чтобы включить восходящую и нисходящую линии выделенного канала передачи. В свою очередь PCRF вызывает P-GW для того, чтобы медиа поток направлялся в P-GW.

P-CSCF передает SIP 200 OK INVITE к вызывающей UE. UE принимает 200 OK, и посылает сообщение SIP ACK, чтобы подтвердить, что вызов был установлен.

На данном этапе мы имеем установленное VoLTE соединение с передачей голосового трафика по RTP, передаваемого по выделенному каналу. Сигнальный трафик передается по каналу, выделенному по умолчанию [1].

В описанном выше сценарии абоненты знают публичный идентификаторы друг друга и находятся в одной сети, однако если их не знать, необходимо прибегнуть к помощи системы ENUM. Рассмотрим далее ее подробней.

Система ENUM

Работа IETF имела цель создать архитектуру и протоколы, которые бы основывались на системе DNS необходимые для соответствия телефонного номера и ресурсами, предназначенными для осуществления вызова обладателя данного номера. Первоначально протокол ENUM (*tElephone NUmber Mapping*) был описан в документе RFC 2916, затем дополнен и исправлен в RFC 3761. Основу протокола составляет простой алгоритм, согласно которому телефонный номер преобразуется в адрес DNS-домена, называемого «универсальный идентификатор ресурса» (*Unified Resource Identifier*, URI). Данный номер DNS-сервер интерпретирует как адрес уникального ENUM-домена.

Преобразование может быть сведено к следующему: из записи телефонного номера выкидываются все ненужные символы (скобки, пробелы, дефисы, начальный символ «+»), сам номер записывается справа налево, затем все соседствующие цифры разделяются точками, а справа к результату добавляется «.e164.arpa». Например, телефон +7(812)123-4567 будет преобразован в уникальный ENUM-домен 7.6.5.4.3.2.1.2.1.8.7.e164.arpa [2].

Информация об адресах, сопоставленных с ENUM-номером, хранится на DNS-серверах. Каждому URI ставятся в соответствие несколько записей NAPTR (*Naming Authority Pointer Resource Records)* с указателями на конкретные коммуникационные сервисы и соответствующие им идентификаторы абонента, по одной записи на каждый сервис.

При вызове абонента системы ENUM набранный телефонный номер преобразуется ENUM-шлюзом в URI. Последний используется для поиска и извлечения содержимого записей NAPTR. Затем в соответствии с предпочтениями, определенными вызываемой стороной, вызов маршрутизируется к соответствующему сервису либо завершается.

Ниже приведен пример записи NAPTR, в котором указывается, что доступными протоколами являются либо SIP, либо SMTP-почта [3].

```
$ ORIGIN 2.1.2.1.5.5.5.0.7.7.1.e164.arpa.
    ;;          order pref flags   service          regexp     replacement
IN NAPTR 100 10 "u" "sip + E2U" "! ^. * $! Sip: information@tele2.se!" .
IN NAPTR 102 10 "u" "mailto + E2U" "! ^. * $! Mailto: information@tele2.se!" .
```

Применение ENUM в VoLTE

Услуга VoLTE обеспечивается платформой IMS, которая использует в качестве сигнального протокола SIP. Как известно, SIP-адрес состоит из двух частей. Первая часть адреса – это имя пользователя, зарегистрированного в домене сети или на рабочей станции. Во второй части адреса указывается имя домена сети, хоста или шлюза. Для определения IP-адреса устройства необходимо обратиться к службе доменовых имен DNS (*Domain Name Service*). Если же во второй части SIP-адреса размещается IP-адрес, то с рабочей станцией можно связаться непосредственно [4]. Таким образом DNS позволяет связать IP-адрес с целевым URI для поиска во время процесса маршрутизации.

При наборе номера E.164 необходимо представить его в маршрутизируемый адрес конечного пункта назначения, исправленный для переноса номера. GSMA и IETF рекомендуют перевод номера E.164 в SIP URI и исправление для переноса номеров осуществляется через стандартизированную технологию поиска номера ENUM.

Для получения имени домена конечной сети используется поиск ENUM в исходной сети из S-CSCF. Как известно, одной из основных функций S-CSCF является маршрутизация SIP-сообщений. Если пользователь набирает телефонный номер вместо SIP URI, то S-CSCF производит преобразование номера формата E.164 в соответствии с RFC3761 [5].

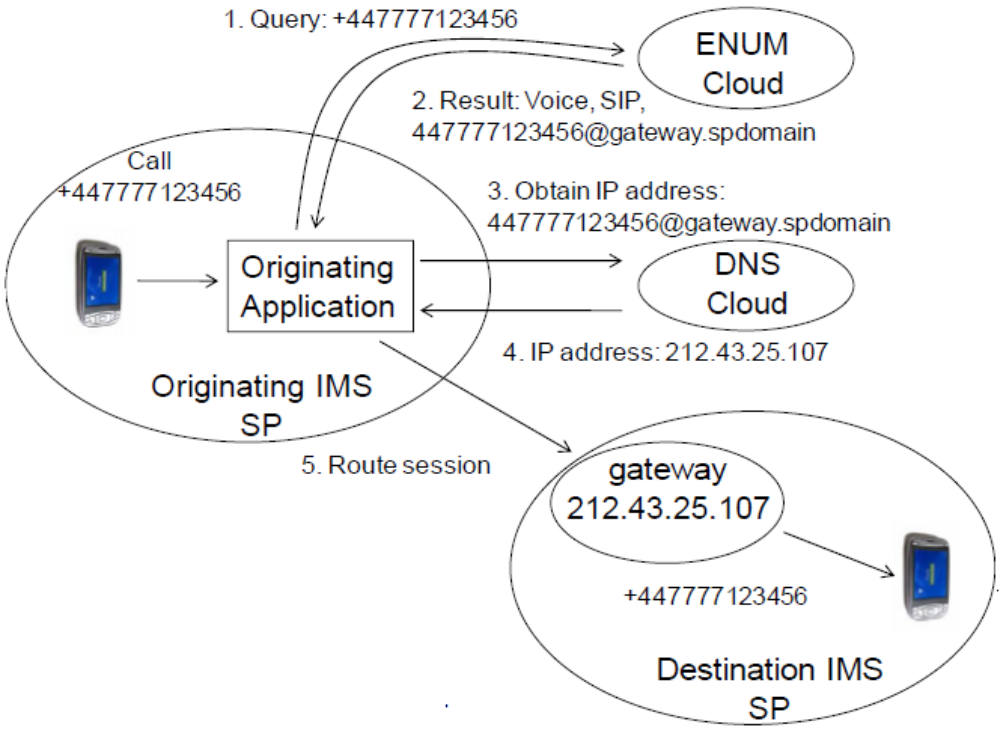


Рис. 2. Маршрутизация на основе ENUM

На рис. 2 выше показан пример того, как ENUM используется во время установления сессии между абонентами. В этом общем примере база данных ENUM показана, как облако, так как есть возможности для хранения и управления данными ENUM. Исходящий абонент устанавливает сеанс в направлении стороны назначения. Исходящая инфраструктура определяет номер, прежде чем принимать решение о маршрутизации путем доступа к базе данных ENUM. База данных ENUM возвращает URI, связанный с адресатом. Исходящая инфраструктура сопоставляет URI назначения в IP-адрес через DNS. Маршрутизация производится исходя из IP-адреса назначения [1].

На основании описанного выше возможный сценарий определения IP адреса из номера E.164 будет выглядеть как показано на рис. 3.

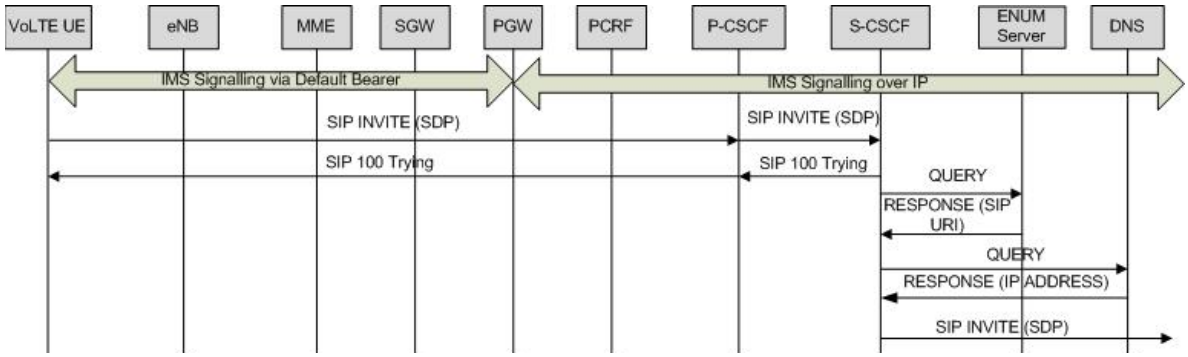


Рис. 3. Сценарий определения IP адреса на основе номера E.164

В заключении необходимо отметить, что применение ENUM становится важной задачей при реализации услуги VoLTE. Процесс реализации давно описан в различных документах, но необходимо учитывать специфику сети LTE для использования данной системы. Также еще остается ряд вопросов, требующих исследований: задержки при организации вызова с использованием ENUM, увеличение трафика в сети, требования к оборудованию и т. д.

Список используемых источников

1. GSMA N2020.01, VoLTE Service Description and Implementation Guidelines. 2014.
2. Червяков О., Керженцев Ю. Реализация конвергентной услуги «Единый номер» на основе технологии ENUM // Connect. 2011. № 5. С. 70–73.
3. Faltstrom P. RFC 2916 E.164 number and DNS. 2000.
4. Гольдштейн А. Б., Гольдштейн Б. С. SOFTSWITCH. СПб. : БХВ-Петербург, 2006. 368 с.: ил.
5. Гольдштейн Б. С., Кучерявый А. Е. Сети связи пост-NGN. СПб. : БХВ-Петербург, 2014. 160 с.: ил.

УДК 004.056.55

АНАЛИЗ ПРОИЗВОДИТЕЛЬНОСТИ РЕАЛИЗАЦИИ АЛГОРИТМОВ ШИФРОВАНИЯ В СЕТЯХ LTE

М. И. Ермолаев, И. А. Ушаков

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

В ходе работы приведены результаты реализации алгоритмов шифрования в сетях LTE: KASUMI, 128-EEA1 (на базе SNOW 3G), 128-EEA2 (на базе AES), 128-EEA3 (на базе ZUC). Все алгоритмы реализованы на языке программирования Python.

Кроме того, приведен анализ производительности этих алгоритмов (затрачиваемое время в секундах для шифрования различных блоков данных) на разных процессорах (Core i7-3610QM с тактовой частотой 3,3 ГГц, Core i5-3230M / 2,6 ГГц и Core i3-2350M / 2,3 ГГц). Даны рекомендации по использованию алгоритмов для шифрования данных в сетях LTE.

LTE, KASUMI, SNOW 3G, AES, ZUC, шифрование.

В век развития информационных технологий мобильный широкополосный доступ получает все большее распространение, поскольку необходимость в нем уже давно переросла рамки офисов или домашнего пользования. На сегодняшний день можно с легкостью смотреть онлайн-трансляции на мобильных устройствах, проводить видеоконференции, передавать значительные объемы информации, находясь при этом практически в любой точке земного шара. Технология в области беспроводной передачи данных – LTE (*Long Term Evolution*) – позволяет сделать это с минимальной задержкой.

Не стоит забывать и о безопасности информации в LTE. Чем больше данных мы передаем, тем больший по объему перехват может совершить злоумышленник и тем больший вред он способен нанести. Чтобы избежать данной проблемы, необходимо зашифровать информацию, причем сделать это с максимально возможной криптоустойчивостью и наименьшими временными затратами на данный процесс [1, 2].

Для LTE основными алгоритмами шифрования являются:

– KASUMI [3];
– 128-EEA1 (на базе алгоритма Snow 3G) [4];
– 128-EEA2 (на базе алгоритма AES);
– 128-EEA3 (на базе алгоритма ZUC) [5].

Далее были рассмотрены показатели для алгоритмов шифрования, а именно:

– скорость шифрования алгоритмов – в результате проведения теста выявлено, сколько времени необходимо для шифрования разных по величине файлов каждым из предложенных алгоритмов;

– шифрование алгоритмов на разных системах – была проведена проверка зависимости скорости шифрования определенным алгоритмом от вычислительных систем (проверены разные поколения процессоров при идентичных остальных условиях в тестовом стенде).

Для того чтобы проанализировать скорость шифрования алгоритмов в сетях LTE, были выбраны файлы фиксированной длины от 512 до 16384 Кб, которые были подвержены шифрованию каждым из способов. Все алгоритмы были реализованы на языке программирования Python и сведены в общую программу.

Чтобы не вводить каждый раз строку весом в 16 Мб, был придуман упрощенный способ. Для данной проверки была взята строка *“e6705355d3b6a8a14e769c18c903fd2c0fa2c5471d3b8b7114a6f79f9e56ccc1”* весом 64 байта, и она умножалась на определенное число *N*, что приводило к повторению данной строки N раз, и, как следствие, размер файла доводился до определенного значения.

Ниже в таблице 1 представлены константы N, на которые умножалась строка и полученный вес файла.

ТАБЛИЦА 1. Получение необходимого размера файла для шифрования

N	Вес файла (Кб)
8192	512
16384	1024 = 1 Мб
32768	2048 = 2 Мб
65536	4096 = 4 Мб
131072	8192 = 8 Мб
262144	16384 = 16 Мб

При шифровании алгоритмами KASUMI и 128-EEA1 на больших (8, 16 Мб) файлах требовалось некоторое ожидание для получения результата. Это объясняется тем, что алгоритм имеет потоковую структуру и основан на регистре сдвига с линейной обратной связью – в результате этого тратит большое количество вычислительных ресурсов, поскольку программная реализация потоковых алгоритмов, работающих на регистре сдвига с линейной обратной связью крайне неэффективна: приходится избегать разреженных многочленов обратной связи, так как они приводят к облегчению

взлома корреляционным вскрытием, а плотные многочлены очень медленно просчитываются. Поэтому программная реализация таких алгоритмов работает медленнее, чем реализация AES/DES (*Rijendal*, 128-EEA2/3) [6].

Результаты, полученные в результате теста для 4 алгоритмов на процессоре Core i7-3610QM, приведены далее в таблице 2.

ТАБЛИЦА 2. Время, затраченное на шифрование на стенде с Core i7-3610QM для разных алгоритмов

Вес файла (Кб)	KASUMI	128-EEA1	128-EEA2	128-EEA3
512	0,392	0,382	0,0001	0,002
1024	0,765	0,764	0,0001	0,004
2048	1,550	1,569	0,001	0,007
4096	3,094	2,988	0,002	0,012
8192	6,313	6,219	0,003	0,020
16384	12,963	12,033	0,008	0,030

Следующим пунктом анализа алгоритмов шифрования была проверка их выполнения на разных системах. Производилось сравнение по времени шифрования файлов (размеры файлов представлены в табл. 1) для разных вычислительных систем.

В данном тесте вычисления производились при следующих процессорах в тестовом стенде:

— Core i5-3230M с тактовой частотой 2,6 ГГц.

— Core i3-2350M с тактовой частотой 2,3 ГГц.

Ниже приведены полученные результаты шифрования (табл. 3 и 4).

ТАБЛИЦА 3. Время, затраченное на шифрование на стенде с Core i5-3230M для разных алгоритмов

Вес файла (Кб)	KASUMI	128-EEA1	128-EEA2	128-EEA3
512	0,654	0,661	0,0001	0,003
1024	1,323	1,333	0,0001	0,006
2048	2,649	2,625	0,001	0,008
4096	5,316	5,223	0,002	0,012
8192	10,503	8,145	0,005	0,022
16384	21,499	13,049	0,010	0,031

ТАБЛИЦА 4. Время, затраченное на шифрование на стенде с Core i3-2350M для разных алгоритмов

Вес файла (Кб)	KASUMI	128-EEA1	128-EEA2	128-EEA3
512	0,657	0,666	0,001	0,003
1024	1,328	1,362	0,003	0,007
2048	2,683	2,665	0,004	0,009
4096	5,473	5,305	0,007	0,015
8192	10,601	10,694	0,009	0,037
16384	21,772	20,955	0,017	0,066

В результате проведенной работы получены следующие результаты:

1. Подтверждена прямая пропорциональная зависимость времени, затраченного на шифрование, от мощности процессора.

2. Core i7 и Core i5 демонстрируют в 3-х алгоритмах шифрования из 4-х практически одинаковые результаты (исключение – KASUMI).

3. Core i3 уступает по скорости шифрования во всех алгоритмах примерно в 1,5–2 раза.

Как следствие, если алгоритмом шифрования при передаче данных будет являться любой EEA алгоритм, то нет разницы между i5 и i7, а значит, можно использовать оба при реализации шифрования. Однако не рекомендуется производить шифрование на процессорах i3 ввиду слабых показателей (по скорости) на данном устройстве.

Список используемых источников

1. Киррилов Д. И., Красов А. В., Долгорук Ю. Г., Селиванов А. Е., Ушаков И. А. Основы информационной безопасности сетей и систем: учебное пособие. Часть 1. СПб.: СПбГУТ, 2012. 64 с.

2. Киррилов Д. И., Красов А. В., Долгорук Ю. Г., Селиванов А. Е., Ушаков И. А. Основы информационной безопасности сетей и систем: учебное пособие. Часть 2. СПб.: СПбГУТ, 2012. 64 с.

3. 3GPP TS 35.201 V14.0.0. Specification of the 3GPP confidentiality and integrity algorithms; Document 1: f8 and f9 specification. 2017. 29 p.

4. 3GPP TS 35.216 V14.0.0. Specification of the 3GPP Confidentiality and Integrity Algorithms UEA2 & UIA2; Document 2: SNOW 3G specification. 2017. 7 p.

5. 3GPP TS 35.222 V14.0.0. Specification of the 3GPP Confidentiality and Integrity Algorithms EEA3 & EIA3; Document 2: ZUC specification. 2017. 7 p.

6. Панасенко С. П. Алгоритмы шифрования. Специальный справочник. СПб.: БХВ-Петербург, 2009. 576 с.

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

УДК 004.72

ОСНОВНЫЕ ВИДЫ УЯЗВИМОСТЕЙ В АРХИТЕКТУРЕ SDN

М. И. Ермолаев, И. А. Ушаков

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

Software-defined Networking (программно-определяемые сети) – актуальное решение в построении архитектуры компьютерных сетей на сегодняшний день. Одна из основных причин тому - возможность сделать сеть централизованно-программируемой, функции управления в которой перенесутся с коммутаторов и маршрутизаторов на программные приложения, реализованные на отдельном сервере – контроллере. Однако, такое решение, как и многие другие, имеет свои виды уязвимостей. Они и будут рассмотрены в статье.

SDN, программно-определяемые сети, архитектура SDN, уязвимость.

В современном мире управление сетью через конфигурацию отдельно взятых устройств стало не такой простой задачей. Возникла необходимость динамического перестроения устройств для эффективного управления сетью. Решить данный вопрос стало возможным при помощи технологии программно-определяемой сети (SDN).

SDN – динамичная, управляемая и адаптируемая сетевая архитектура, в которой разделены уровни управления сетью и передачи данных, что обеспечивает программное управление сетью и абстрагирование/изоляцию (уровня) сетевой инфраструктуры от (уровня) приложений и сетевых услуг/сервисов [1].

В отличие от традиционных сетей, программно-определяемая делает возможным отказ от уровня управления для оборудования и, в свою очередь, возлагает данные обязанности на контроллер. В результате, получаем следующую архитектурную модель (рис. 1, см. ниже) [2].

По функционалу SDN можно разбить на три следующие группы:

1. SDN приложения – приложения, у которых взаимодействие с SDN контроллером происходит напрямую. Необходимые ресурсы запрашиваются с помощью API (*application programming interface* – программный интерфейс приложения).

2. SDN контроллер – логический элемент, получающий запросы от SDN-приложений. В дальнейшем переводит их в запросы для сетевых устройств. Обратное взаимодействие включает сбор информации о сети и отправка её SDN приложениям.

3. Сетевые устройства – их роль заключается в перенаправлении данных согласно запросам SDN контроллера.

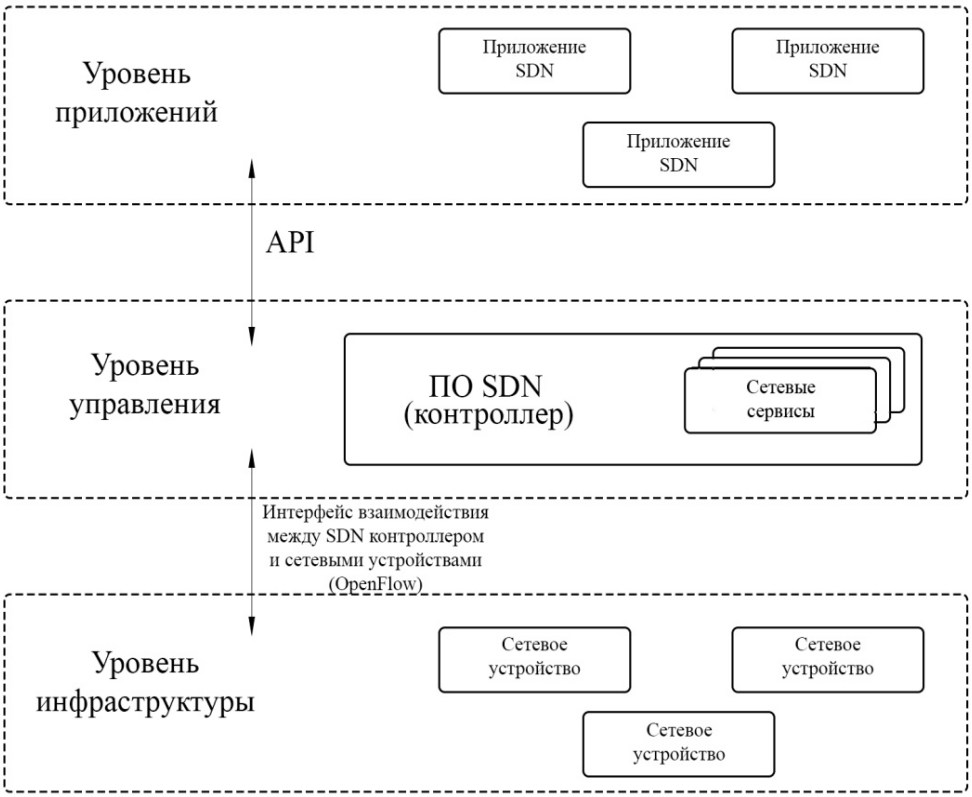


Рис. 1. Архитектура SDN

С возрастанием популярности данной технологии интерес со стороны злоумышленников также увеличился. Одним из способов компрометации данной системы является поиск уязвимостей непосредственно в архитектуре технологии. Вопросы авторизации и аутентификации в работе приложений с контроллером, разграничение доступа сетевых приложений – это, как минимум, основные пункты, на которые стоит обратить внимание при разработке и проектировании SDN-сетей.

Основными атаками, которым подвержены SDN, являются:

- отказ в обслуживании;
- компрометация коммутатора;
- атака на канал управления и контроллер [3, 4];
- искажение данных [5].

Рассмотрим из них подробнее те, что влияют на архитектуру сети, а именно отказ в обслуживании и атаку на контроллер.

Преимуществом технологии SDN и одновременно проблемным местом является централизованное управление сетью и маршрутизацией, за которые отвечает контроллер. Атака на него может повлечь критичные для всей

инфраструктуры последствия и в той или иной мере может нарушить работу всей сети. Разделение доступа сетевых приложений при работе с SDN-контроллером – важная проблема в разграничении зон ответственности сетевых приложений. Когда сетевое приложение способно изменять flow-таблицы любого управляемого данным контроллером коммутатора, это идет вразрез с современными требованиями информационной безопасности. Кроме того, различные виды приложений требуют различного уровня доступа, и чем более детально описаны ограничения каждого приложения (в соответствии с целью выполняемой задачи), тем более надежной будет сеть.

В программно-определяемой сети также могут возникнуть угрозы и от сетевых устройств, такие как подмена контроллера, «отказ в обслуживании» и т. д. Перенос «мозговой» части сети на контроллер вполне логично переносит многие атаки с сетевого оборудования на программное обеспечение, отвечающее за функционирование сети: контроллер сети и сетевые приложения, обращающиеся к контроллеру [6].

При атаках «отказ в обслуживании» уязвимость SDN-коммутатора следует из работы алгоритма при получении неизвестного (отличного от правил flow-таблицы) пакета. Как результат, можем получить два следующих развития событий:

1. Пакет останется в памяти коммутатора, а на контроллер отправятся только заголовки пакета.

2. Пакет полностью отправится для анализа на контроллер.

Оба способа оставляют для атакующего широкое поле для эффективной реализации отказа в обслуживании путем формирования потока различных пакетов в SDN-сети. В результате данная атака может привести к следующему развитию событий:

– Исчерпание ресурсов коммутатора - пакеты, которые имеют право на прохождение, либо не будут обработаны сетевым устройством, либо будут обработаны, но с критичной задержкой.

– Канал связи между контроллером и коммутатором будет загружен большим количеством данных и не сможет гарантировать доставку сообщений управления

– Контроллер не справится с приходящими запросами и не обработает сообщения управления.

Архитектура SDN значительно меняет структуру сети и, как следствие, появляются новые угрозы безопасности, вызванные уязвимостями и недостатками отдельных компонентов инфраструктуры. Кроме того, большинство угроз, связанных с традиционными сетями передачи данных, являются проблемой и в сетях SDN. Однако, нет сомнений, что с течением времени технология SDN претерпит изменения и будет улучшена с точки зрения информационной безопасности.

Список используемых источников

1. Ефимушкин В. А., Ледовских Т. В., Корабельников Д. М., Языков Д. Н. Обзор и классификация решений, реализующих концепции SDN/NFV // В кн.: тез. докл. IX Международной отраслевой научной конференции «Технологии информационного общества», 24 нояб. 2015 г. М. : ИД Медиа Паблишер, 2015.С. 41–42.
2. Левин М. В., Ушаков И. А., Цветков А. Ю., Исаченков П. А. Основы построения компьютерных сетей. СПб. : СПбГУТ, 2016. 56 с.
3. Киррилов Д. И., Красов А. В., Долгорук Ю. Г., Селиванов А. Е., Ушаков И. А. Основы информационной безопасности сетей и систем: учебное пособие. Часть 1. СПб. : СПбГУТ, 2012. 64 с.
4. Киррилов Д. И., Красов А. В., Долгорук Ю. Г., Селиванов А. Е., Ушаков И. А. Основы информационной безопасности сетей и систем: учебное пособие. Часть 2. СПб. : СПбГУТ, 2012. 64 с.
5. Martin Casado, Tal Gerfinkel, Aditya Akella, Michael J. Freedman Dan Boneh, Nick Mckeown, Scott Shenker SANE: A protection Architecture for Enterprise Networks // 15-th Usenix Secutiry Symposium, Vancouver, Canada, August 2006.
6. Коляденко Ю. Ю., Лукинов И. Г. Модель распределенных атак в программно-конфигурируемых сетях связи // Вестник ЮУрГУ. Серия «Компьютерные технологии, управление, радиоэлектроника», 2017. Т. 17, No 3. С. 34–43.

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

УДК 004.77

АНАЛИЗ ВАРИАНТОВ ПОСТРОЕНИЯ ИНФОКОММУНИКАЦИОННОЙ СЕТИ ДЛЯ ОПЕРАТИВНОГО КОНТРОЛЯ ПАРАМЕТРОВ ОКРУЖАЮЩЕЙ СРЕДЫ НА ОСНОВЕ ТЕХНОЛОГИИ SDN

К. Э. Есалов[1], С. В. Кисляков[1,2], А. О. Пархоменко[1,2], Ю. А. Фролова[1]

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

Статья посвящена исследованию возможных подходов к управлению сетями SDN. Для оценки возможностей данной технологии разработана модельная сеть, объединяющая контроллеры Интернета вещей, сегмент SDN, облачное хранилище для данных, получаемых с датчиков. В статье описывается модель сети, её программно-аппаратная реализация с обоснованием выбора программ и устройств, приводятся результаты исследования.

IoT (Internet of Things), SDN, OpenDaylight, Open Network Operating System, OpenFlow, OpenvSwitch, Raspberry Pi

Введение

Актуальность использования сетей SDN объясняется рыночными тенденциями. В настоящее время наблюдается резкое сокращение доходов операторов связи от стандартных услуг, при этом потребляемый трафик передачи данных стремится вверх. Технология Software-Defined Networks должна способствовать переориентации операторских бизнес-моделей на облачные и цифровые сервисы, а также освобождению сетей от переизбытка оборудования [1].

В исследовании предлагается разобраться, как осуществлять управление сетями, построенными на новой технологии, решать задачи управления: неисправностями, конфигурацией, качеством, производительностью, безопасностью. Для этого смоделирована сеть, связывающая контроллеры ИВ, ПКС и «Облако» с подключенными подписчиками (или без оных) (рис. 1).

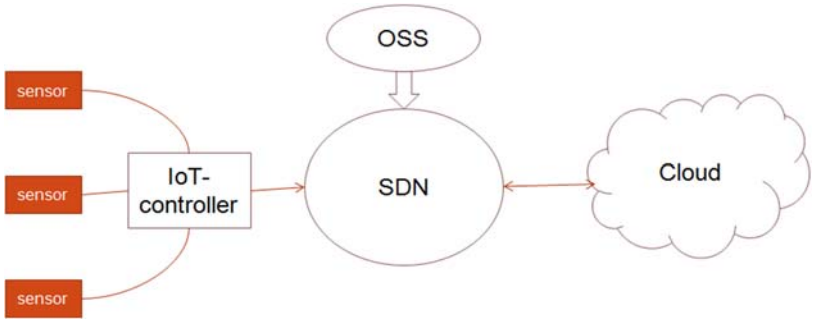


Рис. 1. Схема целевой модели сети SDN

Выбор такой модели обусловлен тем, что область IoT (*Internet of Things*) является динамично развивающейся технологией и актуальной на рынке телекоммуникаций сегодня. IoT – *к*онцепция вычислительной сети физических объектов («вещей»), оснащённых встроенными технологиями для взаимодействия друг с другом или с внешней средой, имеет в наличии большое число объектов управления, а также возможность быстро и гибко управлять ими и всей инфраструктурой.

Модель исследования состоит из фрагмента сети IoT, сегмента SDN сети, «Облака». В работе отражены результаты эксперимента управления датчиками IoT, подключенных к контроллеру IoT. Данные с датчиков передаются через SDN в «облако» для хранения, отображения, передачи подписчикам. Управление осуществляется со стороны OSS, в процессе эксперимента исследованы подходы к реализации управления сетью SDN.

1 Эталонная модель SDN и модельная сеть

Основным отличием SDN от традиционных сетей является централизованные интеллектуальное управление и мониторинг сети, которые обеспечивают проверку, контроль и модификацию потоков, передаваемых данных [2].

Основным элементом концепции SDN является протокол OpenFlow, который обеспечивает взаимодействие контроллера с сетевыми устройствами на «южной» стороне (рис. 2). На «северной» стороне контроллер предоставляет программные интерфейсы (API), наличие которых позволяет создавать приложения для управления сетью. Благодаря контроллеру, вся сеть, состоящая из множества разнотипных устройств разных производителей, воспринимается приложением как один логический коммутатор [3].

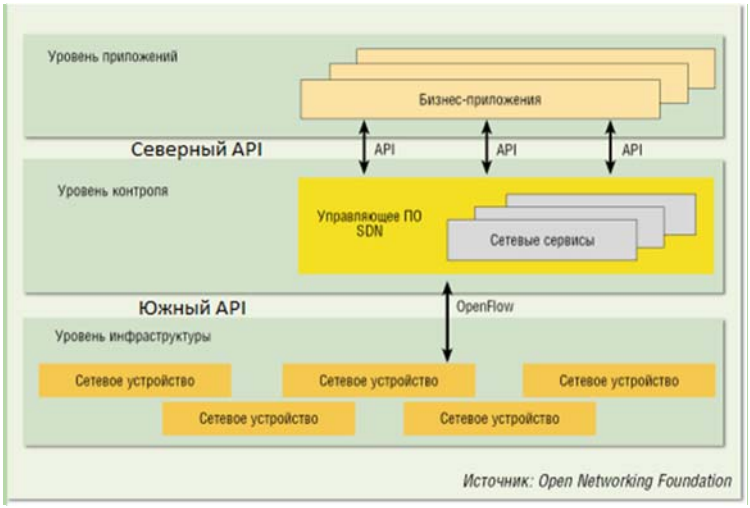


Рис. 2. Эталонная схема SDN-архитектуры

Для реализации задачи было решено использовать наиболее доступное на рынке телекоммуникации оборудование для исследований и софт с открытым исходным кодом.

Решения SDN можно разбить на три основные категории:

- академические проекты;
- решения с открытым исходным кодом в рамках сообществ;
- коммерческие продукты.

При детальном изучении стало очевидным следующее: несмотря на то, что на рынке присутствует множество SDN-контроллеров, формируются три лидирующие платформы, все они «из мира» open source – проекты OpenDaylight (ODL), Open Network Operating System (ONOS) и Floodlight [4]. Эти платформы набирают популярность в индустрии, а значит, риски несовместимости продуктов минимальны, также они находятся в бесплатном доступе и активно используются для исследований возможностей сети SDN.

Floodlight – контроллер с открытым исходным кодом ПО, поддерживаемый открытым сообществом разработчиков. Разработан на основе платформы контроллера Beacon, на языке Java. Имеет лицензию Apache, т. е. может использоваться для любых целей [4].

OpenDaylight (ODL) – консорциум крупных производителей, основанный в 2013 году, с целью создания модульного SDN-контроллера. Но, фактически, ODL вырос в огромную платформу, где контроллер – всего лишь её часть. Наиболее интересный факт касательно ODL – многие вендоры используют код OpenDaylight в качестве «базы» для собственного коммерческого продукта, в их числе Cisco и Citrix.

Open Network Operating System (ONOS) – открытый проект сообщества The Linux Foundation, в рамках которого создается операционная система для управления ПКС телекоммуникационных операторов. Одной из главных задач, решаемых ONOS, является масштабируемость, которая лежит в будущем планировании исследуемой в статье сети [5].

Для уровня контроля рассматривались именно эти платформы, однако для нашего эксперимента был выбран Floodlight в связи с обширностью материалов по установке этого контроллера и простоте его использования.

Для моделирования на уровне инфраструктуры (данных) было реализовано ядро виртуальной сети – Open vSwitch (или OvS, которое работает по протоколу OpenFlow с устройствами сети) для объединения виртуальных и физических сетевых устройств, а именно, для создания макета SDN на базе компьютера Raspberry Pi.

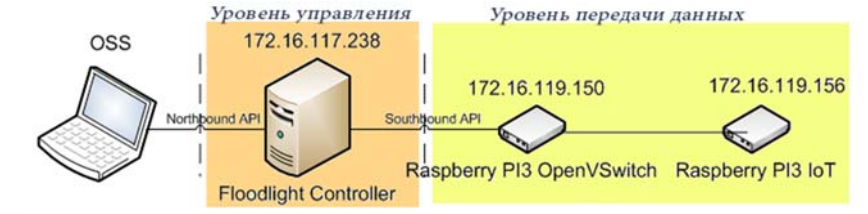


Рис. 3.Схема архитектуры SDN-сети собираемого макета

2 Экспериментальная часть. Описание макета

Для реализации модели сети по совокупности технических параметров и ценовой возможности был выбран компьютер Raspberry Pi3, позволяющий устанавливать различное ПО (*Raspbian* и *Android*), а также подключать соответствующие датчики. И, что является немаловажным, официальное ПО для Raspberry Pi3 – Raspbian, относится к семейству Linux и поддерживает конфигурацию сети с терминалом, в отличие от обыкновенного планшета на Android. В качестве датчика для исследования был выбран датчик влажности и температуры воздуха DHT11.

На макете планируется тестирование управления трафиком, анализ возможностей IoT/SDN сети в связке, мгновенная отправка данных с датчиков в облако, а также их анализ и обработка.

3 Экспериментальная часть. Описание результатов эксперимента

1. На первом этапе работы на аппаратную платформу Raspberry было установлено самое актуальное ПО Raspbian. Проведены первичные пользовательские настройки интерфейса и сети.

2. Следующим этапом работы стало создание макета, объединяющего контроллер и датчик влажности и температуры воздуха DHT11, сенсор имеет собственный протокол обмена данными 1-Wire. Результаты запросов представлены на рис. 4, 5.

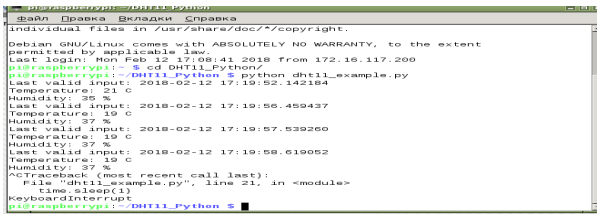


Рис. 4. Запрос о данных влажности и температуры воздуха с датчика (работа с терминала Raspberry)

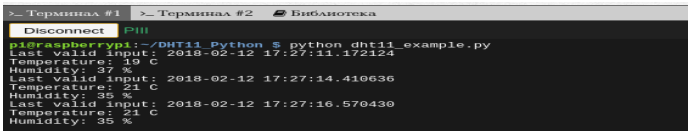


Рис. 5. Запрос о данных влажности и температуры воздуха с датчика (работа с виртуальной лаборатории НОЦ «ИКТ» СПбГУТ)

3. Реализация ядра виртуальной сети – OpenvSwitch для создания макета SDN на Raspberry Pi. Для установки OpenVSwitch используется дистрибутив последней версии 2.9.0, для работы были установлены модули и заголовки Raspbian, запущены модули OVS, создана база данных и ее конфигурационный файл. При выполнении скрипта запускается OVS и все необходимые для его работы модули. На рис. 6 представлены созданные в сети виртуальные коммутаторы.

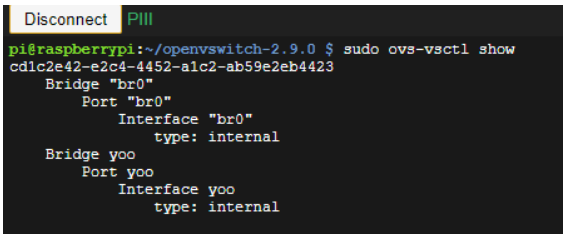


Рис. 6. Виртуальные коммутаторы в *OvS*.

Заключение

В ходе исследования была проделана работа, связанная с настройкой компьютера Raspberry Pi, организацией первичного макета сети (контроллер-датчик). Планируется доработать начатую реализацию ядра виртуальной платформы для масштабирования сети, создание синхронизации с облачным хранилищем НОЦ «ИКТ». Разработанный макет сети IoT/SDN планируется использовать для моделирования и исследования алгоритмов управления с учётом результатов, полученных в [6].

Список используемых источников

1. Джонес H.Top 10 IoT Technologies for 2017 and 2018 // Gartner G00296351 2016.
2. Архитектура SDN [Электронный ресурс] // Open Networking Foundation.2014 URL: https://www.opennetworking.org/ (дата обращения 18.01.2018).
3. Журнал сетевых решений / LAN [Электронный ресурс]. URL: https://www.osp.ru/lan/2012/12/13033012 (дата обращения 22.01.2018).
4. Владыко А. Г., Матвиенко Н. А., Новиков М. И., Киричек Р. В. Тестирование контроллеров программно-конфигурируемой сети на базе модельной сети // Информационные технологии и телекоммуникации. 2016. Том 4. № 1. С. 17–28.
5. SDN-блог [Электронный ресурс]. URL: https://sdnblog.ru/odl-and-onos-sdn-opensource-leaders/ (дата обращения 30.01.2018).
6. Гольдштейн А. Б. Модели и методы эксплуатационного управления телекоммуникационными сетями // Электросвязь. 2017. № 8. С. 35–41.

УДК 004.93

АНАЛИЗ АРХИТЕКТУР НЕЙРОННЫХ СЕТЕЙ ДЛЯ РЕШЕНИЯ ЗАДАЧ КЛАССИФИКАЦИИ ТРАФИКА

К. Э. Есалов, С. М. Маслюхин, М. Е. Павленко

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

Классификация сетевого трафика стала важной задачей в связи с быстрым ростом объёма трафика, передаваемого по сети интернет. Существует большое количество различных подходов, решающих эту задачу. Большинство этих подходов используют сигнатуры, извлеченные экспертом для классификации сетевого трафика. В настоящее время появляются новые способы классификации трафика, основанные на машинном обучении и глубоких нейросетевых архитектурах. В этом исследовании проводится анализ существующих глубоких нейронных сетей, решающих задачу классификации трафика и их сравнение с устоявшимися подходами.

классификация трафика, глубокое обучение, нейронные сети.

При предоставлении услуг интернет большое внимание уделяется восприятию предоставляемых услуг пользователем. Приложения должны быстро реагировать на действия человека, файлы должны быстро скачиваться, голос не должен прерываться, иначе пользователь может выбрать другого поставщика услуг. Для достижения достаточного качества обслуживания необходимо обеспечить возможность управления трафиком. Для этого необходимо знать какому протоколу, приложению принадлежит трафик. Существует несколько подходов к решению этой важной задачи, большинство из них использует предопределённые функции (сигнатуры).

Порт-ориентированный подход является одним из старейших и наиболее отработанных способов. Классификаторы на основе портов используют информацию из заголовка TCP/UDP пакетов для извлечения номера порта, который, как предполагается, связан с конкретным приложением. После извлечения номера порта, он сравнивается с назначенным IANA TCP/UDP номером портов для классификации трафика. Извлечение – простая процедура и номера портов не затрагиваются схемами шифрования. Из-за высокой скорости извлечения, этот метод часто используется в брандмауэре и списке управления доступом. Известно, что классификация на основе портов является одним из самых простых и самых быстрых способов идентификации сетевого трафика. Однако распространенность обфускации портов, трансляции сетевых адресов, переадресации портов, и использования случайных портов значительно сократили точность этого подхода. Согласно статистике, только 30–70 % текущего интернет трафика можно классифицировать с использованием методов классификации на основе портов. В следствии этого появились новые подходы.

Метод инспекции полезной нагрузки основан на анализе информации, доступной в полезной нагрузке пакетов приложений. Большинство методов проверки полезной нагрузки, также известных как DPI (*deep packet inspection*), используют предопределенные сигнатуры для определения каждого протокола. Необходимость обновления шаблонов всякий раз, когда появляется новый протокол, и проблема конфиденциальности пользователей являются одними из самых важных недостатки такого подхода. Также для формирования новых сигнатур необходимо прибегать к помощи экспертов, что делает добавление новых протоколов трудоёмким и затратным.

Графические методы основаны на анализе взаимодействия узлов сети на уровне приложения методами теории графов. Каждое приложение имеет свой собственный граф, который почти уникален для этого конкретного приложения. Iliofotou предложил график дисперсии трафика (TDG) под названием «Graption» для классификации приложений P2P. Они достигли 95 % точности, охватывающей Gnutella, e-Donkey, FastTrack, Soribada, MP2P и BitTorrent P2P [1].

Простые и сложные статистические методы основаны на предположении, что базовый трафик для каждого приложения имеет некоторые статистические функции, которые почти уникальны для каждого приложения. Каждый статистический метод использует свои собственные функции и статистику.

Для классификации трафика было опубликовано огромное количество работ по применению методов машинного обучения. Auld и др. предложили байесовскую нейронную сеть, которая была обучена классифицировать наиболее известные протоколы P2P, включая Kazaa, BitTorrent, GnuTella, и достигла 99 % точности. Moore и др. достигли 96 % точности в том же наборе приложений, используя классификатор Naive Bayes и оценку плотности ядра [2]. Однако достаточно плохо исследована область применения методов глубокого обучения. Далее представлен обзор имеющихся решений.

Нейронные сети представляют собой вычислительные системы, состоящие из множества простых, взаимосвязанных элементов, которые обрабатывают информацию, поступающую на вход и реагируют соответствующим образом. На практике эти сети, как правило, построены из огромного количества строительных блоков, называемых нейронами, где они соединены через связи друг с другом. Каждой связи присваивается вес. Во время обучения нейронной сети подаётся большая выборка подготовленных данных. Широко используемый алгоритм обучения, используемый для обучения таких сетей метод обратного распространения ошибки (*backpropagation*), корректирует веса для достижения желаемого результат. Известно, что при использовании больших выборок данных, обученные модели могут эффективно решать задачи классификации. Следовательно, обычно рекомендуется использовать нейронные сети, когда имеется достаточный объем данных для обучения и тестирования сети. При решении задач классификации трафика возможен сбор больших корпусов данных, что позволяет считать возможным эффективное применение глубоких нейронных сетей. Глубокое обучение можно рассматривать как особый вид нейронных сетей с большим количеством скрытых слоёв. В связи с быстрым ростом вычислительной мощности и наличием высокопроизводительных графических процессоров, обучение глубоких нейронных сетей стало более доступным, поэтому исследователи из разных научных областей рассматривают возможность использования глубоких нейронных сетей в своей области исследований. Следует отметить, что глубокое обучение достигло хороших результатов во многих областях, таких как распознавание речи, машинное зрение и обработка естественного языка.

В данной работе рассматривается применение трёх архитектур нейронных сетей: многослойный перцептрон, свёрточная нейронная сеть и автокодировщик.

Многослойный перцептрон представляет собой базовую нейронную сеть прямого распространения. Он состоит из входного слоя, одного или нескольких скрытых слоев и выходного уровня. Поэтому многослойный перцептрон всегда имеет как минимум 3 слоя. В многослойном перцептроне все узлы полностью связаны между слоями. Для обучения используются две процедуры, прямое распространение, которое инициализирует веса, и обратное распространение ошибки, которое вычисляет ошибку выходного слоя, а затем обновляет веса проходя слои в обратно направлении. Один проход называется эпохой и состоит из обработки нескольких наборов данных [3, С. 150–173].

Сверточные нейронные сети – это еще одна разновидность модели глубокого обучения, в которой извлечение признаков из входных данных осуществляется с использованием слоев, состоящих из свёрточных функций. Подобно другим типам моделей глубокого обучения, извлечение признаков играет важную роль в свёрточных сетях. Признаки, извлеченные в более мелких слоях свёрточной сети, будут передаваться в последующие свёрточные слои для получения более абстрактных признаков. Свёрточная нейронная сеть использует нейроны с локальными связями между слоями. Важным компонентом свёрточной нейронной сети является механизм пуллинга. Обычно его добавляют между последовательными свёрточными слоями. Функция таких слоев заключается в постепенном уменьшении пространственного размера представления данных, чтобы уменьшить количество параметров и вычислений в сети. Свёрточные нейронные сети были успешно применены к различным областям, включая обработку естественного языка и машинное зрение [3, С. 282–290].

Автокодировщик состоит из двух нейронных сетей: кодер, который извлекает абстракции и декодер, который восстанавливает исходные данные. Автокодировщик позволяет достичь уменьшения размерности данных и уменьшения шума в данных. Скрытые блоки в кодере сохраняют важную информацию и в то же время удаляют шум. Это в конечном итоге приводит к более эффективному и содержательному представлению данных на выходе из декодера. В исследуемой модели использовался многослойный перцептрон для кодировщика и декодера, с переменным количеством нейронов в скрытом слое кодировщика для построения более эффективной модели вариативный автокодировщик. Вместо запоминания структуры нечетких данных он генерирует скрытые векторы, следующие за гауссовским распределением. В следствии чего, чтобы вычислить потерю вариативному автокодировщику необходимо рассмотреть два типа потерь: ошибку между входными и восстановленными данными и потерю между скрытыми переменными и гауссовыми элементами, отражёнными информационным расхождением. Обучение вариативного автокодировщика обладает высокой

сложностью из-за компромисса между этими двумя разными типами потерь [3, С. 422–428].

Результаты экспериментального сравнения описанных выше моделей представлены в таблице 1 [4].

ТАБЛИЦА 1. Сравнение моделей глубокого обучения

Метрики	Истиноположительная оценка	Ложноположительная оценка
Автокодировщик (80)+k-NN	97.89	2.07
Автокодировщик (100)+SVM	97.6	1.47
Автокодировщик (80)+k-FP	96.2	0.98
Многослойный перцептрон	96.56	2.78
Свёрточная нейронная сеть	96.72	1.78

Все тестируемые модели показали высокую точность классификации. Наибольшей точности достигла модель автокодировщика с алгоритмом классификаци k ближайших соседей. Однако стоит помнить, что свёрточная сеть требует значительно меньших вычислительных затрат и при этом показывает хорошие результаты классификации, поэтому она более предпочтительна.

Результаты сравнения свёрточной нейронной сети и стандартных методов машинного обучения представлены в таблице 2 [5].

ТАБЛИЦА 2. Сравнение результатов глубокого и машинного обучения

Задача	Алгоритм	Метрики	%
Классификация трафика приложений	Свёрточная нейронная сеть	Accuracy	95,4
	k-NN		93,9
Классификация трафика по типам	Свёрточная нейронная сеть	Precision	97,0
	C4.5		89,7

Свёрточная нейронная сеть позволяет достичь большей точности на задачах классификации трафика в сравнении с алгоритмами машинного обучения. Кроме того, данная модель не требует участия экспертов при добавлении новых классов, что положительно отличает её от метода инспекции полезной нагрузки.

Исследование применения глубоких нейронных сетей к задачам классификации трафика является перспективной областью. В дальнейшем планируется расширить количество исследуемых моделей и их разновидностей на большем количестве классов (приложений).

Список используемых источников

1. Iliofotou M., Kim H.-c., Faloutsos M., Mitzenmacher M., Pappu P., Varghese G. Graption: A graph-based p2p traffic classification framework for the internet backbone, Computer Networks, 2007

2. Auld T., Moore A. W., Gull S. F. Bayesian neural networks for internet traffic classification, IEEE Transactions on neural networks 223–239, 2012

3. Гадфеллоу Я., Бенджио И., Курвилль А. Глубокое обучение: 2 изд. М. : ДМК Пресс, 2017. 652 с. ISBN 978-5-97060-618-6.

4. Oh S. E., Sunkam S., Hopper N. Traffic Analysis with Deep Learning, arXiv preprint arXiv: 1711.03656, 2017, С. 8.

5. Lotfollahi M., Zade R. S. H., Siavoshani M. J., Saberian M. Deep Packet: A Novel Approach For Encrypted Traffic Classification Using Deep Learning, arXiv preprint arXiv:1709.02656, 2017, С. 16.

Статья представлена директором НИИ Технологий связи, кандидатом технических наук А. Г. Владыко.

УДК 004.822

АНАЛИЗ ВНУТРЕННИХ ВИКИ-РЕСУРСОВ В ЗАДАЧАХ ФОРМИРОВАНИЯ ОНТОЛОГИЧЕСКОЙ БАЗЫ ЗНАНИЙ

А. А. Зарубин[1], А. Р. Коваль[1], В. С. Мошкин[2], А. А. Филиппов[2]

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

Исследования авторов посвящены решению задачи разработка интеллектуальных алгоритмов и методик обработки и анализа внутрикорпоративных вики-ресурсов, позволяющих динамически формировать содержимое единого хранилища знаний. Извлечение из вики-ресурсов нечеткой синтагматической структуры и дальнейшее представление извлекаемых семантически-определенных знаний в виде единой унифицированной предметной онтологии позволяют обращаться к полученной базе знаний при решении сложных экспертных задач.

семантика, онтология, вики-ресурсы, база знаний.

В настоящее время деятельность любой крупной организации предполагает работу специалистов с большим объемом информации с целью получения и извлечения необходимых знаний для взаимодействия с партнерами, принятия управленческих решений и т. д. Для хранения подобного рода знаний зачастую используют внутренние вики-ресурсы, которые, однако, плохо приспособлены к семантической структуризации и поиску.

Wiki-ресурс – веб-сайт, структуру и содержимое которого пользователи могут самостоятельно изменять с помощью инструментов, предоставляемых самим сайтом, с применением специального языка разметки [1, 2, 3].

Таким образом, корпоративные wiki-ресурсы позволяют:

1. Формировать определенные фрагменты корпоративной базы знаний (КБЗ), не требуя от эксперта дополнительных навыков в области онтологического анализа, инженерии знаний и использования различных специализированных программных средств.

2. Вносить правки в сформированные фрагменты КБЗ нескольким экспертам, давая возможность в определенной мере избавиться от проблемы субъективности данных.

3. Отслеживать динамику развития содержимого БЗ, а при необходимости производить возврат к одной из предыдущих версий содержимого КБЗ.

4. Использовать развитый набор программных интерфейсов (API) и расширений, позволяющих в автоматическом либо автоматизированном режиме формировать или редактировать фрагменты содержимого БЗ.

5. Формировать каркас онтологии БЗ ПрО и актуализировать ее фрагменты на основе анализа содержимого различных КБЗ [4, 5].

При всех преимуществах wiki-ресурсов и их явной направленности на неподготовленного пользователя, данный вид КБЗ имеет существенный недостаток - отсутствие механизма проверки логической целостности и семантической согласованности содержащихся в них объектов ПрО.

Таким образом, существует необходимость в интеграции прикладной онтологии ПрО и корпоративных wiki-ресурсов в рамках единой БЗ.

В качестве основной задачи онтологической БЗ можно выделить предоставление механизма адаптации программной среды [6] к конкретной ПрО с помощью методов онтологического анализа и инженерии знаний.

Под способностью БЗ учитывать динамический характер процессов понимается наличие в онтологии БЗ средств, позволяющих описать процесс ПрО с указанием допустимого множества входных объектов онтологии, накладываемых на них ограничений, и новых или измененных объектов онтологии, полученных в результате выполнения этого процесса [7].

Контекст онтологии ПрО – это определенное состояние содержимого БЗ, которое может быть выбрано из множества состояний онтологии,

полученного в результате версионирования либо формирования содержимого БЗ с различных точек зрения («point of view») [8].

Формально онтологию БЗ можно представить в виде следующего выражения:

$$O = \left\langle T, C^{T_i}, I^{T_i}, P^{T_i}, S^{T_i}, F^{T_i}, R^{T_i} \right\rangle, i = \overline{1,n},$$

где n – количество контекстов онтологии, $T = \{T_1, T_2, \ldots, T_n\}$ – множество контекстов онтологии, C^{T_i} – множество классов онтологии в рамках i-го контекста, I^{T_i} – множество объектов онтологии в рамках i-го контекста, P^{T_i} – множество свойств классов онтологии в рамках i-го контекста, S^{T_i} – множество состояний объектов онтологии в рамках i-го контекста, F^{T_i} – множество процессов ПрО, зафиксированных в онтологии в рамках i -го контекста, R^{T_i} – множество отношений онтологии в рамках i -го контекста вида:

$$R^{T_i} = \left\{ R_C^{T_i}, R_I^{T_i}, R_{II}^{T_i}\ R_P^{T_i}, R_S^{T_i}, R_{F_{IN}}^{T_i}, R_{F_{OUT}}^{T_i} \right\},$$

где $R_C^{T_i}$ – множество отношений, определяющих иерархию классов онтологии в рамках i-го контекста, $R_I^{T_i}$ – множество отношений, определяющих связь «класс-объект» онтологии в рамках i-го контекста, $R_{II}^{T_i}$ – множество отношений, определяющих связь «объект-объект» онтологии в рамках i-го контекста, $R_P^{T_i}$ – множество отношений, определяющих связь «класс-свойство класса» онтологии в рамках i-го контекста, $R_S^{T_i}$ – множество отношений, определяющих связь «объект-состояние объект» онтологии в рамках i-го контекста, $R_{F_{IN}}^{T_i}$ – множество отношений, определяющих связь между входом процесса $F_j^{T_i}$ и остальными сущностями онтологии в рамках i-го контекста, $R_{F_{OUT}}^{T_i}$ – множество отношений, определяющих связь между выходом процесса $F_j^{T_i}$ и остальными сущностями онтологии в рамках i-го контекста.

На рис. 1 представлен иллюстративный пример онтологии БЗ, в котором приводится описание процесса производства детали.

Представленная онтология содержит классы «Объект» и «Субъект», для которых заданы определенные наборы свойств. Данные классы являются родителями для всех остальных классов онтологии, при этом свойства родителей наследуют их потомки.

Онтология также содержит объекты «Станок», «Деталь» и «Мастер», каждый объект имеет свой набор состояний. «Создание объекта «Деталь» – зафиксированное в онтологии описание процесса производства детали. Данный процесс имеет два входа: «Станок» и «Мастер», и один выход – «Деталь», характеристики которой напрямую зависят от характеристик станка и квалификации мастера.

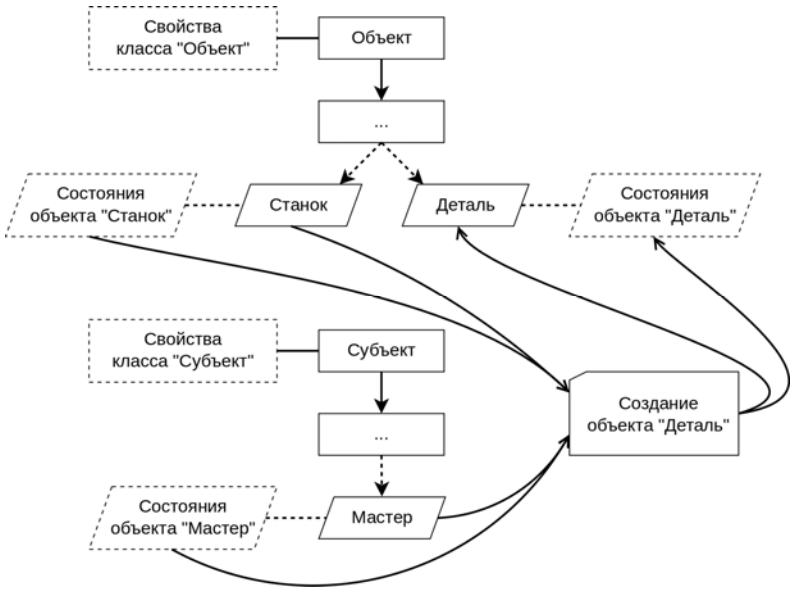


Рис. 1. Иллюстративный пример онтологии БЗ

Для автоматизации работы эксперта по созданию онтологии ПрО в рамках рассматриваемой БЗ используется метод автоматического формирования структуры онтологии на основе содержимого внешних wiki-ресурсов. При этом структура онтологии строится в процессе анализа системы категорий данного ресурса и «шаблонов-карточек» («*infoboxes*») – стандартизованных таблиц, содержащих основную информацию о предмете, описываемом в статье [9, 10].

Формирование внешних wiki-ресурсов на основе содержимого БЗ осуществляется по следующему алгоритму:

1. Эксперт указывает, какие классы онтологии должны учитываться в процессе формирования внешнего wiki-ресурса в качестве категории, подкатегории и страницы.

2. Эксперт указывает, какие отношения онтологии описывают связь объекта с его описанием, например, в виде текста.

3. Система на основе анализа отношений онтологии формирует структуру внешнего wiki-ресурса, заполняет «шаблоны карточек» и, если встречаются отношения, описывающие связь «объект-описание», заполняет страницу содержимым данного описания.

Также существует альтернативный подход к формированию wiki-ресурсов (внутренние wiki-ресурсы) на основе содержимого БЗ: пользователь применяет механизмы самой БЗ для получения и редактирования данных с использованием динамически сгенерированных экранных форм. Данный подход позволяет совместить преимущества онтологии и wiki-ресурсов за счет клиенто-ориентированных средств управления и механизмов проверки логической целостности и семантической согласованности содержимого БЗ. Архитектура разработанной БЗ представлена на рис. 2.

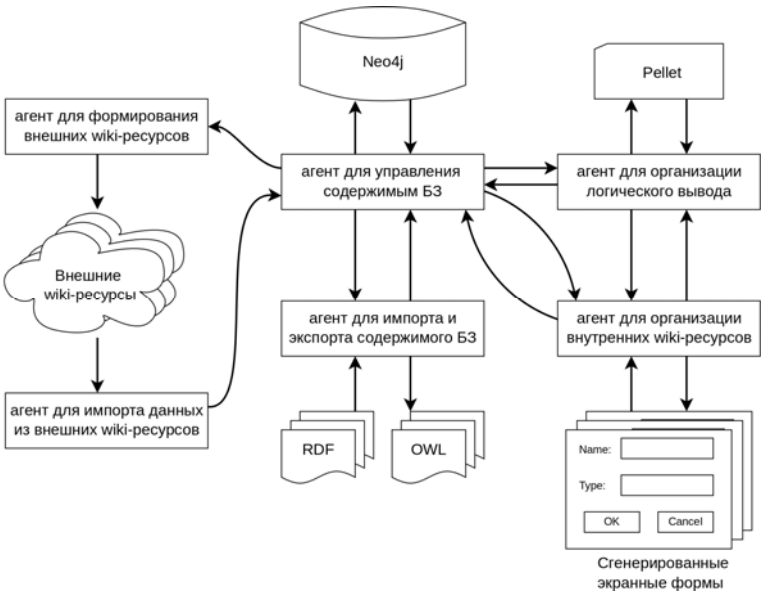


Рис. 2. Архитектура БЗ

Таким образом, расширение функционала онтологической платформы посредством использования агентов управления экспертными знаниями позволяет обеспечить специалистов организаций разных профилей универсальным инструментарием анализа особенностей проблемной области с возможностью автоматизированного пополнения, расширения базы знаний из общедоступных источников, а также ее визуализации в виде сложноструктурированного материала.

Особенно важным в аспекте решения задачи полного информационного обеспечения деятельности специалистов является наличие возможности представления знаний в сетке их контекстов, в том числе временных, а также контекстов разных точек зрения («point of view») на рассматриваемые объекты ПрО.

Исследование выполнено в рамках ПНИЭР по теме «Разработка архитектуры, методов и моделей построения программно-аппаратного комплекса семантического анализа слабоструктурированных информационных ресурсов на российской элементной базе» согласно Соглашению о предоставлении субсидий № 14.607.21.0164 в рамках ФЦП «Исследования и разработки по приоритетным направлениям развития научно-технологического комплекса на 2014-2020 годы».

Список используемых источников

1. Андреев И. А., Башаев В. А., Клейн В. В., Мошкин В. С., Ярушкина Н. Г. Оценка терминологичности лексических единиц на основе онтологии предметной области // Открытые семантические технологии проектирования интеллектуальных систем (OSTIS-2015): материалы V Междунар. научн. техн. конф. (Минск, 19–21 февраля 2015 г.) / редкол.: В. В. Голенков (отв. ред.) [и др.]. Минск : БГУИР. 2015. С. 395–400.

2. Смирнов С. В. Онтологическое моделирование в ситуационном управлении // Онтология проектирования. 2012. № 2. С. 16–24.

3. Тузовский А. Ф. Разработка систем управления знаниями на основе единой онтологической базы знаний // Известия Томского политехнического университета. 2007. Т. 310. № 2. С. 182-185.

4. Гаврилова Т. А. Онтологический подход к управлению знаниями при разработке корпоративных информационных систем // Новости искусственного интеллекта. 2003. № 2. С. 24–30.

5. Голенков В. В., Гулякина Н. А. Семантическая технология компонентного проектирования систем, управляемых знаниями // Материалы V международной научно-технической конференции OSTIS-2015, Минск, Республика Беларусь, 2015.

6. Ярушкина Н. Г., Мошкин В. С. Применение алгоритма логического вывода на основе FuzzyOWL-онтологии // Радиотехника. 2015. № 6. С. 68–72.

7. Карабач А. Е. Системы интеграции информации на основе семантических технологий // Наука, техника и образование. 2014. № 2(2). С. 58–62.

8. Мошкин В. С., Ярушкина Н. Г. Логический вывод на основе нечетких онтологий // Интегрированные модели и мягкие вычисления в искусственном интеллекте. Сборник научных трудов VIII-й Международной научно-практической конференции (Коломна, 18–20 мая 2015 г.). В 2-х томах. Т. 1. М. : Физматлит, 2015. С. 259–267.

9. Suchanek F. M., Kasneci G., Weikum G. YAGO: A Core of Semantic Knowledge Unifying WordNet and Wikipedia // In Proceedings of the 16th International Conference on World Wide Web, USA. 2007.

10. Шестаков В. К. Разработка и сопровождение информационных систем, базирующихся на онтологии и Wiki-технологии // Труды 13-й Всероссийской научной конференции «Электронные библиотеки: перспективные методы и технологии, электронные коллекции» – RCDL’2011, Воронеж, Россия, 2011.

УДК 004.021

СПОСОБЫ ВНУТРИОБЪЕКТОВОГО ПОЗИЦИОНИРОВАНИЯ ПРЕДМЕТОВ И ПЕРСОНАЛА

А. А. Зарубин, Н. М. Редругина, А. В. Тарлыков

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

В рамках исследования проведен поиск наилучшего решения для системы внутриобъектового позиционирования предметов и персонала. Решение достигается путем сравнения способов контроля занятости персонала, выявления их плюсов и минусов. В статье рассматриваются такие системы как RFID, RTLS, биометрические системы, системы видео-фиксации, а также системы, в которых используются специальные программные средства.

позиционирование, моделирование, датчики, RFID, RTLS.

Статья описывает выбор наилучшего решения для системы внутриобъектового позиционирования предметов и персонала. Выбор достигается путем сравнения способов контроля местоположения персонала, выявления их плюсов и минусов [1]. Ниже будут рассмотрены способы внутриобьектового позиционирования, их плюсы и минусы. Дается объяснение выбора способа позиционирования.

RFID (*Radio Frequency IDentification*, радиочастотная идентификация) – способ автоматической идентификации объектов, в котором посредством радиосигналов считываются или записываются данные, хранящиеся в так называемых транспондерах, или RFID-метках. Большинство таких меток состоит из двух частей. Первая – интегральная схема (ИС) для хранения и обработки информации, модулирования и демодулирования радиочастотного (RF) сигнала и некоторых других функций. Вторая – антенна для приёма и передачи сигнала. Данные решения уже долгое время работают на многих предприятиях, где нужен контроль персонала в закрытых помещениях.

Назначением таких систем является контроль доступа при помощи считывателя, встроенного в турникеты или электронные замки. Конечно, система может указывать на количество часов, когда сотрудник отсутствовал на рабочем месте, но это не указывает на занятость персонала и не гарантирует, что радиометка, которую имеет сотрудник, не будет передана другому лицу. К тому же с использованием RFID-меток в повседневной жизни связан ряд проблем.

Можно сказать, что данная система является не лучшим решением для задачи внутриобьектового позиционирования, так как не может оперативно отслеживать координаты перемещения объекта. Но может подойди как дополнение к более функциональному, в зависимости от требований заказчика.

Аналогами RFID-систем служат биометрические системы, в которых в качестве считывателей применяются сканеры биометрических параметров отпечатки пальцев, сканер сетчатки глаза и др. Это устраняет возможность использования чужой радиометки, но предполагает большие затраты, что не выгодно заказчикам. Биометрические системы информируют о том, что объект находится в данном помещении, или пользуется данным оборудованием, но не информирует о его перемещении. Кроме того, этот способ плохо подходит для позиционирования предметов.

Также идентифицировать работников можно с помощью распознавания лиц системами видео фиксации, применение которых расширяется благодаря снижению стоимости вычислительных мощностей. Но такие системы могут быть не точными в случае большого скопления людей и также не подходят для контроля за предметами.

При работе сотрудника за личным ПК, можно использовать программные средства. Регистрация и вход в систему под своим логином, не устраняет возможность использования ПК третьим лицом, которому была передана учетная запись. Так же не указывает на местонахождение работника в нужный момент времени.

Все эти системы слабо подходят для оперативного контроля местонахождения персонала.

Для решения поставленной задачи целесообразно рассмотреть системы локального позиционирования в режиме реального времени (RTLS) которые появились относительно недавно. Главное их достоинство – отслеживание координат контролируемого объекта с низкой погрешностью, которая, впрочем, зависит от применяемых радиочастотных технологий и алгоритмов обработки сигналов. Радиометки минимизируют возможность подмены контролируемого лица, и при необходимости (по желанию заказчика) обеспечивают контроль местоположения работников и предметов.

Такие системы решают поставленную задачу позиционирования персонала, благодаря точности определения местоположения объектов и достоверности контроля, а в сравнении с другими системами решает более широкий круг задач.

ТАБЛИЦА. Сравнение систем позиционирования

Тип системы/ Параметр	RFID-системы	Биометрич. системы	Системы видео-фиксации	Програм. системы	RTLS-системы
Точность локации	зона обслуживания терминала	зона обслуживания терминала	створ камеры	при работе за ПК	до 1 м
Распознавание в массе людей	факт нахождения в зоне	факт нахождения в зоне	ограничено	нет	да
Возможность подмены контролир. лица	да	нет	сложно	да	зависит от исполнения метки
Деление помещений на зоны	сложно	сложно	да	нет	да
Отвлечение персонала	да	да	нет	зависит от программы	нет
Аналитика с целью оптимизации занятости и логистики	ограничена	ограничена	ограничена	ограничена	ограничена

Следует заметить, что наиболее современные технологии [2], реализуемые в RTLS-системах, часто обеспечивают не только технические, но и финансовые преимущества перед другими типами систем. То есть в ряде случаев их выгодно применять даже когда не требуется высокая точность определения местоположения объекта, а достаточно только установить факт его нахождения в помещении.

Кроме того, на их базе можно выполнять и другие функции (расчет временных нормативов, управление доступом, логистический анализ работы транспортных средств, обеспечение безопасности, параметрического мониторинга и др.).

В то же время ряд функций эти современные технологии не могут обеспечить, например, видеофиксацию. Как уже говорилось ранее, возможна их интеграция с другими типами систем, включая системы видеонаблюдения, системы контроля и управления доступом.

В настоящее время в RTLS-системах используются три основных метода локального позиционирования, различающиеся исходными измеряемыми параметрами [3, 4]:

1. По уровню радиосигнала RSSI (*Received Signal Strength Indicator*).

Программный интерфейс сервиса iOS i-Beacon является наиболее известной технологией в рамках данного метода. В роли излучателей выступают неподвижные маячки i-Beacon, в роли приемников – устройства, поддерживающие спецификацию BLE (*Bluetooth Low Energy*), прежде всего смартфоны на платформах Apple и Android (начиная с версии 4.3), находящиеся на расстоянии до 50 м от излучателей. Позже в рамках этой технологии стали применяться также подвижные маячки (радиометки – излучатели), которые раздаются людям или устанавливаются на подвижные объекты (то есть необходимость в обязательном использовании смартфонов отпала). При этом в качестве неподвижных приемников используются устройства со встроенным GSM/GPRS-модемом. Приемник опрашивает все видимые радиометки 26 и в режиме реального времени передает информацию на сервер. При этом по каждой радиометке за любой период доступны следующие данные: UID (*User identifier*, уникальный идентификатор для всех маячков данной компании), Major, Minor (для нумерации маячков в пределах одного идентификатора), RSSI и точное время фиксации данных. По полученным данным определяется местоположение радиометок.

2. По времени распространения радиосигнала.

Данный метод базируется на технологиях беспроводной связи, описываемых группой стандартов IEEE 802.15.4 и имеющих важную опцию измерения времени распространения сигнала между приемником и передатчиком. Так как такое измерение происходит во время посылки данных, то выполнение этой функции не требует дополнительных затрат энергии и большей пропускной способности каналов. Кроме того, появляется

возможность одновременного решения задач позиционирования и параметрического мониторинга. Дальность передачи данных на закрытых пространствах составляет 30–50 м и может быть увеличена с помощью ретрансляторов, в роли которых могут выступать те же считыватели. При этом определение местоположения производится с погрешностью до 2-х метров или с еще большей точностью. Технологии беспроводной связи, подпадающие под действие стандарта IEEE 802.15.4, предполагают низкую скорость передачи данных (2 Мбит/с для аппаратуры nanoLOC) и малое энергопотребление (в противовес Wi-Fi) [1, 2]. Минусом подобных средств является то, что они не так широко распространены, как средства Wi-Fi [4]. Для построения сетей в верхних слоях в рамках указанных технологий используются менее распространенные спецификации ZigBee, WirelessHAR, MiWi, ISA100.11, не интегрированные в массовую абонентскую аппаратуру – смартфоны. Но в рамках контроля занятости персонала можно не ориентироваться на этот недостаток, ведь иначе придется выдавать смартфоны работникам, для их позиционирования.

3. По углам относительно известных направлений – метод триангуляции.

В рамках этого метода сигнал от мобильной радиометки принимается стационарно установленными считывателями, имеющими известные координаты. При этом определяются углы его приема разными считывателями, на основании которых затем рассчитываются координаты радиометки. С помощью одного считывателя система может вычислить местоположение радиометки в двухмерной плоскости (этого достаточно, например, для установления факта нахождения объекта контроля в определенной зоне), а 2 считывателя дают местоположение радиометки в трехмерном пространстве с заявленной точностью до 0,5 м. На практике расстановка устройств производится таким образом, чтобы каждая радиометка находилась в зоне локации нескольких считывателей, что существенно повышает точность и надежность работы системы. Радиус действия каждого считывателя весьма существенный – 300 м. У технологии Quuppa Intelligent Locating System есть еще одно важное достоинство – она использует спецификацию BLE. Это обусловливает следующие преимущества:

a. длительный срок службы батареи (1 год и более);

b. совместимость со стандартными мобильными устройствами – таким образом устройства iOS и Android можно сделать «видимыми» для системы, просто добавив несколько строк кода в приложение;

c. возможность переноса данных с массы датчиков, оснащенных модулями BLE, то есть использование в качестве шлюза к Интернету вещей.

Данные датчиков могут быть отображены через открытый и настраиваемый программный интерфейс API. По всей видимости, для обеспечения

высокой точности измерений необходимо обеспечить примерно одинаковую высоту над уровнем пола для всех радиометок. Однако в случае контроля занятости персонала это несложно сделать, закрепив радиометки на работниках определенным образом. Минусом данного метода является отсутствие на сегодняшний день комплектующих, на основе которых можно было бы реализовать свою разработку, хотя в ближайшем будущем ситуация может измениться. Это может быть связано с выходом новой версии спецификации Bluetooth 5.0, поддерживающей навигационные функции и обеспечивающей связь устройств в радиусе 300 м при скорости передачи данных около 2 Мбит/с.

Список используемых источников

1. Кривченко Т. Программно-аппаратные методы измерения расстояния по времени распространения радиосигнала при помощи приемопередатчика nanoLOC [Электронный ресурс] // Беспроводные технологии: электрон. научн. журн. 2012. № 3. С. 48–53. URL: http://app.efo.ru/storage/art/wless/nanoLOC_2012.pdf (дата обращения 19.01.2018).

2. Molteni, R. WhAC: a WiFi-Based Application for Indoor Customer Localization [Электронный ресурс] // Politecnico di Milano: электрон. научн. журн. 2011. Н. 92–110. URL:https://www.politesi.polimi.it/bitstream/10589/21306/1/2011_07_Molteni_Perini.PDF (дата обращения 19.01.2018).

3. Миниахметов Р. Х., Рогов А. А., Цымблер М. Л. Обзор алгоритмов локального позиционирования для мобильных устройств [Электронный ресурс] // Вестник ЮУрГУ. Серия «Вычислительная математика и информатика»: электрон. научн. журн. 2013. Т. 2. № 3. С. 83–96. URL: https://vestnik.susu.ru/cmi/article/view/879/761 (дата обращения 19.01.2018).

4. Фофанов О. Б. Алгоритмы и структура данных // Томский политехнический университет. 2014. № 2. С. 126.

УДК 004.056

ТЕХНОЛОГИЯ TRUSTSEC, КАК ИНСТРУМЕНТ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Т. Е. Захарова, И. А. Ушаков, В. Ю. Холоденко

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

Данная работа посвящена вопросам обеспечения информационной безопасности с использованием технологии TrustSec. Рассматривается архитектура безопасности

TrustSec, как инструмент, предоставляющий комплексную защиту сетей. Данный компонент позволяет создать единую, обобщенную политику доступа в сеть для всех типов устройств и подключений, обеспечивая защиту каналов передачи данных в коммутируемых средах с помощью стандарта шифрования IEEE 802.1AE. Производится анализ работы TrustSec на основе оборудования компании Cisco: маршрутизаторов, коммутаторов, в которые встроена данная технология.

TrustSec, информационная безопасность, сегментация, сети, аутентификация, авторизация, IEEE 802.1, SGT.

Технология сегментации TrustSec, предоставляющая комплексную защиту сети, считается многими специалистами одним из самых перспективных инструментом обеспечения информационной безопасности. Её использование позволяет значительно снизить издержки, связанные с различными инцидентами безопасности. Данная технология эффективна даже в случае проникновения злоумышленника во внутренний контур корпоративной сети [1].

Общепринято, что TrustSec – это технология сегментации, которая предоставляет комплексную защиту сети. Технология сегментации занимается распределением пользователей и ресурсов в среде. Благодаря ей появляется возможность тщательней и современней спроектировать политики доступа с их углубленной детализацией и применением прозрачно через всю локальную или глобальную вычислительную сеть [2].

Архитектура Trustsec включает в себя:

– Media Access Control Security (MacSec IEEE 802.1AE), предназначен для шифрования канала в проводной среде;

– Security Group Tagging (SGT) – метка, предназначенная для авторизации (проверка прав пользователя);

– IEEE 802.1X – стандарт, предназначенный для аутентификации.

MacSec IEEE 802.1AE и IEEE 802.1X относятся к стандарту рабочей группы IEEE 802.1, которая занимается протоколами нижних уровней модели OSI, общими характеристиками управления ЛВС, а также вопросами информационной безопасности (ИБ). Говоря о ИБ стоит в первую очередь вспомнить о триаде сервисов IT-инфраструктуры: конфиденциальность, целостность, доступность. В архитектуре TrustSec вопросы конфиденциальности и целостности передаваемых тегов и данных относятся к технологии Media Access Control Security. Шифрование канала основано на 128 битном алгоритме AES (*Advanced Encryption Standard*) с использованием режима счетчика с аутентификацией Галуа.

MacSec шифрует связь между пользователем и коммутатором и между коммутаторами тем самым обеспечивает защиту канала от пассивного прослушивания и обеспечивает безопасность SGT меток от подмены. На рис. 1 представлен кадр Ethernet, в котором будет производиться шифрование:

– поле 802.1Q описывает процедуру тегирования,
– поле Cisco Meta Data которое несет в себе метку SGT,
– поле EtherType которое содержит информацию о типе протокола инкапсуляции,
– поле Payload полезной нагрузки 46–1500 байт.

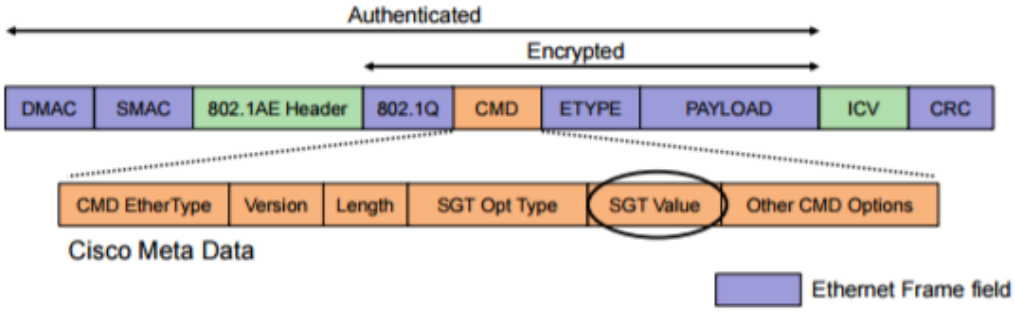


Рис. 1. Ethernet кадр

Поле Cisco Meta Data, которое несет в себе метку SGT вместе с ней добавляет в фрейм дополнительные 20 байт. Данная метка разработана специально для эффективного управления доступом в сети. Её назначают сервером контроля и учета доступа на оконечное устройство. При этом SGT несет в себе информации об определенном подключении:

– время доступа;
– тип доступа в сеть;
– метод аутентификации;
– тип устройства;
– параметры аутентификации;
– пользователь и его параметры [3].

Данная метка является идентификатором прав пользователя в сети и назначается как результат авторизации сессии оконечного подключившегося устройства, уникально его идентифицирует и переносится через всю сеть вместе с трафиком оконечного устройства. Таким образом дается возможность каждому распределяющему устройству, через которое идет пакет, видеть, принимать решение по фильтрации и журналировать транзакции, опираясь на широкий спектр информации об источнике трафика, помимо легко подменяющегося IP адреса [4].

Третьим аспектом архитектуры TrustSec является IEEE 802.1X – стандарт, описывающий процесс инкапсуляции данных проверки пользователей (EAP), передаваемых между клиентами, коммутаторами и серверами проверки подлинности [5]. IEEE 802.1X обеспечивает контроль доступа на основе аутентификации и авторизации пользователя в сети. Если оборудование не поддерживает 802.1X, то используются Mac Authentication Bypass (прим. принтеры) и Web Authentication.

Важными характеристиками является возможность сервера при аутентификации распределять пользователей в определенные логические компьютерные сети, назначать списки управления доступом, устанавливать время, в которое пользователь может подключиться к сети.

На рис. 2 изображены две ситуации:

– компьютер не аутентифицировался, и от данного компьютера могут отправляться только пакеты EAP, которые предназначены для аутентификации пользователя по протоколу EAPol (*extensible authentication protocol over* LAN);

– после аутентификации становится возможно передаваться пакеты, которые были разрешены пользователю в метке SGT.

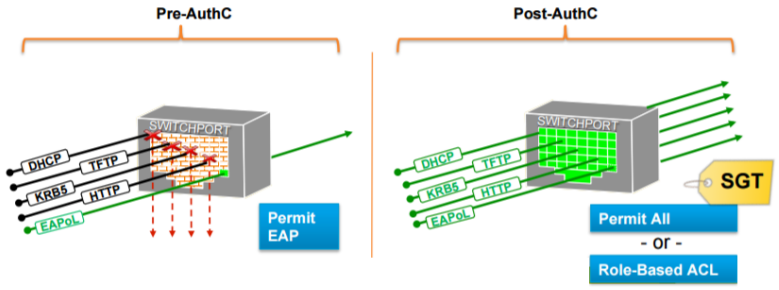


Рис. 2. Прохождение пакетов до и после аутентификации

В рамках лаборатории был собран стенд на основе реального оборудования Cisco для экспериментальной проверки результативности технологии TrustSec (рис. 3). Для её эффективного использования необходимо высокопроизводительные устройства, в эксперименте были задействованы коммутаторы Catalyst 3750-X, маршрутизаторы ASR1001, а также RADIUS сервер, в качестве устройства проверки подлинности [6].

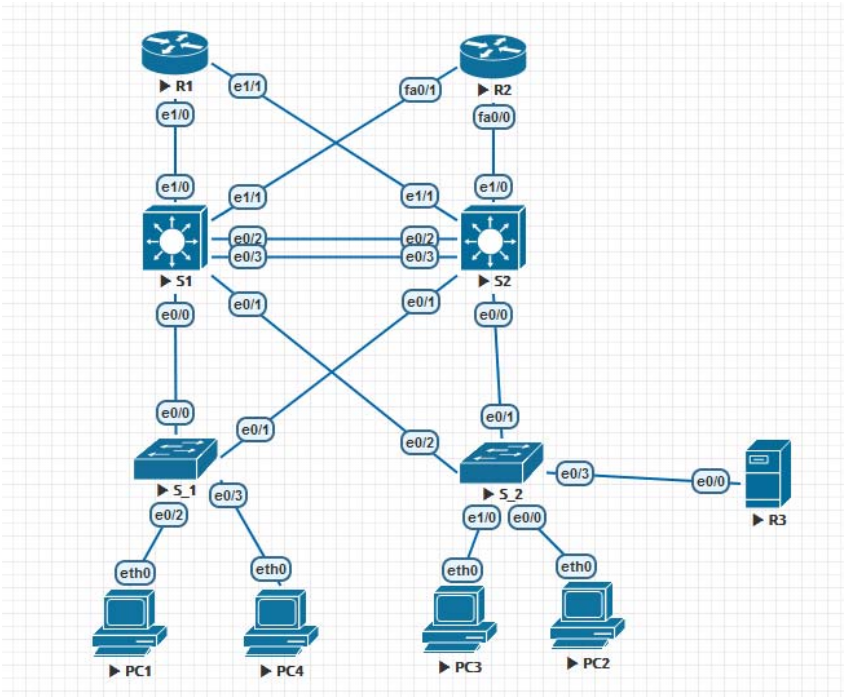


Рис. 3. Топология сети

Конфигурация MacSec на интерфейсе коммутатора:

```
Switch# show authentication sessions interface gigabitethernet1/0/26
Interface: GigabitEthernet1/0/26
MAC Address: 001b.2140.ec3c
IP Address: 1.1.1.103
User-Name: ms1
Status: Authz Success
Domain: DATA
Security Policy: Must Secure ß--- New
Security Status: Secured ß--- New
Oper host mode: multi-domain
Oper control dir: both
Authorized By: Authentication Server
Vlan Policy: 10
Session timeout: 3600s (server), Remaining: 3567s
Timeout action: Reauthenticate
Idle timeout: N/A
Common Session ID: 0A05783B0000001700448BA8
Acct Session ID: 0x00000019
Handle: 0x06000017
Runnable methods list:
Method State
dot1x Authc Success
```

Конфигурация IEEE 802.1x на коммутаторе:

```
Switch# configure terminal
Switch(config)# aaa new-model
Switch(config)# aaa authentication dot1x default group radius
Switch(config)# dot1x system-auth-control
Switch(config)# interface gigabitethernet1/0/15
Switch(config)# switchport mode access
Switch(config-if)# dot1x port-control auto
Switch(config-if)# end
Switch(config)# radius-server host 172.120.39.46 auth-port 1612 key default
```

Подводя итоги, можно сказать что, используя технологию TrustSec с программно-определяемым сегментированием, упрощается предоставление доступа в сеть, ускоряется работа службы безопасности и обеспечивается согласованное применение политик в любом месте сети. Технология TrustSec встроена в такие продукты Cisco, как коммутаторы, маршрутизаторы, беспроводные устройства и устройства защиты.

Реализация данной архитектуры управления доступом дает неоспоримую гибкость в реализации политики сетевой безопасности компании, имеет глубочайшую интеграцию внутри продуктового портфолио Cisco. Компании, которые хотят внедрить данную технологию у себя, в первую очередь должны сделать предварительную оценку безопасности информа-

ции и уязвимости сети. Это поможет им решить есть ли потребность в данной технологии, так как для её реализации необходимо высокопроизводительное, дорогое оборудования. Помимо этого, стоит остро вопрос о взаимодействие с оборудованием других вендеров.

Список используемых источников

1. 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. 2015. С. 310–313.

2. Официальное руководство по изучению TrustSec «Cisco TrustSec Prakticky», 2013 [Электронный ресурс]. URL: https://cisco.com/

3. Казаков Д. Управление доступом в архитектуре Cisco TrustSec [Электронный ресурс] // Блог Cisco в России и СНГ. URL: https://gblogs.cisco.com/ru/dkazakov_cisco_trustsec/

4. Ковалев Д. TrustSec на защите корпоративных сетей // Век качества. 2010. № 4. С. 44–45.

5. Network Complexity – Michael H. Behringer: Classifying Network Complexity; slides; ACM ReArch'09 workshop; 2009 [Электронный ресурс]. URL: http://networkcomplexity.org/wiki/index.php?title=References

6. Implementing and Configuring Cisco Identity Services Engine / Student Guide, 2015. [Электронный ресурс]. URL: https://cisco.com/

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

УДК 004.056

ОЦЕНКА ПРОИЗВОДИТЕЛЬНОСТИ IP-АТС ELASTIX В ЗАВИСИМОСТИ ОТ ИСПОЛЬЗУЕМЫХ СЕРВИСОВ

И. П. Зуев, М. М. Ковцур

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

IP-телефония получила широкое распространение в корпоративном секторе. Для организации сервисов компании могут использовать как аппаратные, так и программные IP-АТС на базе аппаратного или виртуального сервера. Однако в открытых источниках недостаточно описаны методики нагрузочного тестирования IP-АТС. Доклад посвящен разработке методики оценки производительности IP-АТС, представлены рекомендации по аппаратной конфигурации, необходимой для функционирования IP-АТС.

IP-АТС, Elastix, методика тестирования, информационная безопасность.

На сегодняшний день IP-телефония получила широкое распространение в корпоративном секторе. Для развертывания необходимых сервисов могут быть использованы как аппаратные, так и программные IP-АТС. Одной из самых популярных среди IP-АТС является Elastix на базе Asterisk. Однако методики нагрузочного тестирования таких АТС и инструменты для их реализации описаны недостаточно, в том числе особенности тестирования при использовании протоколов информационной безопасности IP-телефонии.

Проанализировав существующие методы тестирования [1, 2] можно сделать следующие заключения: во-первых, в каждом нагрузочном тестировании использовалось базовое решение Asterisk/FreePBX без подключения дополнительных модулей для использования различных сервисов, необходимых корпоративным клиентам. Во-вторых, не представлены результаты тестирования с использованием протоколов информационной безопасности IP-телефонии, что является некорректным в условиях построения корпоративных сетей. Наконец, в результатах нагрузочных тестирований не представлены наглядные зависимости использования CPU/RAM от числа одновременных вызовов, что не дает однозначного понимания о возможностях и производительности IP-АТС. Этот недостаток, в свою очередь, затрудняет подбор оптимальной конфигурации сервера, на котором будет размещена АТС Elastix.

В разрабатываемой методики тестирования IP-АТС за основу наблюдения при оценке производительности предлагается взять следующие параметры:

– количество одновременных вызовов с использованием протоколов информационной безопасности (ИБ) и без них;

– количество звонков с протоколами ИБ и без ИБ при включенной функции записи разговоров;

– количество звонков, которые одновременно может обрабатывать IVR (*Interactive Voice Response*) – сервис голосового интерактивного меню;

– количество некорректных SIP-пакетов по отношению к общему объему трафика;

– количество некорректных RTP-пакетов.

При тестировании учитываются такие параметры, как:

– количество ядер CPU;

– количество выделенной RAM-памяти для IP-АТС Elastix;

– количество одновременных звонков, обрабатываемых IP-АТС.

Полученным результатом проведенного тестирования будет нагрузка на CPU и RAM по отношению к количеству одновременных звонков, выраженная в процентах.

Оценка параметров IP-АТС без использования протоколов информационной безопасности предполагает, что Elastix развернут на виртуальной машине, что упрощает масштабируемость оборудования. Такой подход позволяет без проблем выбирать определенные количественные характеристики оборудования, на котором будет производиться тестирование. В разрабатываемой методике количественные характеристики подразумевают число ядер центрального процессора и объем выделенной оперативной памяти. Для проведения тестов была выбрана программа SIPp, которая способна генерировать заданное число звонков и поддерживать несколько рабочих SIP-сессий одновременно.

Стоит сказать о проблематике оценки производительности Elastix с использованием протоколов информационной безопасности [4]. В результате исследования не было обнаружено комплексного решения по тестированию IP-АТС с использованием протоколов ИБ. Также имеется сложность выбора программного SIP-клиента, который бы удовлетворял следующим требованиям:

– поддержка протоколов ИБ (например, SRTP, ZRTP);

– поддержка работоспособности нескольких SIP-аккаунтов одновременно;

– использование малого объема вычислительных ресурсов, необходимого для запуска большого количества копий программного SIP-клиента.

Еще одним немаловажным фактом является то, что в общедоступных источниках не представлены сведения о том, насколько использование протоколов ИБ влияет на нагрузку связки CPU/RAM в тех же условиях работы IP-АТС, что и без них.

Перейдем к методике тестирования IP-АТС без использования протоколов информационной безопасности. На рис. 1 представлена схема проведенного тестирования. Имеется клиент № 1 с установленным программным обеспечением (ПО) «SIPp». Посредствам этого ПО генерируется число вызовов в диапазоне от 10 до 170 с шагом в 20, направленных в сторону клиента № 2. Данные звонки, соответственно, обрабатываются IP-АТС Elastix.

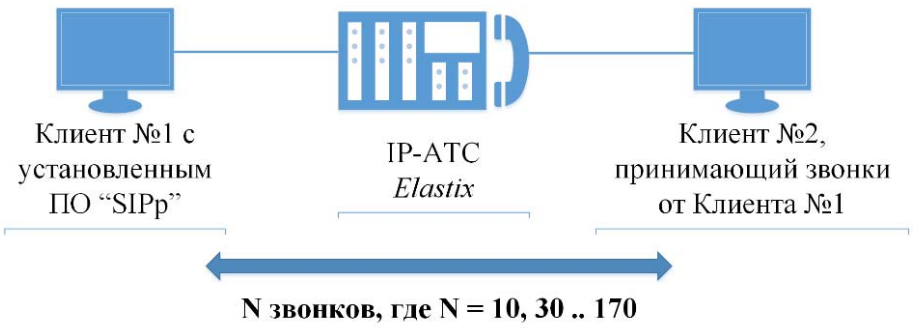


Рис. 1. Схема тестирования IP-АТС Elastix без использования протоколов ИБ

Конфигурация оборудования (виртуальной машины) для проведения тестов была выбрана следующая:

– 2-х ядерный процессор с частотой 4 ГГц;
– 1 Гбайт оперативной памяти.

Показания загруженности CPU/RAM снимались с использованием стандартного модуля мониторинга загруженности IP-АТС Elastix.

Исходя из полученных данных (табл., рис. 2), можно сделать следующие выводы. Загрузка оперативной памяти мало зависит от количества одновременных вызовов – она увеличивается на 1–2 % по сравнению с моментом, когда IP-АТС находится в состоянии покоя. Процент загрузки центрального процессора возрастает прямолинейно при увеличении числа одновременных вызовов. Также можно утверждать, что такая конфигурация оборудования вполне справится с задачами небольшого офиса.

ТАБЛИЦА. Результаты тестирования IP-АТС Elastix без использования протоколов ИБ

Количество одновременных звонков	10	30	50	70	90	110	130	150	170
Загрузка CPU, %	7	20	34	49	57	69	81	95	100
	6	22	35	44	58	68	82	91	99
	7	21	37	47	57	70	82	93	99
Загрузка RAM, %	48	48	48	48	49	49	49	49	49
	48	48	48	48	49	49	49	49	49
	48	48	48	49	49	49	49	49	49

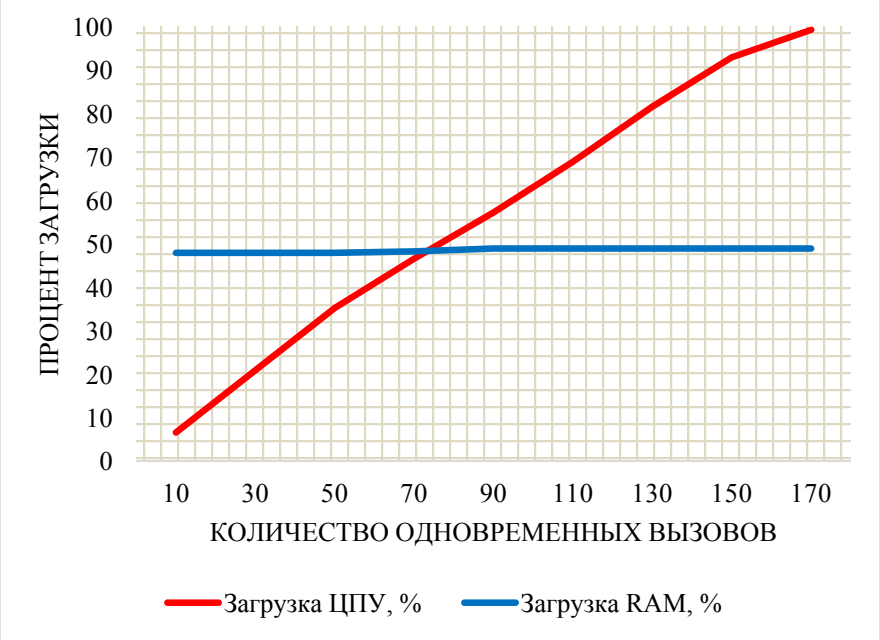


Рис. 2. Результаты тестирования IP-АТС Elastix без использования протоколов ИБ

Для реализации методики тестирования IP-АТС с использованием протоколов ИБ, возможно использовать следующие подходы:

– использование SIP-клиентов с поддержкой протоколов информационной безопасности и нескольких аккаунтов;

– использование нескольких Asterisk серверов для отработки так называемых «внешних» звонков;

– настройка обработки вызовов и их управления с помощью AGI (*Asterisk Gateway Interface*) скриптов, которые расширяют возможности администрирования сервера Asterisk;

– включение и использование различных сервисов – IVR, запись разговоров и т. д.

В статье были проанализированы существующие методы тестирования, их плюсы и минусы, а также представлены собственные решения по методике тестирования IP-АТС Elastix. В дальнейшем на основе разработанных методик планируется оценить зависимости параметров IP-АТС от количества одновременных вызовов и используемых сервисов и вывести аналитические выражение для подбора оптимальных характеристик оборудования для размещения сервера Asterisk.

Список используемых источников

1. Нагрузочное тестирование Астериск [Электронный ресурс] // Режим доступа: https://voxlink.ru/kb/asterisk-configuration/asterisk-test-sipp/

2. Нагрузочное тестирование IP-АТС Asterisk, установленной на сервере средней мощности [Электронный ресурс] // Режим доступа: https://medium.com/@softbcom

3. Производительность Asterisk систем [Электронный ресурс] // Режим доступа: http://asterisk.ru/knowledgebase

4. Ковцур М. Протоколы обеспечения безопасности IP-телефонии // Первая миля. 2012. Т. 32. № 5. С. 18–27.

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. 2015. № 1. С. 141–146

УДК 004.056

АНАЛИЗ СТОЙКОСТИ СПОСОБА АУТЕНТИФИКАЦИИ ДЛЯ ПРОТОКОЛА РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ НА ОСНОВЕ МАГНИТОМЕТРИЧЕСКИХ ДАННЫХ С ПОМОЩЬЮ ПРОГРАММЫ AVISPA

Е. О. Зуева, В. А. Яковлев

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

Проведен анализ протокола аутентификации ключа, распределяемого по алгоритму Диффи-Хеллмана, в основе которого лежит обмен между пользователями случайными данными, полученными от магнитомерических датчиков смартфонов. С помощью программы AVISPA, базирующейся на языке описания протоколов HLPSL (High Level Protocol Specification Language), проведена проверка данного способа на стойкость к различным видам атак. Построены интерактивные схемы, доказывающие его уязвимость к атаке «человек посередине».

AVISPA, HLPSL, «человек посередине».

Важным этапом анализа защищенных протоколов передачи данных является стадия оценки их безопасности, на которой проверяется стойкость протоколов к различным видам атакам. Известно большое число различных подходов к анализу уязвимости протоколов. Одним из них является использование программы AVISPA (*Automated Validation of Internet Security Protocols and Applications*), позволяющей не только находить уязвимости у того или иного протокола, но и определять возможные атаки на него [1].

Архитектура AVISPA допускает анализ протокола одним из четырех модулей: «OFMC», «CL-AtSe», «SATMC», «TA4SP» (рис. 1).

Каждый из модулей представляет собой уникальный верификатор, который может использоваться как самостоятельно, так и в сочетании с другими модулями. Модуль OFMC (*On-the-Fly Model-Checker*) является анализатором для проверки протокола методом «инертного злоумышленника» и используется в случаях, когда сообщения злоумышленника представлены выражениями с переменными, значения которых не фиксируются. Модуль CL-AtSe (*constraint-Logic-based Model-Searcher*) – программа верификации, основанная на логике ограничений, обязывающих нарушителя к выполнению определенных действий, которые могут быть эффективно использованы для нахождения атак на протоколы. Модуль SATMC (SAT-*based Model-Checker*) основан на методах теории решения задач планирования. А модуль TA4SP (*Tree Automata based on Automatic Approximations for the*

Analysis of Security Protocols) является инструментом доказательства свойств секретности протоколов безопасности и позволяет производить доказательства при неограниченном числе сессий на основе знаний нарушителя.

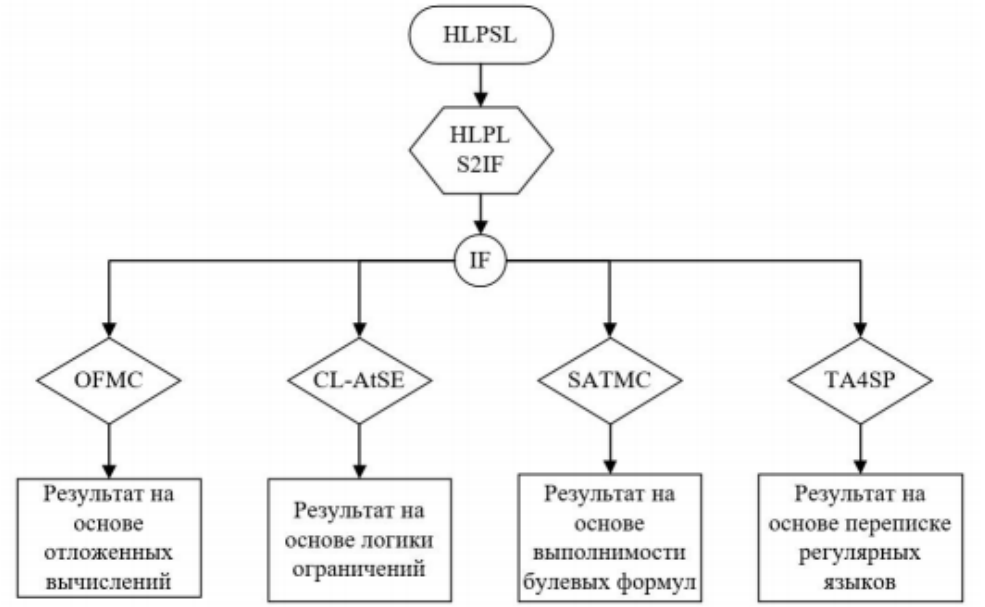


Рис. 1. Архитектура AVISPA

Спецификация анализируемого протокола, основанная на ролевом представлении, записывается на языке высокого уровня HLPSL (*High Level Protocol Specification Language*), который затем переводится в более низкоуровневый язык IF, что дает возможность более детально описывать протоколы по сравнению с аналогами. Результаты, полученные с помощью AVISPA, подробны и конструктивны.

Целью данной работы является анализ стойкости протокола MagPairing [2] аутентификации ключей, распределяемых между двумя пользователями по алгоритму Диффи-Хеллмана, при атаке «человек посередине». В основе протокола лежит обмен между пользователями случайными данными, полученными от магнитомерических датчиков смартфонов. Безопасность протокола основывается на разделении блока случайных данных на две части и поочередном обмене сначала первыми частями, а затем вторыми. Передаваемые части, предварительно шифруются на ключе Диффи-Хеллмана.

С помощью программы AVISPA спроектирована модель проверки протокола MagPairing в условиях активного перехвата.

Ниже представлено описание протокола на языке HLPSL:

```
// Начало протокола
    role role_A(A:agent, B:agent,C01:text,C02:text,C1:text;C2:text,SND,RCV:channel(dy))
```

```
        played_by A
        def=
                local
                        State:nat,D01:text,D1:text,D02:text;D2:text
                init
                        State:=0
                transition
                        1.State=0/\RCV(start)=|>State':=1/\SND(C01.C1)
                        2.State=1/\RCV(D01'.D1')=|>State':=2/\SND(C02.C2)
                        3.State=2/\RCV(D02'.D2')=|>State':=3
        end role
        role role_B(A:agent, B:agent,D01:text,D02:text,D1:text;D2:text,SND,RCV:channel(dy))
        played_by AB
        def=
                local
                        State:nat,C01:text,C1:text,C02:text;C2:text
                init
                        State:=0
                transition
                        1.State=0/\RCV(C01'.C1')=|>State':=1/\SND(D01.D1)
                        2.State=1/\RCV(C01'.C1')=|>State':=2/\SND(D02.D2)
        end role
        role session(C01:text,C02:text,C1:text;C2:text, A:agent, B:agent,D01:text,D02:text,D1:text;D2:text)
        def=
                local
                        SND2,RCV2,SND1,RCV1:channel(dy)
                composition
                         role_B(A,B,D01,D02,D1;D2,SND2,RCV2)/\role_A(A,B,C01,C02,C1;C2,SND1,RCV1)
        end role
        role environment()
        def=
                const
                        hash_0:hash_func,d01:text,d02:text,alice:agent,c1:text,c2:text,c01:text,c02:text,bob:
                 agent,d1:text,d2:text,aec_1:protocol_id
                intruder_knowledge={alice,bob,e01,e1}
                composition
                         session1(c2,c02,c1,c01,alice,bob,d01,d1,d02,d2)
        end role
        goal
                         secrecy_of sec_1
        end goal
        environment()
// Конец протокола
```

При компиляции кода, можно получить диаграмму передачи сообщений, которая наглядно описывает работу протокола MagPairing. Затем, запустив модуль верификации OFMC, в окне программы появляется диаграмма передачи сообщений при участии злоумышленника (рис. 2). В верхнем левом углу в поле «Incoming events» пользователю программы предложен список возможных для передачи между корреспондентами сообщений. Для установления алгоритма обмена данными, необходимо переместить выбранное для передачи сообщение в поле «Past events», после чего на схеме

появится изображение, указывающее направление передачи данного сообщения и его содержание. В нижнем левом углу представлены знания злоумышленника, которые он имел до начала сеанса передачи сообщения и после полного его завершения.

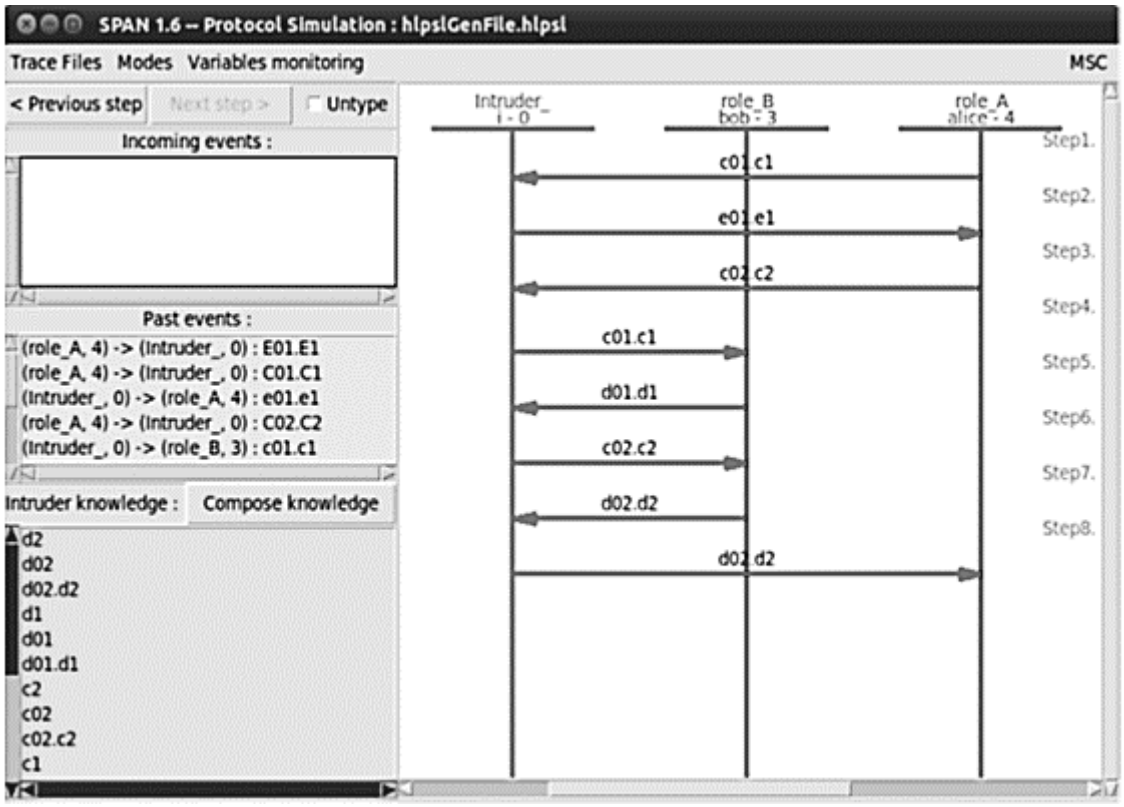


Рис. 2. Анализ MagPairing в программе AVISPA

В ходе анализа протокола MagPairing был определен порядок передачи сообщений, целью которого являлось получение злоумышленником данных одного легального корреспондента и передача их другому. Анализ показал, что, используя атаку «человек посередине», нарушитель может установить соединение с одним из корреспондентов, выдав себя за другого корреспондента.

Таким образом, с помощью программы AVISPA доказана уязвимость протокола MagPairing к атаке «человек посередине», что позволяет сделать вывод о недостаточной стойкости данного протокола аутентификации ключей. Этот же вывод подтверждается исследованиями, проведенными в [3], где на основе детального анализа всех этапов протокола MagPairing, показана его уязвимость к атаке нарушителя «человек посередине».

Список используемых источников

1. IST-2001-39252: AVISPA v1.1 User Manual, June 30, 2006.

2. Jin R., Shi L., Zeng K., Pande A., Mohapatra P. MagPairing: Pairing smartphones in close proximity using magnetometers // IEEE Transactions on information forensics and security, June 2016, pp. 1304–1319.

3. Зуева Е. О., Яковлев В. А. Анализ уязвимости протокола распределения ключей на основе магнитометрических данных «MagParing» // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VII Международная научно-техническая и научно-методическая конференция; сб. науч. ст. СПб. : СПбГУТ, 2018. С. 396–401.

УДК 004.056

АНАЛИЗ УЯЗВИМОСТИ ПРОТОКОЛА РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ НА ОСНОВЕ МАГНИТОМЕТРИЧЕСКИХ ДАННЫХ «MAGPARING»

Е. О. Зуева, В. А. Яковлев

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

Проведен анализ протокола аутентификации ключа (MagParing), распределяемого между двумя пользователями по методу Диффи-Хеллмана. В основе протокола лежит обмен между пользователями случайными данными, полученными от магнитомерических датчиков смартфонов. Безопасность протокола основывается на разделении блока случайных данных на две части и поочередном обмене сначала первыми частями, а затем вторыми. Передаваемые части, предварительно шифруются на ключе Диффи-Хеллмана. Показано, что данный протокол имеет уязвимости к атаке человек посредине на этапе синхронизации. Предложены пути повышения защищенности протокола.

мобильные устройства, аутентификация, магнитометрические данные.

Для распределения ключей к симметричным шифрам может быть использован протокол Диффи-Хеллмана [1]. Перед выполнением этого протокола пользователи, Алиса и Боб, согласуют общие параметры $\boldsymbol{p}$ и $\boldsymbol{g}$, где $\boldsymbol{p}$ – простое число, $\boldsymbol{g}$ – примитивный элемент конечного поля $GF(p)$. Далее выполняется протокол:

1. Алиса генерирует элемент $x \in (1, p - 1)$, вычисляет число $X = g^x (mod\ p)$ и посылает его Бобу.

2. Боб генерирует элемент $y \in (1, p - 1)$, вычисляет число $Y = g^y (mod\ p)$ и посылает его Алисе.

3. Алиса вычисляет значение $K = Y^x (mod\ p)$.

4. Боб вычисляет значение $K = X^y (mod\ p)$.

Из протокола легко видеть, что ключи, найденные Алисой и Бобом, равны:

$$K = g^{yx}(mod\ p) = g^{xy}(mod\ p).$$

Однако при таком обмене пользователи не могут достоверно определить, кем является их собеседник, так как данный протокол чувствителен к атаке «человек посередине». Поэтому для совместной работы Алисе и Бобу необходимо аутентифицировать ключи, сгенерированные по алгоритму Диффи-Хеллмана.

В [2] был предложен метод аутентификации ключей на основе показаний датчиков магнитометров, встроенных в смартфоны. Магнитометрические данные (последовательности) формируются, когда два мобильных устройства, оснащенные магнитными датчиками, удерживаются вблизи друг друга несколько секунд и формируют случайные последовательности достаточно сильно коррелированные друг с другом.

Во время обмена ключами по протоколу Диффи-Хеллмана, корреспонденты шифруют имеющиеся магнитометрические данные и обмениваются ими по открытому каналу. На принимающей стороне данные датчиков дешифруются, сравниваются с магнитометрическими данными собственных магнитометров, и корреспонденты аутентифицируют друг друга, если процент совпадения данных превышает установленный порог. Данный метод аутентификации получил название MagPairing. Проведем анализ протокола MagPairing.

Пусть последовательности магнитометрических данных M_A и M_B в смартфонах A и B соответственно.

Для создания общего секретного ключа пара корреспондентов выполняет следующий протокол обмена данными. Корреспонденты A и B формируют общий секретный ключ K по алгоритму Диффи-Хеллмана.

1. При соприкосновении устройств A и B генерируют строки $\boldsymbol{a}$ и $\boldsymbol{b}$, в которых показания датчиков магнитометра (M_A и M_B) конкатенируются с идентификаторами (ID) самих устройств.

2. Корреспонденты A и B генерируют случайные числа $\boldsymbol{c_0}$ и $\boldsymbol{d_0}$, названные стартовыми векторами.

3. Полученные в ходе соприкосновения устройств, строки данных $\boldsymbol{a}$ и $\boldsymbol{b}$, суммируются со стартовыми векторами. Результат суммирования шифруется по алгоритму AES на ключе K. Формируются криптограммы $\boldsymbol{c}$ и $\boldsymbol{d}$, соответственно: $\boldsymbol{c}$ = E(K, $\boldsymbol{c_0} \oplus$ a), $\boldsymbol{d}$ = E(K, $\boldsymbol{d_0} \oplus$ b).

4. Корреспондент A посылает корреспонденту B строку A1, состоящую из половины своего нешифрованного стартового вектора и половины криптограммы $\boldsymbol{c}$: A1 = $\boldsymbol{c_0}$[0, 63] | $\boldsymbol{c}$[0, 63].

5. Корреспондент *B*, не имеющий возможности дешифровать полученную строку, отправляет корреспонденту *A* строку B1 со своими значениями, построенными по тому же принципу: B1 = $\boldsymbol{d_0}$[0, 63] | $\boldsymbol{d}$[0, 63].

6. Корреспондент *A* также не может дешифровать данное сообщение. *A* отправляет *B* строку A2, состоящую из второй половины своего стартового вектора и второй половины криптограммы $\boldsymbol{c}$: A2 = $\boldsymbol{c_0}$[64, 127] | $\boldsymbol{c}$[64, 127].

7. Корреспондент *B* восстанавливает сообщения $\boldsymbol{c_0}$ и $\boldsymbol{c}$, объединяя первые и вторые части A1 и A2 соответственно: $\boldsymbol{c_0}$ = A1[0,63] | A2[0, 63] = = $\boldsymbol{c_0}$[0, 63] | $\boldsymbol{c_0}$[64, 127], $\boldsymbol{c}$ = A1[64, 127] | A2[64, 127] = $\boldsymbol{c}$[0, 63] | $\boldsymbol{c}$[64, 127].

8. Дешифруя $\boldsymbol{c}$, находит $\boldsymbol{a'}$ = D(K, $\boldsymbol{c}$)$\oplus\boldsymbol{c0}$ и вычисляет коэффициент корреляции между последовательностью $\boldsymbol{a'}$, полученной от *A*, и последовательностью $\boldsymbol{b}$, сформированной самим устройством *B*, по формуле:

$$R = 1 - \frac{1}{l} D(\boldsymbol{a}', \boldsymbol{b}),$$

где D – расстояние Хэмминга последовательностей $\boldsymbol{a'}$ и $\boldsymbol{b}$ длиной *l*. Если коэффициент $R(\boldsymbol{a'}, \boldsymbol{b}) < t$, где *t* заранее установленный порог, соединение прерывается, иначе корреспондент *B* подтверждает подлинность *A*.

Корреспондент *B* отправляет *A* строку B2, построенную аналогичным образом: B2 = $\boldsymbol{d_0}$[64, 127] | $\boldsymbol{d}$[64, 127].

9. Корреспондент *A* восстанавливает зашифрованное сообщение $\boldsymbol{d}$, дешифрует его и сравнивает полученное значение $\boldsymbol{b'}$ показаний датчика со своим значением $\boldsymbol{a}$.

10. Если коэффициент корреляции $R(\boldsymbol{a}, \boldsymbol{b'}) \geq t$, то сгенерированный по алгоритму Диффи-Хеллмана ключ аутентифицируется как подлинный, иначе соединение прерывается.

Стойкость протокола, по мнению авторов [1], основана на том, что сообщения $\boldsymbol{c_0}$ и $\boldsymbol{c}$ передаются не сразу, а равными частями. Половина зашифрованного сообщения не может быть расшифрована пока не будет получена вторая половина этого сообщения. А вторая половина не будет отправлена пока инициатор установления соединения не получит первую половину сообщений от ответчика $\boldsymbol{d_0}$ и $\boldsymbol{d}$.

Проведем анализ данного протокола к атаке «человек посредине», на основе детального анализе взаимодействия корреспондентов *A*, *B* и нарушителя *E* (рис.).

1. Корреспонденты *A* и *B*, подверженные атаке «человек посередине», формируют секретные ключи совместно с нарушителем *E* по алгоритму Диффи-Хеллмана.

2. Корреспонденты *A*, *B* и *E* генерируют строки, в которых показания датчиков магнитометра конкатенируются с идентификаторами самих устройств.

3. Корреспонденты *A*, *B* и *E* генерируют случайные стартовые векторы ($\boldsymbol{c_0}$, $\boldsymbol{d_0}$, $\boldsymbol{f_0}$, $\boldsymbol{h_0}$).

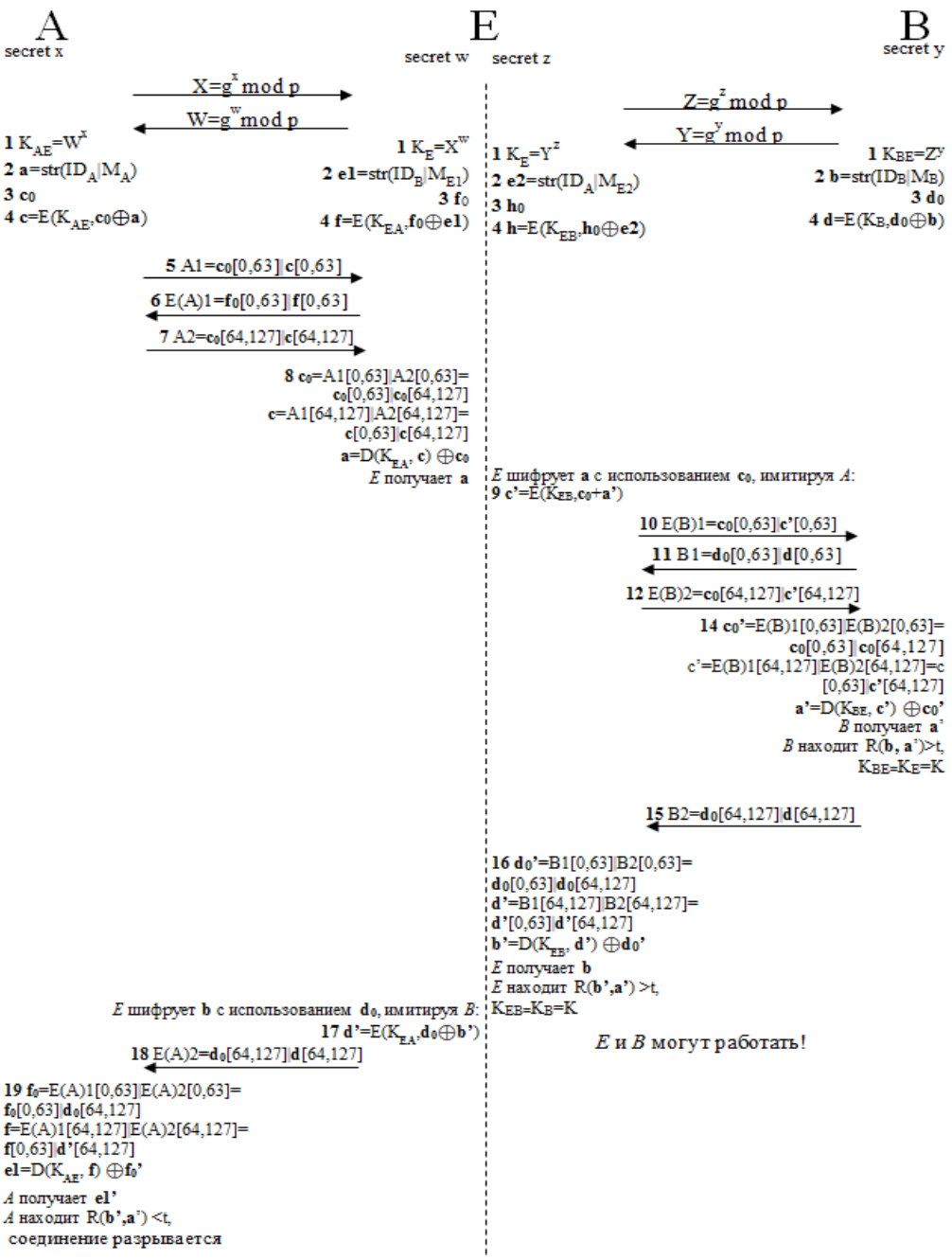


Рисунок. Протокол MagPairing в условиях активного перехвата

4. Строки данных, полученные после конкатенации, суммируются со стартовыми векторами. Результаты суммирования шифруются по алгоритму AES на ключах Диффи-Хеллмана $\boldsymbol{c} = E(K_{AE}, \boldsymbol{c_0} \oplus a)$.

5. Корреспондент *A*, посылает *E* строкуA1, состоящую из половины нешифрованного стартового вектора $\boldsymbol{c_0}$ и половины криптограммы $\boldsymbol{c}$: $A1 = \boldsymbol{c_0}[0, 63] \mid \boldsymbol{c}[0, 63]$.

6. Нарушитель *E* отправляет *A* строку E(A)1, содержащую половину своего стартового вектора $\boldsymbol{f_0}$ и половину криптограммы $\boldsymbol{f}$=E(K_{EA},$\boldsymbol{f_0}$⊕e1): E(A)1=$\boldsymbol{f_0}$[0,63]|$\boldsymbol{f}$[0,63].

7. Корреспондент *A* пока не может дешифровать сообщение, полученное от *E*. *A* отправляет *E* строку A2, состоящую из второй половины своего стартового вектора и криптограммы $\boldsymbol{c}$: A2 = $\boldsymbol{c_0}$[64, 127] | $\boldsymbol{c}$[64, 127].

8. Нарушитель *E* восстанавливает сообщения $\boldsymbol{c_0}$ и $\boldsymbol{c}$. Дешифрует $\boldsymbol{c}$ и вычисляет значение $\boldsymbol{a}$ показаний датчика магнитометра *A*.

9. Нарушитель *E* на основе полученных данных $\boldsymbol{a}$ и $\boldsymbol{c_0}$, формирует строку $\boldsymbol{c'}$ = E(K_{EB}, $\boldsymbol{c_0}$⊕a') с использованием ключа K_{EB}, сгенерированного совместно с устройством *B*.

10. Нарушитель *E*, отправляет корреспонденту *B* сообщение: E(B)1 = $\boldsymbol{c_0}$[0, 63] | $\boldsymbol{c'}$[0, 63], состоящее из первых частей блоков $\boldsymbol{c_0}$ и $\boldsymbol{c'}$.

11. Корреспондент *B*, не имея пока возможности дешифровать полученную строку, отправляет *E* строку B1 со своими значениями B1 = $\boldsymbol{d_0}$[0, 63] | $\boldsymbol{d}$[0, 63], построенными по тому же принципу, что и строка A1.

12. Нарушитель *E* отправляет *B* строку E(B)2, состоящую из второй половины стартового вектора *A* и второй половины блока $\boldsymbol{c'}$: E(B)1 = $\boldsymbol{c_0}$[64, 127] | $\boldsymbol{c'}$[64, 127].

13. Корреспондент *B* восстанавливает блоки $\boldsymbol{c_0}$ и $\boldsymbol{c'}$, дешифрует $\boldsymbol{c'}$ и вычисляет показания датчика магнитометра $\boldsymbol{a'}$ корреспондента *A*.

14. Корреспондент *B* находит коэффициент корреляции R($\boldsymbol{b}$, $\boldsymbol{a'}$). Так как нарушитель, обмениваясь сообщениями с корреспондентом *B* ретранслировал фактические значения показаний датчика магнитометра *A*, то с большой вероятностью R($\boldsymbol{b}$, $\boldsymbol{a'}$) ≥ t. Таким образом, *B* подтверждает подлинность корреспондента *A*. Но на самом деле он установил соединение с нарушителем *E*.

15. Корреспондент *B* отправляет *E* ответное сообщение: B2 = $\boldsymbol{d_0}$[64, 127] | $\boldsymbol{d}$[64, 127].

16. Нарушитель *E*. на основе полученных данных в сообщениях B1 и B2, формирует строки $\boldsymbol{d'}$ и $\boldsymbol{d_0}$. Дешифрует $\boldsymbol{d'}$ с использованием ключа K_{EB}, сгенерированного совместно с корреспондентом *B* и находит коэффициент корреляции R($\boldsymbol{a'}$, $\boldsymbol{b}$). Если магнитометрические данные *A* и *B* отличаются не сильно, то с большой вероятностью R($\boldsymbol{a'}$, $\boldsymbol{b}$) ≥ t. В результате *E* аутентифицировал корреспондента B, хотя последний считает, что он работает с *A*.

17. Нарушитель *E*, получив необходимые данные от устройства *B*, шифрует $\boldsymbol{b}$ с использованием $\boldsymbol{d_0}$.

18. *E* отправляет корреспонденту *A* сообщение: E(A)2 = $\boldsymbol{d_0}$[64, 127] | $\boldsymbol{d'}$[64, 127].

19. Корреспондент *A* восстанавливает блоки $\boldsymbol{f_0}$ и $\boldsymbol{f'}$, дешифрует $\boldsymbol{f'}$ и вычисляет показания датчика магнитометра $\boldsymbol{e1'}$ нарушителя *E*, предполагая,

что это *B*. *A* сравнивает данные, полученные от *E*, со своими данными. Так как нарушитель, использовал ложные значения показаний датчика магнитометра ***e1***, то вычисленный *A* коэффициент корреляции R(***a, e1'***) < t. Соединение между *A* и *E* прерывается.

Анализ протокола показывает, что, используя атаку «человек посередине», нарушитель может установить соединение с одним из корреспондентов, выдав себя за другого корреспондента. Что позволяет сделать вывод о недостаточной стойкости протокола MagPairing для аутентификации ключей, распределяемых по протоколу Диффи-Хэллмана. В связи с этим является актуальной разработка протокола, устойчивого к подобного рода атакам нарушителя.

Список используемых источников

1. Коржик В. И., Яковлев В. А. Основы криптографии. СПб. : Интермедиа. 2016. 276 с.

2. Jin R., Shi L., Zeng K., Pande A., Mohapatra P. MagPairing: Pairing smartphones in close proximity using magnetometers // IEEE Transactions on information forensics and security, June 2016, pp. 1304–1319.

УДК 004.056

РАЗРАБОТКА СПОСОБА ПОМЕХОУСТОЙЧИВОЙ АУТЕНТИФИКАЦИИ ДЛЯ ПРОТОКОЛА РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ ДИФФИ-ХЕЛЛМАНА НА ОСНОВЕ МАГНИТОМЕТРИЧЕСКИХ ДАННЫХ

Е. О. Зуева, В. А. Яковлев

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

Предложен способ аутентификации ключа, распределяемого по методу Диффи-Хеллмана. Способ основывается на формировании аутентификаторов для ключа, из случайных последовательностей, генерируемых магнитометрами смартфонов и использовании помехоустойчивого кода. Проведен анализ протокола к атаке человек посередине. Получены оценки вероятности ложного обнаружения навязывания и вероятности навязывания в зависимости от коэффициента несовпадения магнитометрических данных у взаимодействующих пользователей.

аутентификация, магнитометрические данные, протокол Диффи-Хеллмана, АП-коды.

В [1] был проведен анализ способов обеспечения ключами мобильных устройств (смартфонов) для осуществления конфиденциальной связи между корреспондентами. Показано, что перспективным подходом является применение протокола Диффи-Хеллмана при условии аутентификации данных, которыми обмениваются корреспонденты. Для аутентификации целесообразно использовать дополнительные последовательности, генерируемые корреспондентами на основе данных, полученных от магнитометров, встроенных в смартфоны, при близком их взаимном расположении. Протокол формирования ключа таким способом предложен в [2] и назван MagPairing. В [3] проведен анализ стойкости такого протокола в условиях активного нарушителя, осуществляющего атаку «человек посередине», и показано, что данный протокол не является стойким.

В данной статье предлагается способ аутентификации для протокола Диффи-Хеллмана на основе магнитометрических данных, с использованием аутентифицирующих помехоустойчивых кодов (АП-кодов). Такой способ был впервые предложен в [4] и подробно исследован в [5].

Предположим, что два корреспондента А и В, связаны каналом связи без ошибок и имеют предварительно сформированные двоичные последовательности $\boldsymbol{a}$ и $\boldsymbol{b}$ соответственно, такие, что $p(\boldsymbol{a}_i \neq \boldsymbol{b}_i) = p_m$, $\boldsymbol{i} = 1, 2\ldots$

Для построения АП-кода, корреспонденты A и B заранее договариваются об использовании некоторого (n_a, k_a) – помехоустойчивого систематического кода V и договариваются о порядке сопоставления каждому сообщению $\boldsymbol{m_i}$ кодового слова $\boldsymbol{v_i} \in \boldsymbol{V}$.

Если корреспондент A намерен передать сообщение $\boldsymbol{m_i}$ корреспонденту B, он выбирает кодовое слово $\boldsymbol{v_i} = (\boldsymbol{v_{i1}}, \boldsymbol{v_{i2}}, \ldots, \boldsymbol{v_{ina}})$ кода $\boldsymbol{V}$, $\boldsymbol{v_{ij}} \in (0,1)$ и формирует аутентификатор $\boldsymbol{w_i} = = (\boldsymbol{w_{i1}}, \boldsymbol{w_{i2}}, \ldots, \boldsymbol{w_{i\tau}})$, используя имеющуюся у него аутентифицирующую последовательность $\boldsymbol{a}$ следующим образом. Для всех $j < n_a$, $\boldsymbol{w_{ij}} = \boldsymbol{a_j}$, если $\boldsymbol{v_{ij}} = \mathbf{1}$, в противном случае $\boldsymbol{w_{ij}}$ не формируется. Далее сообщение $\boldsymbol{m_i}$ и аутентификатор $\boldsymbol{w_i}$ передаются по открытому каналу корреспонденту B. Очевидно, что длина τ аутентификатора $\boldsymbol{w_i}$ равна весу кодового слова $\boldsymbol{v_i}$.

Корреспондент B, приняв $(\boldsymbol{m_i}, \boldsymbol{w_i})$, формирует $\boldsymbol{w_i'}$, используя для этого принятое сообщение $\boldsymbol{m_i}$ и аутентифицирующую последовательность $\boldsymbol{b}$, аналогично тому, как это делал корреспондент A. Далее он выполняет сравнение аутентификаторов $\boldsymbol{w_i}$ и $\boldsymbol{w_i'}$. Если число совпадений в $\boldsymbol{w_i}$ и $\boldsymbol{w_i'}$ равно или больше некоторого порога Δ_w, то сообщение $\boldsymbol{m_i}$ считается подлинным, если меньше, сообщение $\boldsymbol{m_i}$ отвергается как ложное.

В [5] показано, что устойчивость к навязыванию ложных сообщений зависит от так называемого асимметричного кодового расстояния $\boldsymbol{d_{01}}$, которое определяется числом переходов из 0 в 1 между кодовыми словами, соответствующими истинному $\boldsymbol{m_i}$ и ложному $\boldsymbol{m_f}$ сообщениям.

Нахождение асимметричного кодового расстояния – сложная задача. Простой, но не слишком экономичный способ построения (n_a, k_a) кода с известным $\boldsymbol{d_{01}}$ предложен в [4], и заключается в следующем.

Выберем некоторый (n, k) – код с известным минимальным расстоянием $\boldsymbol{d}$. Заменим в каждом кодовом слове символ 1 на 10, а символ 0 на 01, получим (n_a, k_a) – код с параметрами:

$$n_a = 2n,\ k_a = k,\ d_{01} = d,\ \tau = n. \quad (1)$$

Основными характеристиками АП-кода являются:

P_f – вероятность ложного отклонения переданного сообщения, когда нарушитель не вмешивался в процесс передачи.

P_d – вероятность успешного навязывания ложного сообщения. В [5] получены следующие соотношения для P_f и P_d.

$$P_f = \sum_{i=\Delta_w+1}^{2n_0} C_{2n_0}^i p_m^i (1-p_m)^{2n_0-i}, \quad (2)$$

$$P_d = \sum_{i=0}^{\Delta_w} C_d^i p_w^i (1-p_w)^{d-i} * \sum_{j=0}^{\Delta_w - i} C_{2n_0-d}^j p_m^j (1-p_m)^{2n_0-d-j}, \quad (3)$$

где $p_m = p(\boldsymbol{a}_i \neq \boldsymbol{b}_i)$ – вероятность несовпадения бит в аутентифицирующих последовательностях $\boldsymbol{a}$ и $\boldsymbol{b}$; $p_w = p(\boldsymbol{a}_i \neq \boldsymbol{e}_i)$ – вероятность несовпадения бит в последовательности $\boldsymbol{a}$ и $\boldsymbol{e}$, где $\boldsymbol{e}$ – аутентифицирующая последовательность у нарушителя. В нашем случае $p_w = 1/2$, поскольку при формировании магнитометрических данных смартфоны законных пользователей находятся рядом, а смартфон постороннего пользователя естественно удален от них.

При выбранных k и n параметр d может быть найден, с использованием границы Варшамова-Гильберта [6]:

$$\frac{k}{n} \geq 1 - g\left(\frac{d}{n}\right), \quad (4)$$

где $g(x) = -xlogx - (1-x)\log(1-x)$ – энтропийная функция.

Рассмотрим далее применение АП-кода для аутентификации данных в протоколе формирования ключа Диффи-Хеллмана на основе последовательностей $\boldsymbol{a}$ и $\boldsymbol{b}$, полученных от магнитометров смартфонов при их сближении друг с другом при встрече корреспондентов A и B друг с другом.

Протокол DH описан в [1]. Рассмотрим следующий протокол аутентификации.

1. Корреспондент A формирует значение Диффи-Хеллмана $DH_A = \boldsymbol{\alpha}^x$. Это значение может быть представлено в виде двоичной последовательности длиной L бит. Последовательность разделяется на N подблоков длиной k бит каждый.

2. Используя свои магнитометрические данные (последовательность $\boldsymbol{a}$), корреспондент А формирует аутентификатор $\boldsymbol{w_{Ai}}$ длиной n бит на основе АП-кода с параметрами ($2n$, k, d) для i-го подблока, $i = 1, 2, ..., N$.

Заметим, что для формирования очередного аутентификатора используется новая часть последовательности ***a.***

3. Значение DH_A и аутентификаторы $\boldsymbol{w_{Ai}}$, передаются корреспонденту *B*.

4. Корреспондент *B*, получив DH_A и используя свои магнитометрические данные (последовательность ***b***), формирует местные аутентификаторы $\boldsymbol{w'_{Ai}}$ и сравнивает их с аутентификаторами $\boldsymbol{w_{Ai}}$, полученными от корреспондента *A* в порядке их поступления. Если число несовпадений символов для пары аутентификаторов $|\boldsymbol{w_{Ai}} \oplus \boldsymbol{w'_{Ai}}|$ меньше некоторого порога Δ, подблок признается подлинным.

После этого аналогичным порядком проводится аутентификация значения Диффи-Хеллмана DH_B, передаваемого от *B* к *A*.

Значения Диффи-Хеллмана *DH* каждого корреспондента признаются подлинными в целом, если число несовпадений бит в каждом принятом аутентификаторе не больше порогового значения Δ.

Если значение *DH* обоими корреспондентами признаны подлинными, то корреспонденты *A* и *B* формируют общий ключ по способу Диффи-Хеллмана, то есть

$$K = (DH_B)^x = (DH_A)^y$$

Вероятность ложного отклонения значения *DH* корреспондентом имеет место, если произойдет ложное отклонение, хотя бы одного подблока.

Можно записать:

$$P_f(DH) = 1 - (1 - P_f)^N \quad (5)$$

Ложная аутентификация, то есть навязывание нарушителем ложного значения Диффи-Хеллмана, будет иметь место, если будут успешно навязаны все *N* подблоков с соответствующими им аутентификаторами. Вероятность этого события:

$$P_d(DH) = (P_d)^N \quad (6)$$

Рассмотрим сначала частный случай применения АП-кода, когда $k = L$, то есть значение *DH* аутентифицируется целиком одним аутентификатором.

Используя (2), (3) построим зависимости $P_f = g(\Delta)$ и $P_d = t(\Delta)$ для разных значений p_m (рис.) и параметрах АП-кода: (128, 32, 28).

Видим, что P_f убывает при уменьшении p_m. Выбирая значение порога Δ можно обеспечить требуемую величину вероятности ложного отклонения P_f. Используя это значение порога, получаем значение P_d.

В таблице показаны значения $P_f, P_d, P_f\,(DH)$, $P_d(DH)$ для различных значений параметров аутентифицирующих кодов при p_m= 0,01 и R = 0,25 и длине значения *DH* = 256 бит.

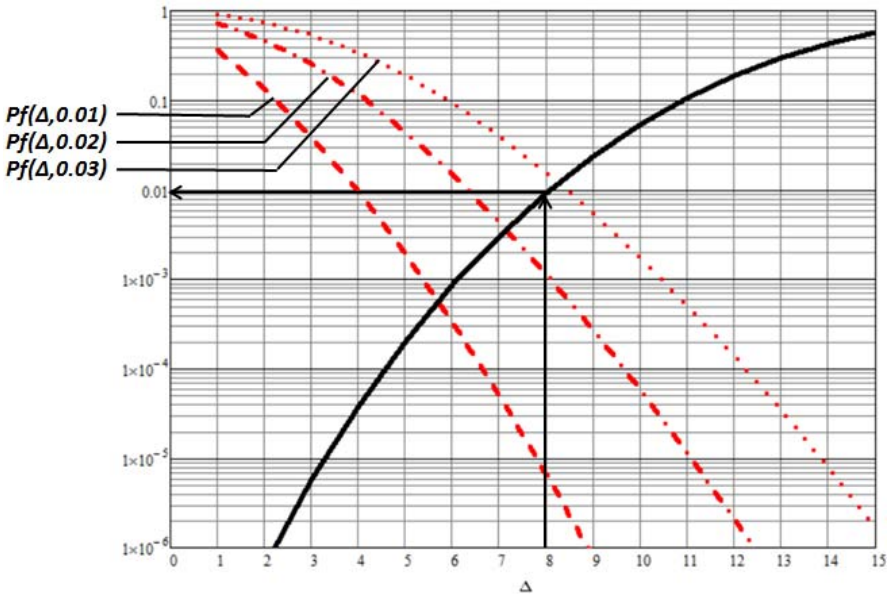


Рисунок. Зависимости P_f, P_d от порога Δ при разных значениях вероятности несовпадения аутентифицирующих последовательностей

Видим, что, используя код (64, 16) можно получить достаточно малые значения $P_f\,(DH)$ и $P_d(DH)$ при невысокой сложности схемы кодирования и скорости $R = 0{,}25$. Длина аутентифицирующей последовательности равна $2Nn = 2L / R = 2048$ бит.

ТАБЛИЦА. Вероятности $P_f, P_d, P_f\,(DH)$, $P_d(DH)$ для разных значений параметров аутентифицирующих кодов со скоростью $R = 0{,}25$

Код	32,8	64,16	128,32	256,64	512,128
P_f	$3{,}125\times10^{-7}$	$6{,}25\times10^{-7}$	$1{,}25\times10^{-6}$	$2{,}5\times10^{-6}$	5×10^{-6}
P_d	1	0,5	0,02	10^{-5}	5×10^{-15}
$P_f(DH)$	10^{-5}	10^{-5}	10^{-5}	10^{-5}	10^{-5}
$P_d(DH)$	1	$1{,}526\times10^{-5}$	$2{,}56\times10^{-14}$	10^{-20}	$6{,}25\times10^{-28}$

Выбор наилучшего кода представляет самостоятельную научную задачу, которая может быть сформулирована следующим образом.

Заданы:

– длина значения DH – n_0;

– допустимая вероятность ложного отклонения $P_f^{\text{доп}}(DH)$;

– допустимая вероятность навязывания $P_d^{\text{доп}}(DH)$;

– вероятность несовпадения бит в аутентифицирующих последовательностях p_m.

Требуется выбрать:

параметры АП-кода: (n_a, k_a, d_{01}); порог системы аутентификации Δ; при которых минимизируется длина аутентифицирующей последовательности и выполняются требования: $P_f(DH) \le P_f^{\text{доп}}(DH)$, $P_d(DH) \le P_d^{\text{доп}}(DH)$.

Эту задачу авторы предполагают решить в ходе дальнейших исследований.

Список используемых источников

1. Зуева Е. О., Яковлев В. А. Анализ способов формирования общего ключа для сопряжения мобильных устройств // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VI Международная научно-техническая и научно-методическая конференция; сб. науч. ст. СПб. : СПбГУТ, 2017. Т. 2. С. 348–353.

2. Jin R., Shi L., Zeng K., Pande A., Mohapatra P. MagPairing: Pairing smartphones in close proximity using magnetometers // IEEE Transactions on information forensics and security, June 2016, pp. 1304–1319.

3. Зуева Е. О., Яковлев В. А. Анализ уязвимости протокола распределения ключей на основе магнитометрических данных «Magparing» // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VII Международная научно-техническая и научно-методическая конференция; сб. науч. ст. СПб. : СПбГУТ, 2018. С. 392–401.

4. Maurer U. Information-theoretically secure secret-key agreement by not authenticated public discussion. Lecture Notes in Computer Science 1233, 1997, pp. 209–223.

5. Korzhik V., Yakovlev V., Gullermo Morales-Luna, Chesnokov R. Performance Evaluation of Keyless Authentication Based on Noisy Channel // Communications in Computer and Information Science. 2007. Т. 1. PP. 115–126.

6. Питерсон У., Уэлдон Э. Коды, исправляющие ошибки. М. : Мир. 1976. 593 с.

УДК 004.042

ПЕРСПЕКТИВЫ ПРИМЕНЕНИЯ МАТЕМАТИЧЕСКИХ МЕТОДОВ ПРОГНОЗИРОВАНИЯ В СИСТЕМАХ МОНИТОРИНГА ЛОКАЛЬНО-ВЫЧИСЛИТЕЛЬНЫХ СЕТЕЙ

В. Г. Иванов, Д. Д. Корякин

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

Актуальной проблемой функционирования информационно-телекоммуникационных сетей специального назначения остается вопрос мониторинга как компонентов сетей, так и отдельных ее элементов. Перспективным методом обработки данных в настоящий момент является метод Хольта-Винтерса, анализу которого посвящена данная статья.

инфотелекоммуникационные сети, метод Хольта-Винтерса.

В классическом представлении система мониторинга представляет собой многокомпонентную систему, представленную системами сбора данных, хранения и анализа (с использованием различных математических методов) ключевых параметров данных и использования результатов анализа, как критерия формирования оценки функционирования элемента сети или сети в целом [1].

Решая вопросы контроля и управления инфотелекоммуникационной сетью необходимо выбрать эффективные математические методы, позволяющие реализовать процедуры получения и обработки данных в соответствии с заданными требованиями. Получаемые данные от контролируемых элементов чаще всего будут являться случайными величинами или случайными процессами, имеющими тем не менее граничные значения. Для оценки значений данных величин целесообразно применять методы математической статистики, в частности получения значений математического ожидания и дисперсии. При этом не следует пренебрегать статистической связью между случайными параметрами, характеризующими работу контролируемых элементов.

Случайные значения получаемых контрольных величин можно представить в виде последовательности временных рядов. Оценивая временной ряд методом сравнения получаемых данных с минимальными и максимальными пороговыми значениями, мы сталкиваемся с проблемой невозможности обнаружения изменений в течении времени, что не позволяет обнаруживать сбои системы с достаточной степенью надежности. Возникает проблема возникновения «ложных» сбоев, за счет некоторой вероятности мгновенно выхода контролируемых параметров за пределы пороговых значений [2].

Логичным способом работы с временными рядами видится использование математических методов прогнозирования. При этоv следует рассматривать методы краткосрочных прогнозов, поскольку долгосрочное прогнозирование не имеет практического смысла применительно к инфотелекоммуникационным сетям.

В связи с этим рассмотрим возможность использования методов экспоненциального сглаживания временных рядов, обеспечивающих наглядное представления о тренде и позволяющих делать краткосрочные прогнозы.

Одним из перспективных методов является метод Хольта-Винтерса, который выгодно отличается от обычного экспоненциального сглаживания способностью обнаруживать тренды, относящиеся к коротким промежуткам времени, непосредственно предшествующим прогнозным, и проводить экстраполяцию данных трендов на предстоящие временные значения [2, 3].

При использовании метода необходимо последовательно вычислять сглаженные значения ряда и значение тренда, накопленное в любой точке ряда.

$$E_i = U(E_{i-1} + T_{i-1}) + (1-U)Y_i;$$
$$T_i = V \cdot T_{i-1} + (1-V) \cdot (E_i - E_{i-1}),$$

где через $\boldsymbol{E}$ и $\boldsymbol{T}$ обозначены сглаженное значение ряда и тренд, рассчитываемые по всем точкам ряда, а $\boldsymbol{U}$ и $\boldsymbol{V}$ – константы сглаживания, относящиеся к оценкам уровня и тренда соответственно. Выбор значений этих констант опять-таки является крайне субъективным. Из приведенных уравнений метода следует, что значения $\boldsymbol{U}$ и $\boldsymbol{V}$ могут находится в интервале **(0..1)**, но чаще всего исследователь выбирает их значения из более узкого диапазона $\mathbf{[0{,}25 < U,\ V < 0{,}5]}$ и при этом значения констант не обязаны совпадать. Лучше всего, если нет специальных соображений, начать моделирование с $\boldsymbol{U = V = 0{,}3}$, а затем по необходимости их несколько варьировать. При более высоких значениях $\boldsymbol{U}$ в большей степени учитываются прошлые значения ряда и тенденция развития процесса, чем мгновенные; аналогично более высокие значения $\boldsymbol{V}$ переоценивают прошлое движение процесса по сравнению с современным [4].

В первой точке ряда значения $\boldsymbol{E_1}$ и $\boldsymbol{T_1}$ не рассчитываются, для их расчета не существует предшествующих экспериментальных значений. Во второй точке ряда принимается, что сглаженное значение $\boldsymbol{E_2}$ в точности равно наблюдаемому $\boldsymbol{Y_2}$, а микротренд за этот период считается линейным и рассчитывается как разность между текущим и прошлым значениями отклика $\boldsymbol{T_2 = Y_2 - Y_1}$. Начиная с третьей точки уже можно пользоваться указанными выше формулами: вначале рассчитывается сглаженное значение $\boldsymbol{E_3}$ по сглаженному значению и микротренду для прошлой точки ряда и отклику для текущей точки, а затем рассчитывается новый микротренд по своему предшествующему значению и разности между прошлым и только что оцененным сглаженным значением. Затем описанная процедура повторяется по всем последующим точкам временного ряда.

При расчете прогноза в методе Хольта-Винтерса предполагается, что сглаженное значение в последней точке является опорным, а определенный для нее микротренд сохранит свое значение и в будущем; функция прогноза оказывается линейной, и тогда:

$$\hat{Y}_{n-1} = E_n + i \cdot T_n,$$

где $\boldsymbol{j}$ – номер периода в будущем, на который рассчитывается прогноз. Микротренд, выступающий в функции прогноза в качестве коэффициента пропорциональности, не сможет сохранить свою оценку на значительный период времени в будущем, но уж во всяком случае за 4–5 периодов он не сможет значительно измениться, и мы получим достоверный прогноз.

Использование методов прогнозирования в системах мониторинга позволяет повысить критерии надежности и устойчивости функционирования инфотелекоммуникационной сети за счет уменьшения количества ложных срабатывания и более подробной оценки поступающих контрольных данных без учета вероятности мгновенных выбросов значений. Анализ систематических аберраций позволяет не формировать требования системы по четкому определению критериев для определения внештатных ситуаций, что, в перспективе, позволяет снизить время реакции на возникающий системные сбои. Данный метод можно применять для любых временных рядов с некой прогнозируемой цикличностью значений.

К недостаткам данного метода можно отнести длительную реакцию системы мониторинга на внештатные ситуации в условиях недостаточных данных для формирования трендов (например, на начальном этапе эксплуатации).

Список используемых источников

1. Ушаков И. А. Вероятностные модели надежности информационно-вычислительных систем. М. : Радио и связь, 1991. 132 с. ISBN 5-256-00795-5.

2. Abberant Behaviour Detection in Time Series for Network Monitoring [Электронный ресурс] // Режим доступа: http://www.usenix.org/events/lisa00/full_papers/brutlag/brutlag_html, свободный (дата обращения 22.03.18)

3. Исхаков С. Ю., Шелупанов А. А. Разработка структуры системы управления сетью // Доклады ТУСУРа. 2011. № 2 (24). Ч. 2. С. 259–262.

4. Бешелев С. Д., Гуревич Ф. Г. Математико-статистические методы экспертных оценок. М. : Статистика, 1980. 349 с.

УДК 621.39/621.316.5

ТРЕБОВАНИЯ К ХАРАКТЕРИСТИКАМ МЕЖДОМЕННЫХ ОПТИЧЕСКИХ ИНТЕРФЕЙСОВ СОВРЕМЕННЫХ ЦИФРОВЫХ ТРАНСПОРТНЫХ СЕТЕЙ

В. С. Иванов, Б. К. Никитин, А. Н. Сергеев

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

Постоянный рост объёмов передаваемой информации приводит к необходимости ужесточения требований к характеристикам всех компонентов сети, принимающих участие в передаче сигналов. Ввиду того, что параметры каждого из компонентов имеют свои случайные отклонения от номинальных значений, необходимо выработать

и в процессе эксплуатации постоянно совершенствовать общие нормы и правила работы сетей в целом. Для этого нужно задать требования к характеристикам интерфейсов сетей и поддерживать их в точках нормирования.

транспортная сеть, оптический интерфейс, нормирование, оптический сетевой элемент, эталонная точка.

При проектировании современных волоконно-оптических линий передачи необходимо учитывать факторы, ограничивающие время распространения сигнала вдоль среды передачи до другого конца линии, с последующим уменьшением их влияния. В случае эксплуатации систем передачи происходит естественная деградация их отдельных компонентов, а сама линия будет подвергаться воздействию внешних и внутренних естественных и искусственных разрушающих воздействий, которые могут иметь кратковременный или продолжительный характер. Отсюда возникает необходимость нормирования состояния параметров оптического тракта, которое задаёт пределы ухудшения его технических характеристик при проектировании, строительстве и последующей эксплуатации.

В оптической транспортной сети (OTN) интерфейсы IrDI предоставляются однонаправленными, двухточечными, одноканальными и многоканальными линейными системами. Их основная цель заключается в обеспечении возможности поперечно совместимых интерфейсов для пересечения границы между двумя административными доменами. Спецификации IrDI включают внутриофисные приложения, приложения связи на близкие расстояния и приложения дальней связи без линейных усилителей. В данном докладе приводятся требования лишь к междоменным интерфейсам [1].

Оптическая транспортная сеть (*Optical Transport Network,* OTN) – это набор оптических сетевых элементов (*Optical Network Element,* ONE), соединенных оптоволоконными линиями. Такая сеть обеспечивает доставку информационных сигналов по заданному адресу. Она разделяется на ряд подсетей, отличающихся как по форме принадлежности к конкретному оператору, так и по технологии, используемой в данной подсети. Основная сеть, имеющее название Core Network, – это сеть, обеспечивающая взаимодействие периферийных сетей. Таким образом, OTN обеспечивает функции передачи, мультиплексирования, маршрутизации, автоматического обслуживания и живучести. Оптические каналы и сети OTN несут сигналы любого формата независимо от их специфики (например, STM, ATM, IP). Такие сети могут быть как одноканальными, так и многоканальными (WDM) [2].

Универсальные эталонные точки в OTN изображены на рис. [3].

Эталонные точки на рисунке определены следующим образом:

− MPI-S – (одноканальная) эталонная точка сразу после выходных оптических разъемов трибютарного интерфейса каждого оптического сетевого элемента;

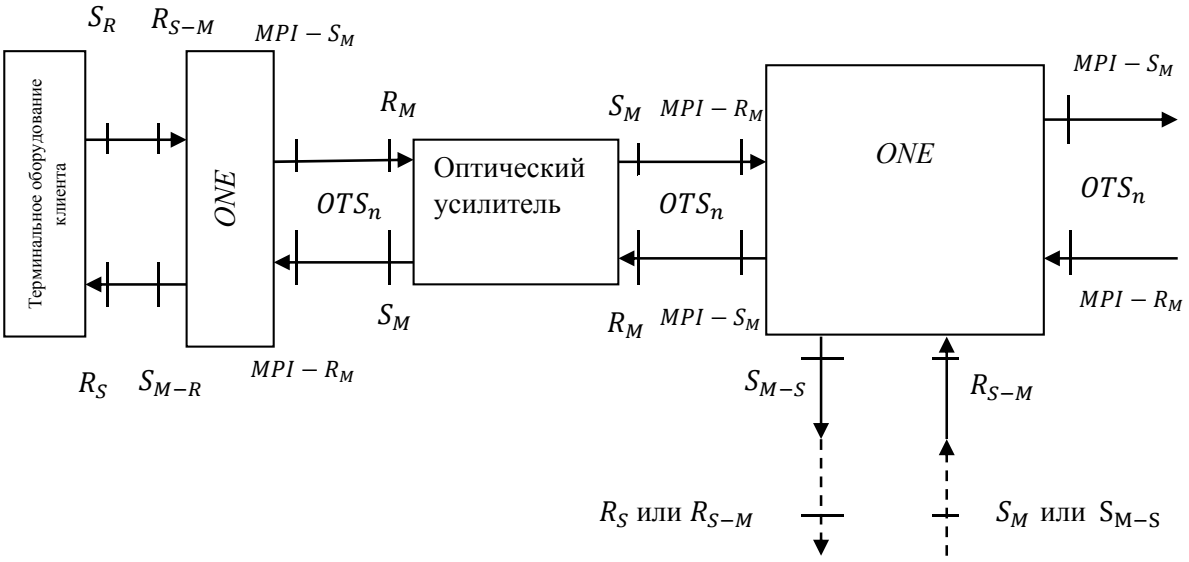


Рисунок. Универсальные эталонные точки в оптической транспортной сети

− MPI-R – (одноканальная) эталонная точка в оптическом волокне непосредственно перед входным оптическим разъемом трибютарного интерфейса каждого оптического сетевого элемента;

– MPI-S_M – (многоканальная) эталонная точка в оптическом волокне сразу после выходного оптического разъема транспортного интерфейса оптического сетевого элемента;

− MPI-R_M – (многоканальная) эталонная точка в оптическом волокне непосредственно перед входным оптическим разъемом транспортного интерфейса оптического сетевого элемента.

Характеристики сетей организованы согласно прикладным кодам, которые учитывают множество возможных комбинаций числа каналов, типов оптических трибутарных сигналов, расстояний, типов волокон и конфигураций систем. Спецификации одноканальных междоменных интерфейсов предоставляются по следующим характеристикам: скоростям передачи в канале, соответствующим классам NRZ 2.5G, NRZ 10G и NRZ 40G для передачи внутри офиса, на малые расстояния и при дальней связи и однонаправленной передаче. Ожидается также разработка характеристик одноканальных IrDI со скоростью передачи и линейного кодирования класса RZ 40G.

В случае одноканальных систем нормирование осуществляется по следующим критериям:

А. Параметры передатчика:

1. Рабочий диапазон длин волн, внутри которого система не выходит за предельные значения.

2. Максимальная и минимальная средняя излучаемая мощность (в точке MPI-S).

3. Минимальный коэффициент потерь.

В ближайшем будущем к вышеперечисленным параметрам передатчика добавятся:

– максимальная ширина спектра по уровню –20 дБм;

– параметр линейной частотной модуляции α;

– максимальная спектральная плотность мощности мВт/10МГц;

– минимальный коэффициент подавления боковой моды.

Б. Параметры оптического линейного тракта MPI-S – MPI-R:

1. Диапазон максимального и минимального ослабления.

2. Максимальная и минимальная накопленная хроматическая дисперсия.

3. Максимальное ДГВЗ.

4. Минимальные оптические потери на отражение кабеля в точке MPI-S, включая все соединительные элементы.

5. Максимальное дискретное отражение между точками MPI-S и MPI-R.

В. Параметры приемника:

1. Минимальная чувствительность при КОБ = $1*10^{-12}$.

2. Максимальная перегрузка.

3. Максимальные потери оптического пути.

4. Максимальное отражение приёмника, измеренное в точке MPI-R.

Кроме этого для хорошей работы системы необходимо знать и учитывать:

– отношение оптических сигнал/шум в точках MPI-S и S′. Отношение оптических сигнал/шум на передаче определяется как отношение средней мощности оптического сигнала к средней мощности оптического шума на передаче в точке MPI-S в полосе частот 1 нм рабочего диапазона длин волн;

– поляризационно-модовую дисперсию на участке ЭКУ, которая определяется как допустимое значение разности времен распространения двух взаимоперпендикулярных поляризационных составляющих моды оптического сигнала.

В случае многоканальных приложений (WDM) к вышеперечисленным параметрам добавляются еще несколько, таких как:

– отношение оптических сигнал/шум в каждом оптическом канале в точках *MPI-*S_m и и S_m;

– суммарная мощность оптического излучения в точках *MPI-*S_m и S_m, *MPI-*R_m и R_m;

– перекрываемое затухание между точками *MPI-*S_m и *MPI-*R_m, *MPI-*S_m и R_m, и S_m и R_m, и S_m и *MPI-*R_m (в пределах одного ЭКУ);

– суммарная дисперсия между точками *MPI-*S_m и *MPI-*R_m, *MPI-*S_m и R_m, и S_m и R_m, и S_m и *MPI-*R_m (в пределах одного ЭКУ);

– оптическая переходная помеха между оптическими каналами в точках *MPI-*S_m и *MPI-*R_m;

– максимум различия мощности в оптических каналах в точках *MPI-*S_m и и S_m, *MPI-*R_m и R_m.

К нормируемым параметрам оптического стыка на передаче для каждого i-го канала (i = 1, ..., n) дополнительно относятся:

- центральная частота (длина волны) оптического канала;
- расстояние между оптическими каналами;
- отклонение центральной частоты оптического канала;
- ширина линии излучения лазера.

Технические требования к параметрам оптических стыков в точках *MPI-S* и S' приведены в таблице 1.

ТАБЛИЦА 1. Технические требования к параметрам оптических стыков в точках нормирования *MPI-S* и S' [2]

Точка нормирования	*MPI-S*	S'
Наименование параметров	Значение параметров	
Уровень суммарной мощности, не более, дБ	+27,0	+27,0
Уровень мощности на один оптический канал, не более, дБ	+20,0	+20,0
Отношение оптических сигнал/шум, не менее, дБ	20,0	20,0

Технические требования к параметрам оптических стыков в точках *MPI-R* и R' приведены в таблице 2.

ТАБЛИЦА 2. Технические требования к параметрам оптических стыков в точках нормирования *MPI-R* и R'

Точка нормирования	*MPI-R*	R'
Наименование параметров	Значение параметров	
Уровень суммарной мощности, не более, дБ	+1,0	+10,0
Уровень мощности на один оптический канал, не более, дБ	–36,0 ÷ –15,0	–36,0 ÷ –15,0
Отношение оптических сигнал/шум, не менее, дБ	18,0	18,0

Таким образом, для качественной передачи сигнала вдоль волоконно-оптической линии связи надо выполнить ряд условий. Во-первых, для того, чтобы узнать необходимые требования к характеристикам линии, надо точно определиться с кодом применения при проектировании и знать его

при строительстве/ эксплуатации линии [2]. Во-вторых, необходимо задаться скоростью передачи, которая зависит от числа приложений, использующих данное оптическое волокно. В-третьих, надо определиться с количеством ЭКУ и расстановкой усилителей, а также с их общим количеством на трассе. После этого требуется произвести расчёт основных показателей сигнала в разных точках нормирования и сравнить полученные результаты с нормами, приводимыми в [3]. Если все рассчитанные показатели соответствуют нормам, то всё будет работать без замечаний, если хотя бы один из них выходят за пределы, то необходимо внести изменения в проект будущей трассы (при проектировании) либо произвести ремонт (при эксплуатации).

Список используемых источников

1. Фриман Р. Волоконно-оптические системы связи. М. : Техносфера, 2006. 496 с.
2. Гитин В. Я., Глаголев С. Ф., Кочановский Л. Н. Волоконно-оптические телекоммуникационные системы / под ред. Гитина В. Я. Санкт-Петербург, РИО СПбГУТ, 2006. 176 с.
3. ITU-T Rec. G.959.1 Интерфейсы физического уровня оптической транспортной сети.
4. ОСТ45.178-2001. Системы передачи с оптическими усилителями и спектральным уплотнением. Стыки оптические. Классификация и основные параметры.
5. РД 45.195-2001. Применение транспортных технологий связи, использующих в качестве среды передачи оптическое волокно.
6. ОСТ 45.104-97 Стыки оптические систем передачи синхронной цифровой иерархии. Классификация и основные параметры.

УДК 004.056.53

ТЕХНИЧЕСКИЕ КАНАЛЫ УТЕЧКИ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

К. А. Игнатенко, Ю. В. Левин, И. А. Мартынюк, В. И. Штаненко

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

Рассмотрены возможные варианты образования технических каналов утечки информации. Работа инфокоммуникационных систем специального назначения и передача информации с использованием каналов связи, сопровождается образованием электромагнитных, акустических полей и электрических сигналов. В связи с этим создаются определенные предпосылки для образования технических каналов утечки информации при работе разных технических средств.

технические каналы, съём информации, носители информации, составной канал, пропускная способность, физическая природа носителя.

В основе причин образования технических каналов утечки информации лежат физические процессы, связанные с обработкой, передачей и хранение информации.

Общеизвестно, что информация передается полем или веществом. Это либо акустическая волна (звук), либо электромагнитное излучение, либо лист бумаги с текстом. Переданная энергия или доставляемое вещество служат только носителями информации. Человек как носитель информации и выступает субъектом отношений или источником.

Утечка информации – бесконтрольный выход информации с ограниченным доступом за пределы организации или вынос лицом, которому она была доверена [1].

Работа инфокоммуникационных систем специального назначения и передача информации с использованием каналов связи, сопровождается образованием электромагнитных, акустических полей и электрических сигналов, которые распространяются в разных средах (в воздухе, в токопроводящих конструкциях и т. д.) [2]. Поэтому создаются определенные предпосылки для образования технических каналов утечки информации при работе разных технических средств и систем.

Необходимым условием образования таких каналов есть наличие опасного сигнала, который содержит информацию с ограниченным доступом, в тех полях (электрических либо акустических сигналах), которые порождаются работой технических средств.

Выявление, прием и анализ носителей опасных сигналов техническими средствами разведки позволяют не санкционированно получать информацию с ограниченным доступом, обрабатываемую техническими средствами связи и информатизации.

В общем виде под техническим каналом утечки информации понимают совокупность источника опасного сигнала, среды распространения – носителя опасного сигнала и средства технической разведки, рис. 1 (см. ниже).

В сущности, под техническим каналом утечки информации понимают несанкционированное получение охраняемых сведении об объекте.

Для возникновения (образования, установления) канала утечки информации необходимы определенные пространственные, энергетические и временные условия, а также соответствующие средства восприятия и фиксации информации на стороне злоумышленника.

В соответствии, с учетом физической природы образования каналы утечки информации их можно объединить в следующие группы:

– визуально-оптические;

– акустические (включая и акустико-преобразовательные);

– электромагнитные (включая магнитные и электрические);

– материально-вещественные (бумага, фото, магнитные носители, производственные отходы различного вида – твердые, жидкие, газообразные).

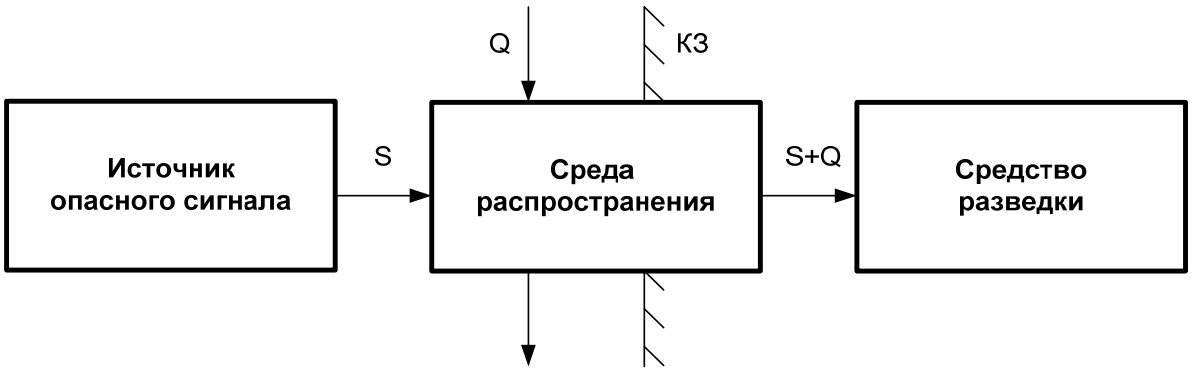


Рис. 1. Зависимость времени передачи от ширины полосы и уровня сигнала (пустая строка): S – сигнал, который содержит информацию с ограниченным доступом; Q – помеха; *КЗ* – контролированная зона

Основным классификационным признаком технических каналов утечки информации является физическая природа носителя [3]. По этому признаку они подразделяются на:

– оптические;

– радиоэлектронные;

– акустические;

– материально-вещественные.

Носителем информации в оптическом канале является электромагнитное поле в диапазоне 0,46–0,76 мкм (видимый свет) и 0,76–13 мкм (инфракрасные излучения).

В радиоэлектронном канале утечки информации в качестве носителей используются электрические, магнитные и электромагнитные поля в радиодиапазоне, а также электрический ток, распространяющийся по металлическим проводам. Частотный диапазон этого вида носителя: от звукового диапазона до десятков ГГц.

Носителями информации в акустическом канале являются механические упругие акустические волны в диапазоне: инфразвуковом (менее 16 Гц), звуковом (16 Гц-20 кГц) и ультразвуковом (свыше 20 кГц) диапазонах частот, распространяющиеся в атмосфере, водной и твердой средах.

Каналы утечки по информативности можно представить, как информативные и неинформативные [4]. Информативность канала оценивается ценностью информации, которая передается по каналу.

Канал утечки информации, состоят из передатчика, среды распространения и приемника. Имеют место варианты, когда утечка информации происходит по нескольким последовательным или параллельным каналам [5]. В выделенных помещениях, при ведении конфиденциальных разговоров, утечка информации возможна не только по акустическому каналу через стены, двери, окна, но и по оптическому – путем съема информации лазерным лучом со стекла окна или по радиоэлектронному каналу с использованием установленных специальных средств (радиозакладок). При этом образуется канал, состоящий из последовательно соединенных акустического и оптического (на лазерном луче) или акустического и радиоэлектронного (радиозакладка – среда распространения – радиоприемник) каналов.

Возможность образования технических каналов утечки закрытой информации в системах и средствах связи, и информатизации на объектах военного управления, исходит из следующих причин:

– наличием информационных радио-, оптических и электрических сигналов в разных технических средствах передачи и обработки информации;

– наличием нежелательных электромагнитных излучений в системах и средствах связи и информатизации;

– образованием электромагнитных излучений на разные токоведущие поля и конструкции;

– образованием специальных наводок на различных проводах;

– использованием разных закладок (программных и аппаратных жучков);

– образованием и распространением в окружающей среде акустических колебаний во время обсуждения вопросов, связанных с информацией с ограниченного доступа

– наличием случайных электроакустических преобразователей в элементах технических средств.

Канал утечки информации, как и любой канал связи характеризуется показателями:

– - пропускной способностью;

– - дальностью передачи информации.

Пропускная способность канала связи оценивается количеством информации, передаваемой по каналу в единицу времени с определенным качеством [6]. Согласно общей теории связи пропускную способность канала (в бодах или битах в секунду) можно рассчитать по формуле:

$$C = AF \log_2(1 + P_c/P_{\text{п}}),$$

где AF – ширина полосы пропускания канала связи; P_c и P_n – мощность сигнала и помехи (в виде белого шума) в полосе пропускания канала соответственно.

Интегральная характеристика является пропускной способностью канала связи. Учитывает, как ширину полос частот сигнала, которую пропускает канал, так и его энергетику. Чем меньше отношение мощностей сигнала и помехи, тем больше ошибок в принятом сообщении и тем меньше количество переданной информации [7]. Поэтому сущность защиты информации заключается в увеличении в каналах утечки информации сигнала помехи до порогового уровня. Соотношение уровней сигнала и помехи зависит и от расстояния в точке измерения (съема). Это положение лежит в основе организационных мероприятий и технических мер по защите информации ограниченного доступа на объектах органов управления.

Рассмотренные варианты образования технических каналов утечки информации дают представление в общем виде некоторые возможности по съему информации с ограниченным доступом, циркулирующей на защищаемых объектах.

Список используемых источников

1. Липатников В. А., Стародубцев Ю. И. Защита информации. СПб. : ВУС, 2001. С. 348–350.

2. Сидоренко Е. Н., Стародубцев Ю. И., Сухорукова Е. В., Фёдоров В. Г. Способ защиты информационно-телекоммуникационных сетей специального назначения от сетевых компьютерных атак // Актуальные проблемы инфотелекоммуникаций в науке и образовании. V Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 3-х томах. 2016. С. 333–337.

3. Бударин Э. А., Васюков Д. Ю., Дементьев В. Е., Колбасова Г. С., Краснов В. А., Лепешкин О. М., Лаута О. С., Митрофанов М. В., Худайназаров Ю. К. Обеспечение защиты информации в локальных вычислительных сетях; Военная академия связи им. Маршала Советского Союза С.М.Буденного. Санкт-Петербург, 2013.

4. Коцыняк М. А., Иванов Д. А., Лаута О. С., Нечепуренко А. П. Методика оценки защищенности информационно-телекоммуникационной сети в условиях информационного противодействия // Радиолокация, навигация, связь. Сборник трудов XXIII Международной научно-технической конференции. В 3-х томах. 2017. С. 83–89.

5. Лепешкин О. М., Карпов А. В., Шостак Р. К. Актуальность осуществления сетевого контроля защищенности информационных сетей // Радиолокация, навигация, связь. Сборник трудов XXIII Международной научно-технической конференции. В 3-х томах. 2017. С. 1198.

6. Иванов Д. А., Коцыняк М. А., Лаута О. С., Нечепуренко А. П. Модель распределения факторов информационного воздействия по элементам информационно-телекоммуникационной сети // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2017). VI Международная научно-техническая и научно-методическая конференция: сборник научных статей: в 4 т. 2017. С. 420–425.

7. Скиба В. Ю., Курбатов В. А. Руководство по защите от внутренних угроз информационной безопасности. СПб. : Питер, 2008. 320 с.

УДК 621.396

АКТУАЛЬНЫЕ СРЕДСТВА ПОВЫШЕНИЯ ПРОИЗВОДИТЕЛЬНОСТИ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И СЕТЕЙ

М. Н. Иманкул

Казахский агротехнический университет им. С. Сейфуллина

Сегодня на рынке сетевых технологий царит ускоряющаяся гонка скоростей. Инфокоммуникационные технологии продолжают свое развитие в направлении к более высокой производительности и всё большему числу возможностей. Производительность инфокоммуникационных систем проявляется в скорости обработки задач и в степени использования ресурсов системы. SDN эффективно решает задачи на стыке виртуальных и физических сред.

инфокоммуникационная система, полоса пропускания, ресурс, виртуализация.

Проблема повышения производительности инфокоммуникационных сетей в последние годы существенно обострилась, что обусловлено рядом причин, например, постоянно возрастающей структурной сложностью и размерностью современных сетей, характеризующихся множественными изменяющимися во времени информационными связями; постоянно возрастающими требованиями к уровню информационной безопасности. Для решения этой проблемы требуется, в частности, найти наиболее эффективный метод увеличения пропускной способности и подобрать телекоммуникационную технологию, в рамках которой будет работать система передачи, др.

При предоставлении современных инфокоммуникационных услуг необходима высокая производительность систем и сетей связи с соблюдением требований качества обслуживания и высокой надежности. В общем случае, рост производительности во многом зависит от конфигурации устройств, присутствующих в сети: конфигураций инфокоммуникационных систем, компонентов, программного обеспечения, операций и функций. Любое изменение любого из этих факторов может привести к разным результатам.

Производительность устройств, выполняющих обработку в инфокоммуникационных системах (ИКС), определяется техническими и программными средствами. Чем больше загружены ресурсы, тем выше производительность ИКС, а недогрузка ресурсов свидетельствует о наличии резервов для повышения производительности. Сеть объединяет систему разных раз-

меров. Ресурсы разделяются между пользователями сети. Если трафик превышает пропускную способность сети, то производительность сети будет снижена. Без эффективного управления трафиком сетевые операторы не могут эффективно использовать имеющиеся ресурсы. В частности, повышение пропускной способности каналов за счет обновления аппаратной части состоит в: использовании более производительного оборудования (например, в замене *Fast Ethernet* на *Gigabit Ethernet*); увеличении количества портов соединения (например, замене сетей типа 802.11a/b на 802.11g/n); т. п.

Балансировка нагрузки (распределение/выравнивание нагрузок, приходящихся на несколько серверов**)** решает проблему вертикального масштабирования (увеличения ресурсов сервера, таких как память, скорость диска и т. д.) и обеспечения резервных ресурсов. При росте нагрузки вертикальное масштабирование достигает предела и не дает высоких результатов. Тогда прибегают к горизонтальному масштабированию – добавлению новых серверов с перераспределением нагрузки между ними.

В частности, к параметрам, характеризующим производительность программных средств, обычно относят: количество операций, скорость выполнения программы, частоту использования программы. Эффективность программы (кода) имеет две составляющие: память (или пространство) и время. Пространственная эффективность – количество памяти, требуемое для выполнения программы. К параметрам, характеризующим производительность каналов связи, относят скорость передачи данных. Наиболее важными факторами, определяющими производительность, с точки зрения аппаратных ограничений, служат: структура иерархической организации многоуровневой памяти; пропускная способность коммуникационных каналов [1].

Рост спроса на высокоскоростные мультимедийные услуги привел к необходимости решения задачи эффективного использования пропускной способности системы для ограниченного объема частотно-временных ресурсов мультисервисных сетей связи. При выборе инфраструктурных решений одним из факторов служит возможность перехода на следующее поколение сетевых технологий (поддержка более высоких скоростей) [2].

Для рационального использования полосы следует знать структуру/критичность трафика к задержке и то, как фактически используется канал связи. Компрессия данных, применение тонких клиентов, кэширование, использование решений для оптимизации трафика позволяют добиться сокращения трафика от 2 до 5 раз.

Сложность беспроводных сетей вызывает проблемы, которые нельзя решить путем применения локальных и реагирующих на какие-либо действия протоколов. В частности, в актуальных средствах беспроводной связи существенный рост скорости передачи данных может быть достигнут путем

использования технологии MIMO (*Multiple Input – Multiple Output*). Применение MIMO значительно снижает вероятность ошибки при обмене данными, увеличивает пропускную способность за счет формирования физически различных каналов. Повысить пропускную способность линии можно за счет увеличения частотной эффективности выделенной полосы пропускания, то есть использованием рационального вида модуляции [3].

Решения IoT (Internet of Things) обладают высокими скоростями передачи, низким временем задержки, надежным установлением связи, а с выходом 5G новые возможности применения станут намного более разнообразными при увеличении точности. Скорость проникновения инновационных технологий пока сдерживается характеристиками коммуникационной среды, а управление сетевой инфраструктурой становится программным. Растёт роль проблемы преодоления разрыва между аппаратными средствами и используемыми методами программирования. Построение сетей с программно-ориентированным подходом – будущее телекоммуникаций. Для увеличения производительности ИКС следует использовать самые последние перспективные результаты фундаментальных исследований в сфере построения микропроцессоров, коммуникационных сетей, программных средств, микроэлектронных и оптических технологий, т. п.

Компания AT&T плодотворно работает над технологиями, позволяющими расширять возможности по передаче данных. AT&T объединила в одной технологии миллиметровые волны и линии электропередачи (проект AirGig) [4]. В AT&T считают, что будущее широкополосного доступа и беспроводной связи за технологией AirGig. При эксплуатации сети AirGig используют программно-ориентированный подход, что позволяет отказаться от широкого применения маршрутизаторов, коммутаторов, межсетевых экранов.

Сегодня рост производительности процессов обработки информации достигается новыми подходами (методами молекулярной электроники, квантового компьютинга, пр.). Отметим, что достижения электроники, цифровая обработка дают выигрыш в разах, а нужно на порядки. Достижения наноэлектроники приближаются к квантовым пределам, установленным самой природой. По мнению экспертов, пост-Муровские технологии будут на основе сверхпроводниковой логики и криогенной памяти [5].

В условиях набирающей популярность автоматизации всех видов деятельности предприятий цифровая трансформация (ЦТ) предъявляет повышенные требования к их сетям и обмену бизнес-информацией. ЦТ в сфере инфотелекоммуникаций опирается на внедрение принципов SDN (*Software Defined Networking*) и NFV (*Network Function Virtualization*) для повышения гибкости сетей, без чего невозможна эффективная поддержка облаков и IoT. Сеть превращается в офисную платформу [6]. Появление сотен тысяч новых

серверов в процессе перехода к SDN/NFV увеличивает пропускную способность каналов. Концепция SDN интегрирует виртуальные и физические сетевые ресурсы, и их функционал в рамках единой виртуальной сети. При виртуализации решается вопрос с недостаточностью загрузки оборудования, и появляются свободные ресурсы для развертывания новых сервисов. Виртуальные сети, в отличие от физических, независимы от оборудования, имеют высокую скорость инициализации и возможность развертывания без прерывания работы систем.

Перегрузка узлов доступа и динамическая природа беспроводной среды ставят перед пользователями задачи повышения и поддержания производительности беспроводной сети. В частности, для техники передачи данных важно поддерживать связь даже в ситуациях, когда мобильные терминалы перемещаются между базовыми станциями. Для реализации сетевой передачи обслуживания при переключении маршрута связи мобильных терминалов можно использовать протокол PMIPv6 (*Proxy Mobile* IPv6), поддерживающий движение мобильного узла MN (*Mobile Node*) в сети, используя только собственный механизм обработки сети. Связь мобильных терминалов проходит через прокси-сервер LMA (*Local Mobility Anchor*), который реализует функцию ретрансляции IP-пакетов между MN и корневым узлом. Домен PMIPv6 включает в себя LMA, шлюз мобильного доступа MAG (*Mobile Access Gateway*), выполняющего функцию шлюза MN по умолчанию, и сеть, в которой размещаются MN. В домене PMIPv6 маршруты связи MN являются избыточными, что увеличивает загрузочную нагрузку на LMA. Наконец, задержка связи увеличивается за счет процесса туннелирования между MAG и LMA. Эти обстоятельства снижают производительность сети

В частности, оптимизировать маршруты связи можно путем применения OpenFlow к сети PMIPv6. OpenFlow – протокол управления процессом обработки данных, передающихся по сети передачи данных маршрутизаторами и коммутаторами, и реализующий технологию программно-определяемой сети. Метод OpenFlow отделяет функции сетевых устройств, которые пересылают пакеты в блок управления маршрутами пакетов (плоскость управления) и в блок функции передачи данных (плоскость данных). OpenFlow состоит из OpenFlow Switch, который выполняет обработку передачи данных, и OpenFlow Controller, отвечающего за передачу пакетов по каждому из переключателей OpenFlow.

Совершенствующиеся технологии компьютерной памяти становятся решающим фактором при создании высокопроизводительных систем [7]. Например, основными компонентами систем Memory-Driven Computing (компании *Hewlett Packard Enterprise* и «Крок») являются: быстродействующая постоянная память; высокопроизводительная коммутационная фабрика (структура), гарантирующая передачу данных между узлами ком-

пьютерных систем с использованием фотонных коммуникаций; вычисления, ориентированные на задачи; новое программное обеспечение, позволяющее радикально упростить программирование и создавать приложения, к которым невозможно приступить сегодня.

Список используемых источников

1. Корнеев В. Модель программирования: смена парадигмы // Открытые системы. 2010. № 3. С. 29.

2. Барсков А. Сетевая инфраструктура в комплексе // Журнал сетевых решений / LAN. Март 2017. С. 19.

3. Гладких А. А., Шакуров Р. Ш. Повышение эффективности декодирования по упорядоченным статистикам // Труды Российского научно-технического общества радиоэлектроники и связи им. А. С. Попова. Выпуск LXVI. 2011. 239 с.

4. Григорьев Д. Электросети могут обеспечить всем связь “пятого” поколения [Электронный ресурс]. URL: https://nag.ru/articles/article/31040/elektroseti-mogut-obespechit-vsem-svyaz-pyatogo-pokoleniya.html

5. Чернобровцев А. Наше микропроцессорное завтра // Computerworld, Россия. 26 мая 2017. С. 14.

6. Ганьжа Д. Связь в процессе трансформации // Computerworld, Россия. 26 мая 2017. С. 19.

7. Чернобровцев А. Компьютеры эпохи Больших Данных [Электронный ресурс] // Computerworld Россия. 2017. № 19. URL: https://www.osp.ru/cw/2017/19/13053429/

УДК 004.7

МОНИТОРИНГ СЕТИ ТАКТОВОЙ СЕТЕВОЙ СИНХРОНИЗАЦИИ В ТЕЛЕКОММУНИКАЦИОННОЙ СИСТЕМЕ

А. А. Казакевич, Е. А. Степанова

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

Цифровое коммутационное оборудование необходимо синхронизировать, чтобы предотвратить проскальзывания в эластичной памяти. Проскальзывания не оказывают заметного влияния на обычные телефонные разговоры, но они существенно влияют на передачу данных. Именно поэтому сети синхронизации необходимо снабжать системами контроля, которые позволят непрерывно в реальном масштабе времени проводить проверку рабочих характеристик распределения синхросигнала.

мониторинг, система мониторинга, синхронизация, сеть тактовой сетевой синхронизации.

В последние годы стало очевидно, что сетевая синхронизация важна не только для сетей синхронной цифровой иерархии. В сетях ATM (асинхронный режим), сотовых мобильных телефонных сетях GSM (Глобальная система мобильной сотовой связи), GPRS (Общая служба пакетной радиопередачи), UMTS (Универсальная система мобильной связи) сетевая синхронизация также оказывает решающее влияние на качество предоставляемых услуг. Именно поэтому сети синхронизации необходимо снабжать системами контроля, которые позволят непрерывно в реальном масштабе времени проводить проверку рабочих характеристик распределения синхросигнала [1].

Для решения этой проблемы авторами предлагается использовать схему измерений с независимыми устройствами синхронизации, т. е. без общего ведущего устройства для двух сигналов, между которыми измеряют погрешность времени. В качестве второго эталонного сигнала синхронизации было принято решение использовать сигнал от системы спутниковой навигации ГЛОНАСС. Следовательно, для реализации проекта потребуется установка дополнительного оборудования, необходимого для получения и обработки внешнего сигнала синхронизации от спутников; и сравнения его с сигналом синхронизации, следующим по сети тактовой сетевой синхронизации (ТСС). Самым простым способом измерения стабильности сигнала синхронизации является непосредственное измерение его погрешности времени по отношению к опорному сигналу (непосредственное цифровое измерение *TE*) [2].

При помощи внешнего опорного сигнала от системы ГЛОНАСС существует два способа проведения измерений. В первом случае (рис. 1, см. ниже) опорный сигнал сравнивается с сигналом 2048 кбит/с, поступающим на вход счетчика с аппаратуры АРСС/РСС или напрямую с выхода Т4 мультиплексора.

Основой системы мониторинга является разработанное авторами устройство сличений, необходимое для приема и обработки нескольких независимых синхросигналов, и дальнейшего расчета погрешности времени $TE(t)$ между ними [3].

Одним из основных компонентов устройства сличений является системный синхронизатор СЦИ/SONET ZL30130. Это высокоинтегрированное устройство, которое обеспечивает все функции, необходимые для обработки сигналов синхронизации, поступающих на его входы с частотами 2 кГц или *N**8 кГц вплоть до 77,76 МГц. После преобразования, сигнал синхронизации нужной частоты поступает на вход контроллера мониторинга, который представляет собой совокупность из микропроцессора, необходимого для управления системным синхронизатором и цифрового счетчика времени, принцип работы которых подробно разобран в предыдущем разделе.

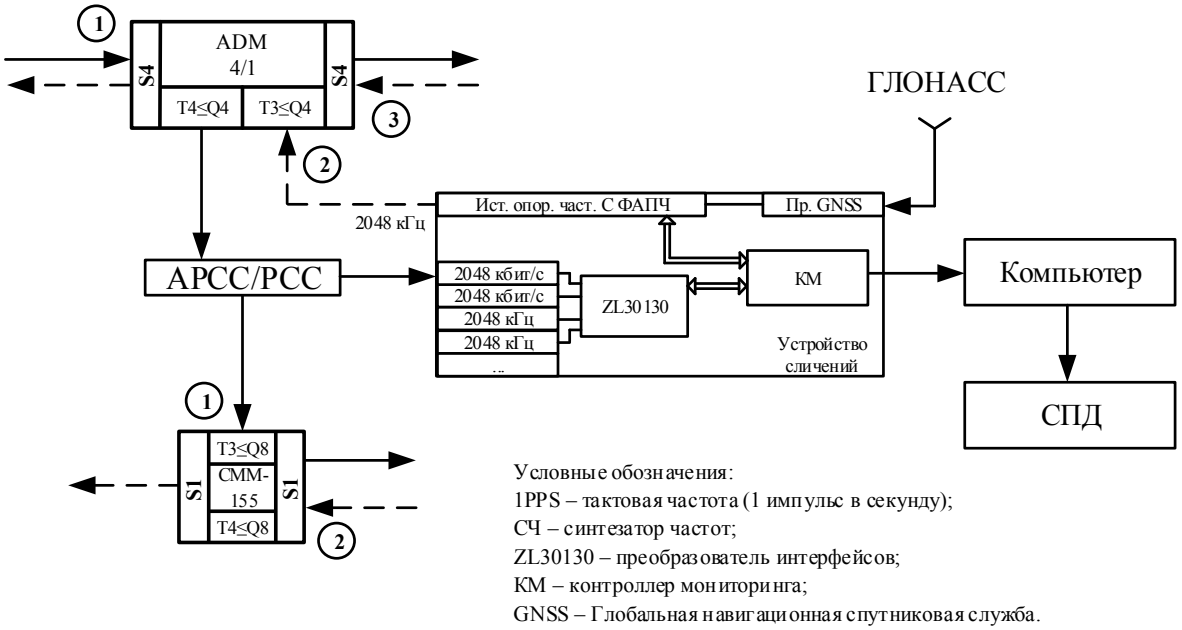


Рис. 1. Схема проведения измерений стабильности сигнала синхронизации, полученного от АРСС/РСС

Измеренная цифровым счетчиком погрешность времени $TE(t)$ между двумя сигналами синхронизации поступает на компьютер, где происходит вычисление основных характеристик синхронизации (МОВИ, ДВИ и др.), позволяющих оценить ее качество. Важно не забывать, что величина *TE(t)*, измеренная по такой схеме, будет зависеть не только от внутреннего фазового шума исследуемого устройства синхронизации, но и от влияния любого сдвига или дрейфа частоты, присущих всем устройствам в схеме измерений [4].

Измерения происходят непрерывно, в режиме реального времени. По мере накопления информация будет передаваться с компьютера в единый центр мониторинга через сеть передачи данных (СПД), где и будет приниматься дальнейшее решение о состоянии сети синхронизации на конкретном пункте.

Второй способ организации системы мониторинга представлен на рис. 2 (см. ниже).

Преимущество данной схемы в том, что она также позволяет наблюдать искажения, вносимые ведомым устройством синхронизации (его внутренние шумы). Однако для этого необходим более функциональный синхронизатор ZL30143, способный получать и преобразовывать с помощью SFP-модуля сигнал синхронизации напрямую с мультиплексора.

Для отведения части оптического сигнала на синхронизатор используются 5 % ответвители – устройства, позволяющие осуществлять неравномерное деление оптической мощности, поступающей на один входной канал, между несколькими выходными каналами. Максимальные

вносимые потери составляют 0,5 дБ, что практически не скажется на дальности передачи оптического сигнала, а 5 % мощности будет достаточно для проведения измерений. Единственным существенным недостатком данной схемы измерений является то, что для подключения на входе и выходе мультиплексора оптических ответвителей, необходимо, пусть и на очень короткое время, разорвать тракт передачи.

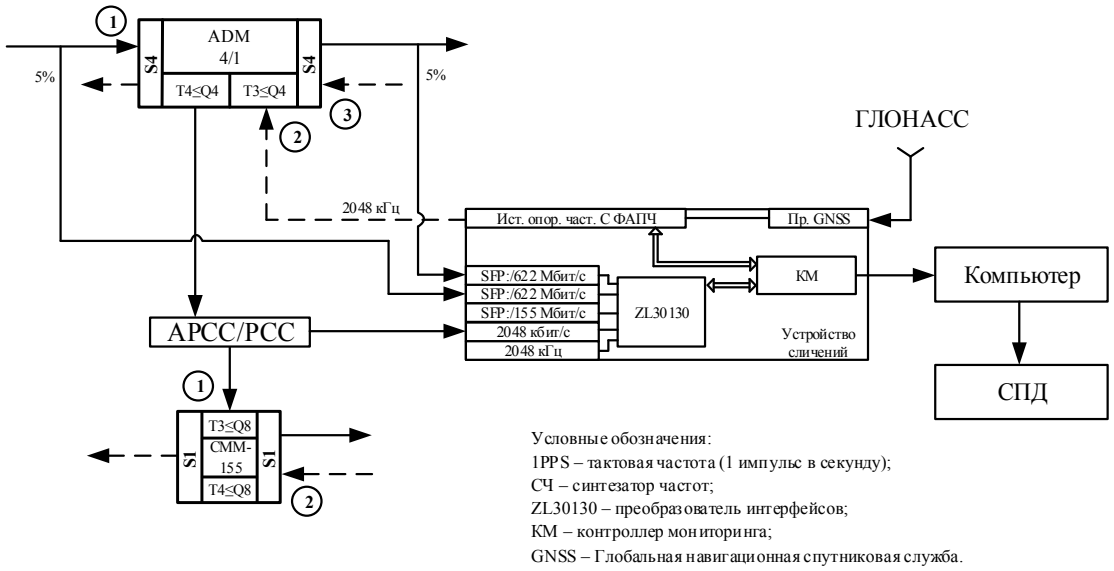


Рис. 2. Схема проведения измерений стабильности сигнала синхронизации, полученного со входа и выхода мультиплексора

После преобразования, сигнал синхронизации нужной частоты также поступает на вход контроллера мониторинга для измерения цифровым счетчиком погрешности времени $TE(t)$. Затем данные с цифрового счетчика передаются на компьютер, и уже качественные характеристики сигнала синхронизации через СПД попадают единый центр мониторинга.

Применение разработанных схем осуществляется в соответствии с разработанным алгоритмом функционирования системы мониторинга (рис. 3, см. ниже). Данный алгоритм разбит на три функциональных блока, каждый из которых характеризует определенный этап работы системы мониторинга.

Разработанные алгоритм и схемы проведения измерений стабильности сигнала синхронизации позволят обнаруживать искажения сигнала синхронизации прежде, чем они окажут влияние на качество работы телекоммуникационной системы.

Список используемых источников

1. Ксенз С. П., Полтаржицкий М. И., Алексеев С. П., Минеев В. В. Борьба с диагностическими ошибками при техническом обслуживании и ремонте систем управления связи и навигации: учебное пособие. СПб. : ВАС, 2010. 240 с.

2. Стефано Брени. Синхронизация цифровых сетей связи. М. : Мир, 2003. 417 с.

3. Паляничко Д. А., Згуря В. И., Папуша Р. Г. Обработка результатов измерений // Электротехнические и компьютерные системы. 2012. № 06 (82). С. 34–38.

4. Бакланов И. Г. Методы измерений в системах связи. М. : Эко-трендз, 1999. 195 с.

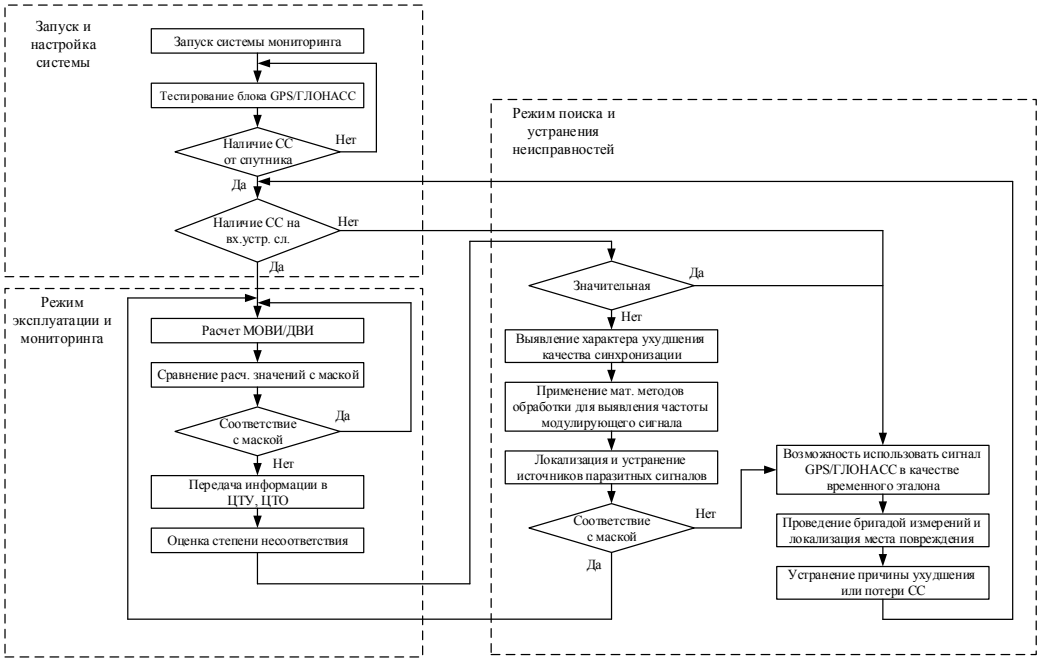


Рис. 3. Алгоритм функционирования системы мониторинга

Статья представлена заместителем начальника Научно-исследовательского центра ВАС, кандидатом технических наук, полковником Д.О. Федосеевым.

УДК 004.056

РАЗРАБОТКА ИНТЕГРИРОВАННОГО РЕШЕНИЯ ЗАЩИЩЕННОЙ IP-ТЕЛЕФОНИИ ДЛЯ СЕТИ МАСШТАБА ВУЗА С УДАЛЕННЫМИ ФИЛИАЛАМИ

Д. Б. Казаков, М. М. Ковцур, А. В. Козьмян

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

IP-телефония позволяет значительно снизить расходы на связь и предоставляет широкий спектр дополнительных возможностей. В рамках доклада рассматривается возможность интеграции решения защищенной IP-телефонии на базе IP-АТС в существующую сеть вуза. Решение обеспечивает отказоустойчивость, поддерживает протоколы информационной безопасности IP-телефонии, видео-телефонию, а также

имеет модуль сбора статистики по отдельным группам пользователей в рамках университета.

VoIP, asterisk, биллинг, отказоустойчивость.

Asterisk – это программная АТС с открытым исходным кодом, которая может быть использована для разработки решений IP-телефонии, обладающая возможностями классических АТС, а также широким дополнительным функционалом, доступным только в дорогих аппаратных системах связи корпоративного уровня, например, Unified Cisco CallManager, Alcatel-Lucent OmniPCX Enterprise и т. п. Asterisk не требователен к аппаратным ресурсам и может быть развернут на персональном компьютере, нетбуке, на виртуальной машине. Возможна интеграция с существующей аппаратной АТС. Может быть обеспечено соединение с ТФОП по сигнализациям ISDN или ОКС7 с недорогим дополнительным оборудованием в качестве шлюза IP-TDM.

В данном проекте поставлено несколько задач: анализ недостатков существующей системы связи, на их основе необходимо сформировать требования к решению и разработать модель системы связи с их учетом, а также разработать модуль статистики для учета звонков для IP-АТС.

Текущая система IP-телефонии основана на решении компании Cisco Systems – Cisco Unified Communications Manager (CUCM), в ее основные недостатки входят:

– использование проприетарных протоколов сигнализаци и отсутствие шифрования сигнализации и разговорного трафика на основе разрешенных в РФ алгоритмов шифрования;

– высокая стоимость обновлений версий и годовых подписок технической поддержки.

Таким образом, конечное решение должно:

– обеспечивать отказоустойчивость и надежность высокого уровня;

– поддерживать протоколы информационной безопасности IP-телефонии;

– использовать открытое (бесплатное) программное обеспечение (ПО) и протоколы;

– иметь модуль сбора статистики по отдельным группам пользователей в рамках ВУЗа;

– иметь шлюзы в ТФОП;

– поддерживать функционал IVR и центра обработки вызова.

Для проекта выбрана платформа FreePBX, которая является одним из наиболее распространенных дистрибутивов Asterisk с графическим интерфейсом и множеством дополнительных модулей, упрощающих и расширяющих настройку и администрирование сервера телефонии.

FreePBX предлагает простой, интуитивно понятный интерфейс для настройки и управления Asterisk. Для лучшей совместимости с различным оборудованием следует избегать использования проприетарных стандартов, сигнализации, протоколов и ПО.

Решение использует кластеризацию, скрытую от пользователей. В решении применяется протокол телефонной сигнализации SIP, как на пользовательских устройствах, так и транках. Программные АТС реализуются в виде виртуальных машин.

Система обеспечивает высокую доступность путём использования кластера из двух серверов (рис. 1). Они работают в режиме Active / Standby: если активный по умолчанию сервер отказывает, то второй незаметно для абонентов переключает обработку вызовов на себя. АТС имеет возможность «горячей» смены серверов без отключения от системы, где необходимый сервер может быть заменен даже в онлайн условиях без нарушения работы служб. Системное ПО способно использовать обнаружение ошибок, автоматическое восстановление системы и отправлять сообщения администратору на почту в случае отказа одного из серверов. В FreePBX имеются возможности для мониторинга состояния IP АТС, а в ПО кластеризации возможности мониторинга состояния самих серверов и запущенных служб.

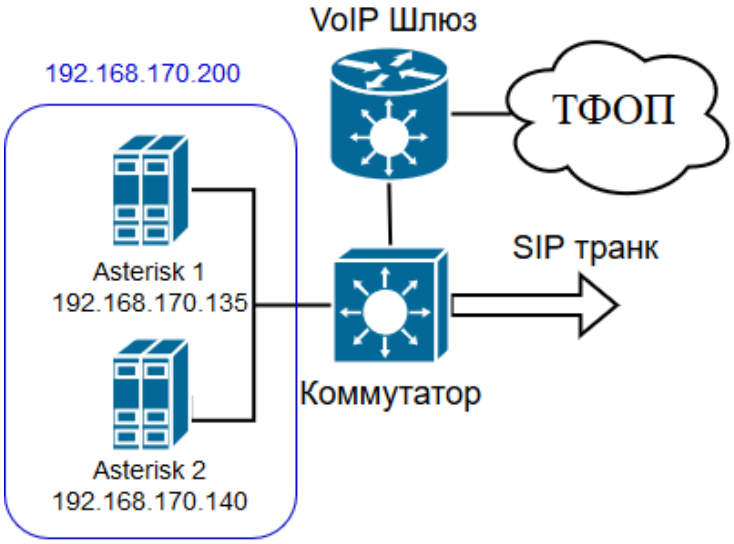


Рис. 1 Схема модели

Отказоустойчивость обеспечивается с помощью служб Pacemaker и Corosync или Heartbeat. Corosync и Heartbeat являются аналогичным ПО, позволяющим реализовать простую кластеризацию из 2-х узлов с отслеживанием их состояния и динамическим виртуальным IP [1].

Один из узлов назначается главным (*master*), а другой ведомым (*slave*). Slave получает виртуальный адрес в случае отказа master. Работа службы

происходит путем создания виртуального сетевого суб-интерфейса Linux на узле, который в данный момент считается главным или активным.

Узлы обмениваются UDP пакетами, и, если в течение времени, превышающем заранее заданный параметр, от master не поступают сообщения, он объявляется отказавшим, а в журнал событий заносится соответствующая запись, и адрес кластера перейдет к slave. За частоту обмена сообщениями отвечает параметр контроля состояния, который устанавливает интервал в секундах между отправкой пакетов.

Однако отказоустойчивости на уровне сервера может быть недостаточно, если сам сервер еще работает, а служба АТС отказала. В таком случае в дополнение к созданию кластера можно использовать «менеджер ресурсов», например, Pacemaker. В его задачу входит мониторинг работы отдельных служб на каждом из узлов кластера и их включение или отключение в соответствии с параметрами. Если на активном сервере процесс Asterisk остановится, то динамический адрес перейдет к другой сервер, на которой он работает.

Синхронизация конфигураций серверов обеспечивается встроенными возможностями Asterisk и FreePBX. Резервный сервер настроен таким образом, чтобы он подключается к основному серверу по SSH и синхронизирует настройки Asterisk, содержимое истории звонков, голосовой почты, базу данных и др. Это может производиться вручную или по расписанию [2].

Для повышения безопасности Asterisk имеет возможность реализовать шифрование вызовов из конца в конец, для чего может использоваться защищенный протокол реального времени – Secure Realtime Transport Protocol (SRTP). Он обеспечит криптографическую защиту (шифрование и/или аутентификацию по выбору) голосовых сообщений с помощью известного алгоритма шифрования AES [3].

Основные задачи протокола SRTP:

- шифрование передаваемых сообщений;
- аутентификация;
- защита от повторной передачи пакетов;
- сохранение полосы пропускания, сжатие RTP-заголовков.

Протоколы защиты сигнализации служат для скрытия сведений о телефонных номерах вызывающего и вызываемого абонентов, а также об используемых кодеках. Для этого используется протокол Secured SIP. Он работает по аналогии с протоколом HTTPS – между корреспондентом и сервером организовывается SSL-туннель с использованием сертификатов и открытого ключа для передачи SIP сообщений.

SIP over TLS обеспечивает конфиденциальность и целостность информации в канале, осуществляет аутентификацию прокси-серверов с использованием сертификатов. В рамках модели SIP over TLS

безопасность достигается на каждом участке по пути следования сигнальных сообщений [4].

Для работы протокола TLS требуются сертификаты. Есть возможность использования сертификатов, выданных в Центрах сертификации, а также генерация самоподписанного сертификата. Поскольку шифрование включается в настройках каждого пользователя отдельно, есть возможность включения опции только для избранных пользователей [5].

FreePBX имеет встроенный межсетевой экран, специально предназначенный для обработки VoIP трафика. Он постоянно контролирует удаленных пользователей, которым разрешено подключаться к этому серверу, и автоматически разрешает доступ подлинным узлам. Автоматически определяются доверенные транки и клиентские терминалы, принимается только трафик разрешенного протокола от них. Таким образом, от взломанного SIP клиента не будет приниматься паразитный трафик. Все входящие сетевые соединения считаются частью зон. Каждый сетевой интерфейс имеет зону по умолчанию, и данные, поступающие на этот интерфейс, рассматриваются как принадлежащие этой зоне, если только она не является известной сетью, которая переопределяет зону по умолчанию. Сервисы предоставляются индивидуально каждой зоне.

Есть возможность использования «отзывчивого» фаервола (*Responsive Firewall*). Его суть заключается в том, что любые входящие VoIP-соединения получают очень ограниченное количество попыток регистрации. Если попытка регистрации прошла успешно, удаленный хост затем добавляется в доверенную зону. Если попытки подключения неудачны, трафик с этого компьютера будет отклоняться в течение определенного периода времени.

Биллинг звонков через Астериск – технические средства и меры, предназначенные для учёта и контроля звонков, их длительности и стоимости, выполняемых через АТС Asterisk.

Сам по себе Asterisk располагает минимальными средствами для выполнения такого контроля. Ведётся учёт в специальных CDR-записях [6], в которых есть информация об источнике и получателе звонка, его длительности, и т. д. Записи сохраняются в базе данных базы MySQL, в FreePBX модуль отчетов CDR позволяет просматривать отчет, показывающий телефонные звонки, сделанные и полученные в системе.

Для сбора статистики используется отдельный php скрипт, выполняющий подключение и запрос к базе данных (БД) CDR MySQL. Создав в БД отдельную таблицу с соответствиями номер-департамент, можно получать статистику и историю звонков из них, список отделов в интерфейсе скрипта также будет получаться из базы данных. Для его работы потребуется создание пользователя с правами на выполнение запросов к БД и разрешение удаленного подключения в конфигурации MySQL.

Согласно выдвинутым требованиям разработана модель системы связи на базе IP-АТС Asterisk, в которой обеспечивается безопасность связи и доступа, высокая доступность, возможность ведения учёта звонков по иерархии организации. Дальнейшие задачи состоят в введении основных и дополнительных сервисов, построении модели возможных угроз безопасности. Потребуется провести нагрузочные тесты для определения производительности системы.

Список используемых источников

1. Information and documentation on Linux Open Source High Availability HA Clustering [Электронный ресурс]. – Режим доступа: http://www.linux-ha.org (дата обращения 27.11.2017).

2. Sangoma's Wiki [Электронный ресурс]. – Режим доступа: https://wiki.freepbx.org/ (дата обращения 05.02.2018).

3. Ковцур М. М., Никитин В. Н., Юркин Д. В. Протоколы обеспечения безопасности VoIP-телефонии // Защита информации. Инсайд. 2012. № 3. С. 74–81.

4. Бухарин В. В., Липатников В. А., Сахаров Д. В. Метод управления информационной безопасностью организации на основе процессного подхода // Информационные системы и технологии. Орел : ГТУ, 2013. № 3–77. С. 102–109.

5. Jim Van Meggelen Asterisk: The Future of Telephony // O'Reilly Media, Inc., 2007. Computers. PP. 354–358.

6. Leif Madsen, Russell Bryant Asterisk – The Definitive Guide // O'Reilly Media, Inc., 2013. Computers PP. 567–579.

УДК 004.421

ИСПОЛЬЗОВАНИЕ СИНТЕТИЧЕСКИХ ДАННЫХ ДЛЯ ОБУЧЕНИЯ НЕЙРОННОЙ СЕТИ КЛАССИФИКАЦИИ ЛЕТАТЕЛЬНЫХ АППАРАТОВ

Е. В. Каляшов, А. А. Савельева, А. В. Тарлыков

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

В статье рассмотрен метод подготовки синтетических обучающих данных для задачи классификации, локализации и определения параметров траектории летательных аппаратов. Приведено общее описание реализованного подхода, алгоритмов верхнего уровня и возможностей по их настройке. Дополнительно рассмотрены результаты эксперимента с обучением нейронной сети на модельном примере.

нейронная сеть, обучение, подготовка данных, аугментация.

В качестве задачи рассматривается обнаружение, классификация и определение параметров движения летательных аппаратов для системы пассивного оптического наблюдения. Подобные системы характеризуются практически произвольным положением наблюдаемых объектов в поле зрения системы, более того, множество возможных ориентаций наблюдаемых объектов относительно плоскости наблюдения также достаточно велико. Данные условия приводят к необходимости подготовки большого набора размеченных данных, необходимых для обучения нейронной сети, что является определённой проблемой в связи со спецификой задачи – практически невозможно в свободном доступе найти набор видеоматериалов, содержащих изображения летательных аппаратов, полученных с различных ракурсов и в различных масштабах. С другой стороны, существует достаточно большое количество доступных качественных трёхмерных моделей различных летательных аппаратов, что открывает широкие возможности по генерации обучающих данных.

Одним из путей решения общей задачи является разбиение на этапы: детектирование объекта на изображении, классификация выделенного объекта, определение параметров объекта. На первом этапе используется сегментирующая сеть, результатом является фрагмент изображения с выделенным объектом [1]. На втором этапе классифицирующая сеть определяет тип объекта. И на третьем этапе используется регрессионная сеть, обученная под тип объекта, определённый на втором этапе. Такой подход позволяет в случае добавления новых типов объектов не модифицировать весь комплекс, а добавлять только необходимые фрагменты в общий процесс.

В данной статье рассмотрена подготовка данных и обучение классифицирующей нейронной сети. Генерация обучающего набора изображений производится на основе трёхмерных моделей летательных аппаратов. Для этой цели разработаны программы imgen и maskgen. Программа imgen производит загрузку трёхмерных моделей, получение различных проекций и запись полученных изображений для дальнейшего использования при обучении. Программа maskgen, в свою очередь, обеспечивает создание попиксельных масок проекций.

Программа imgen обеспечивает загрузку трехмерных моделей летательных аппаратов в форматах obj и 3ds. Для работы с исходными моделями используется библиотека OpenSceneGraph [2]. Для генерации набора проекций производится задание диапазонов углов вращения модели, её позиций и масштабов. Значения из диапазонов выбираются линейно либо случайным образом (в зависимости от настроек). Дополнительно, при генерации используется предопределённый набор фоновых изображений небосвода, что позволяет повысить устойчивость решения. Общий алгоритм генерации проекций представлен на рис. 1 с использованием псевдокода.

Конфигурационный файл программы обеспечивает настройку параметров для получения требуемого набора трансформаций – смещений объекта по осям *x*, *y*, *z*, повороты вокруг осей *x*, *y*, *z*, диапазон масштабов объекта. Пример возможного описания трансформаций приведён на рис. 2.

```
model = load_model()
foreach position, rotation, scale:
    projection = project(model, position, rotation,
scale)
    background = next(background)
    image = merge(projection, background)
    save(image)
```

Рис. 1. Псевдокод общего алгоритма генерации проекций

```
   "count":15000, "random":true,
   "position": {
       "x":{"from":-1000,"to": 1000},
       "y":{"from":  200,"to":  200},
       "z":{"from": 1000,"to":-1000}},
   "angle": {
       "x":{"from":-1.2,"to":1.2},
       "y":{"from":-1.2,"to":1.2},
       "z":{"from":-1.2,"to":1.2}},
   "scale":{"from": 0.3,"to":0.8}
```

Рис. 2. Пример задания диапазонов трансформаций объекта

Генерация проекций объекта может производиться как линейно, так и случайно, в границах заданных диапазонов. Одновременно с генерацией проекций, в файл с метаинформацией записываются значения всех параметров трансформации. Данные параметры используются позже, при обучении регрессионной сети определения параметров объекта.

В дополнение к описанию трансформаций исходного объекта, в конфигурационном файле производится настройка входных и выходных параметров (рис. 3).

```
   "input": {
      "model_folder":"../planes/FA5",
      "background_folder":"./bg7",
      "bg_augmentation":true}
   "output": {
      "output_folder":"./train_asp_160_3",
      "size": {"width":320,"height":240},
      "extension":".jpg", "num_multi_samples":4}
```

Рис. 3. Пример описания входных и выходных параметров

Параметры позволяют указать расположение трёхмерных моделей и фоновых изображений небосвода. Реализована поддержка аугментации фоновых изображений (параметр *bg_augmentation*) – случайным образом производится изменение масштаба и добавление отражений относительно одной из осей. Дополнительно поддерживается генерация попиксельных контрастных масок для всех проекций, с использованием параметра mask_background настраивается отдельный фон для масок. Целесообразно использовать однотонный фон для упрощения последующего выделения контуров объекта.

В выходных параметрах настраиваются размеры генерируемых изображений, тип генерируемого файла, выходной каталог. Дополнительно, с использованием параметра mask_folder существует возможность задания отдельного каталога для попиксельных масок.

Отдельная программа maskgen предназначена для генерации масок на основе ранее сгенерированных проекций. В процессе обучения сети детектирования объектов необходимо сопоставлять верную позицию объекта обучающему изображению. При сегментации изображения объекту сопоставляется соответствующая маска. Это может быть контур объекта, обрамляющие объект геометрические фигуры или набор параметров, по которым такую маску можно построить. Для используемых сетей сегментации использовались бинарные маски – контурная маска, описывающий круг, обрамляющий прямоугольник. Обучающие данные состояли из набора входных изображений и соответствующих им масок. Для работы с масками использовалась библиотека OpenCV [3].

При подготовке к обучению регрессионной сети генерируется набор изображений объекта, наблюдаемого с различных ракурсов, и соответствующие метки. Метки являются идентификаторами характеристик изображения – углы поворота объекта, смещение по осям на изображении, масштаб. Для достижения сетью способности к обобщению, целесообразно расширять набор фоновых изображений, например, используя аугментацию фона [4].

На вход классифицирующей и регрессионной сетей должны подаваться фрагменты исходного изображения, выделенные детектирующей сетью. Детектирование объекта может быть приблизительным – в выделенном фрагменте объект может располагаться со смещениями относительно центра. Следовательно, классифицирующая и регрессионная сети должны обучаться с учётом возможных произвольных смещений. Устойчивости предсказания параметров к сдвигу можно достичь, либо добавляя смещения объекта на этапе генерации обучающего набора, либо применяя аугментацию изображений в процессе обучения. Аугментация изображений на этапе обучения может применяться только ограниченно, так как определение

параметров объекта после модификации результирующего изображения невозможно. Тем не менее, в частных случаях, возможно применение аугментации данных на этапе обучения если можно выделить параметры, которые не влияют на размеченные признаки. Например, для ориентации объекта размеченными признаками являются углы поворота. Смещение изображения или его масштабирование не влияют на разметку и могут использоваться для аугментации.

Классифицирующая сеть не использует метки, поэтому позволяет широко применять аугментацию данных на этапе обучения. При обучении регрессионной сети следует ограничиваться только модификацией признаков, не учитываемых в обучении. В данной работе такими признаками являются смещения по осям в плоскости изображения.

В качестве примера рассмотрим результаты обучения классифицирующей сети с использованием синтетических данных, полученных описываемым выше способом. Классификатор обучался на 10 классах объектов, количество обучающих изображений на каждый класс было равным и изменялось от 1000 до 4000 в нескольких экспериментах. При генерации обучающего набора была включена аугментация фона. К фоновым изображениям применялись отражения по вертикали и горизонтали, а также масштабирование в пределах от 1.0 до 2.0 с последующей обрезкой до исходного размера. Для получения набора проекций летательных аппаратов изменялись следующие параметры: смещение объекта по осям x и z, повороты по осям y и z, масштаб. Мерой точности служил средний процент верной классификации для всех 10 классов. В качестве тестового набора использовались сгенерированные изображения в количестве 500 единиц на каждый класс со значениями параметров проекции, близкими к конфигурации обучающего набора. Параметры аугментации в процессе обучения: масштабирование ± 5 %, наклоны ± 3градуса, вращения ± 5 градусов, смещения по вертикали и горизонтали ± 5 %. Результаты обучения приведены в таблице.

ТАБЛИЦА. Результаты обучения

№	Изображений на класс	Аугментация	Точность, %
1	1000	да	96,2
2	2000	да	95,9
3	4000	да	97,0
4	4000	нет	98,4

Данные для эксперимента № 2 получены из оригинальных 1000 изображений эксперимента № 1 двойным проходом с использованием аугментации, данные для №3 получены четырьмя проходами. Дополнительно,

для №№ 2, 3, 4 сеть модифицировалась – был добавлен усредняющий слой, уменьшающий размерность данных в 4 раза.

По результатам эксперимента можно сделать следующие выводы.

– использование синтетических данных позволяет успешно решать поставленную выше задачу;

– расширение обучающего набора естественным образом увеличивает точность классификации;

– уменьшение размерности входных данных ведёт к снижению качества классификации. Очевидно, для классификатора важны детали изображений в высоком разрешении;

– расширение обучающего набора с использованием аугментации позволяет повысить точность. В случае ограниченного набора входных данных представляется целесообразным применение аугментации в процессе обучения.

Список используемых источников

1. Olaf Ronneberger, Philipp Fischer, Thomas Brox. U-Net: Convolutional Networks for Biomedical Image Segmentation [Электронный ресурс] // Электрон. текстовые дан. 2015. URL: https://arxiv.org/abs/1505.04597 (дата обращения 10.02.2018).

2. The OpenSceneGraph Project Website [Электронный ресурс] // Электрон. дан. 2018. URL: http://www.openscenegraph.org (дата обращения 10.02.2018).

3. Open Source Computer Vision Library [Электронный ресурс] // Электрон. дан. 2018. URL: http://opencv.org, (дата обращения 10.02.2018).

4. Aysegul Dundar, Ignacio Garcia-Dorado. Context Augmentation for Convolutional Neural Networks [Электронный ресурс] // Электрон. текстовые дан. 2017. URL: https://arxiv.org/abs/1712.01653, (дата обращения 10.02.2018).

Статья представлена проректором по информатизации, кандидатом технических наук, доцентом А. А. Зарубиным.

УДК 004.056.53

МОНИТОРИНГ ТРАНСПОРТНОЙ СЕТИ СВЯЗИ

А. В. Карпов, О. М. Лепешкин, П. А. Новиков, Р. К. Шостак

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

Мониторинг транспортной сети связи в современных условиях разнородности и высокой сложности функционирования сети становится более актуальным. На сегодняшний день мониторинг является одной из самых важных задач, необходимых для ор-

ганизации полноценного управления транспортной сетью. Транспортные сети требуют более точного и гибкого подхода к мониторингу, который осуществляется путем заблаговременной установки средств мониторинга на элементы транспортной сети. Необходима разработка универсальной системы мониторинга, которая позволит в комплексе решить все важнейшие проблемы транспортной сети.

мониторинг, транспортная сеть связи, системы управления сетью, инциденты безопасности, контроль за безопасностью сети.

В настоящее время уделяется огромное внимание контролю состояния сети связи.

На современном этапе транспортные сети можно разделить на три уровня. Сети первого уровня – локальные или местные. Они организуются в городских или сельских местностях. Сети второго уровня – региональные или внутризоновые. Третий уровень – глобальная (магистральная) сеть. При построении транспортных сетей разных уровней сохраняется единообразие в способах транспортировки информации, методах управления сетями и организации синхронизации. Различия в сетях разного уровня состоят лишь в иерархии используемых скоростей, архитектуре сетей (кольцевая, звездообразная, линейная и др.), мощности узлов кросс-коммутации. В качестве линии передачи в транспортных сетях используются волоконно-оптические линии передачи, радиорелейные и спутниковые стволы, коаксиальные кабели [1, 2].

В современных условиях разнородности и высокой сложности функционирования транспортной сети связи все более актуальным становится процесс мониторинга, который представляет собой систему сбора/регистрации, хранения и анализа небольшого количества ключевых (явных или косвенных) признаков/параметров описания данного объекта для вынесения суждения о поведении/состоянии данного объекта в целом. То есть для вынесения суждения об объекте в целом на основании анализа небольшого количества характеризующих его признаков [3, 4].

Мониторинг является одной из самых важных задач, необходимых для организации полноценного управления транспортной сетью. На сегодняшний день средства мониторинга осуществляют контроль за процессами, происходящими в транспортной сети, на основе двух подходов: наблюдение в реальном режиме времени или контроль с записью результатов. Первый подход обычно используют при изыскании путей для оптимизации работы транспортной сети и повышения её эффективности. Второй подход используют, когда мониторинг выполняется автоматически и (или) дистанционно, о последнем случае результаты мониторинга можно передать удаленной службе технической поддержки для установления причин инцидентов безопасности.

Существует два подхода мониторинга транспортной сети связи:

1. Пассивный – регистрация текущего состояния транспортной сети связи.

2. Активный – сбор и обработка данных, а также принятие решения на устранение последствий инцидентов.

Однако, высокие требования, предъявляемые к транспортной сети связи, требуют комплексного подхода к решению всех возникающих проблем работоспособности транспортной сети.

Мониторинг работоспособности транспортной сети связи – должен выполнять постоянное наблюдение за транспортной сетью в поисках медленных или неисправных систем, а при обнаружении таковых сообщает о них администратору сети с помощью средств оповещения. Процесс выявления самих неисправностей и формирования комплекса мероприятий может занять значительное время и существенно повлиять на функционирование системы связи в целом. Частые отказы или длительные периоды неработоспособного состояния сети могут привести к полной потере работоспособности системы связи. Для повышения оперативности принятия мер, способных вернуть транспортную сеть в режим штатного функционирования, необходимо проведение мониторинга сети, который в большей части зависит от человеческого фактора. Профессионального опыта специалиста, зачастую не хватает для оперативной диагностики сети и принятия решения при устранении сбоев в ее работе [5].

Одной из наиболее простых систем мониторинга, или, правильнее сказать, командой для мониторинга, используемой практически во всех небольших организациях, в которых отсутствуют любые программные или аппаратные системы мониторинга, является команда "ping". Контроль осуществляется периодически, при пропадании сети или в постоянном режиме до определенных узлов сети. После того, как выявляется отсутствие связи с каким-либо из узлов сети, проводится уточняющая работа по выявлению конкретной неисправности сети (сети связи, каналообразующая аппаратура и т. п.). Однако использование команды "ping" не позволяет оперативно найти неисправность и требует постоянного операторского присутствия. Зачастую данная команда может просто не работать.

Современные требования к транспортным сетям требуют более точного и гибкого подхода к мониторингу. Сбои и нарушения работы маршрутизаторов могут нарушать связь между различными частями корпорации и ее филиалами. Задача системы мониторинга – это предупреждение, так как перерывы в работе транспортной сети в целом влияют на авторитет организации, коммерческие организации теряют заработок при неработоспособности вычислительной сети, а государственные организации, такие как МВД или МО РФ, теряют управление подразделениями, а, следовательно, неработоспособность транспортной сети может быть прямой угрозой для жизни и здоровья людей.

Поэтому мониторинг безопасности транспортной сети связи необходимо осуществлять путем заблаговременной установки средств мониторинга на элементы транспортной сети. Активизацию средств мониторинга производить с рабочего места администратора. Фиксацию всех инцидентов безопасности, обрабатывать и предоставлять администратору, а по необходимости пользователям [6, 7].

Поэтому исходя из требований, мониторинг транспортной сети связи должен содержать следующие элементы:

– проводить проверку транспортной сети на предмет целостности;

– проводить контроль структуры, состава и процесса функционирования транспортной сети связи (паспорт объекта, структура сети и оборудования);

– выявлять инциденты безопасности и уровень защищенности транспортной сети связи;

– проводить проверку элементов транспортной сети связи на предмет заданному алгоритму функционирования;

– прогнозирование и предотвращение инцидентов безопасности в транспортных сетях связи;

– журналы и отчеты на наличие ошибок: отдельные сообщения об ошибках в журнале событий и накопление, и анализ таких сообщений (помогает выявить неожиданно частые или систематические отказы).

Для создания комплексного подхода средства мониторинга должны иметь элементы, представленные на рис.

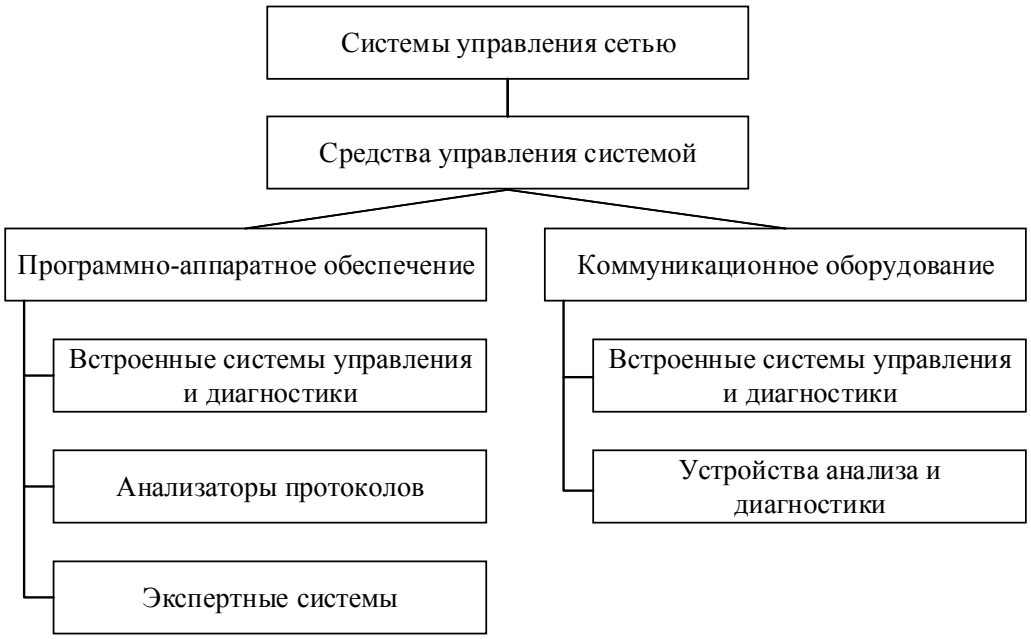


Рисунок. Элементы средств мониторинга

Системы управления сетью, которые собирают данные о состоянии узлов и коммуникационных устройств сети, а также о трафике, циркулирующем в сети. Эти системы не только осуществляют мониторинг и анализ сети, но и выполняют в автоматическом или полуавтоматическом режиме действия по управлению транспортной сетью – включение и отключение портов устройств коммутаторов и маршрутизаторов и т. п.

Средства управления системой часто выполняют функции, аналогичные функциям систем управления, но по отношению к другим объектам. В первом случае объектом управления является программное и аппаратное обеспечение пользователей сети, а во втором – коммуникационное оборудование. Вместе с тем, некоторые функции этих двух видов систем управления могут дублироваться, например, средства управления системой могут выполнять простейший анализ сетевого трафика.

Встроенные системы диагностики и управления, исполненные в виде программно-аппаратных модулей, устанавливаемых в коммуникационное оборудование

Анализаторы протоколов, представляющие собой программные или аппаратно-программные системы, которые ограничиваются, в отличие от систем управления, лишь функциями мониторинга и анализа трафика в сетях.

Экспертные системы аккумулирующие человеческие знания о выявлении причин ненормальной работы транспортной сети и возможных способах приведения сети в работоспособное состояние.

Устройства анализа и диагностики**,** совмещающие функции нескольких устройств.

Имеющиеся системы мониторинга транспортной сети связи являются узконаправленными, решающими определенные задачи, не способными видеть всю проблему в целом. Необходима разработка универсальной системы мониторинга, которая позволит в комплексе решить все важнейшие проблемы транспортной сети. Универсальная система мониторинга должна обеспечить контроль за безопасностью сети, работоспособностью оборудования и оконечного оборудования пользователей, в том числе контроль наличия или отсутствия технического обслуживания всех элементов. Все указанное позволит обеспечить своевременное реагирование на все возникающие неисправности, в некоторых случаях даже до их возникновения, сократить временные и трудовые затраты на восстановление транспортной сети после возникновения неисправностей.

Список используемых источников

1. Лепешкин О. М., Корсунский А. С. Оптимизация структуры комплекса информационно-технических средств в автоматизированных системах управления // Автоматизация процессов управления. 2011. № 4. С. 76–81.

2. Корсунский А. С., Лепешкин О. М. Подход к формализации автоматизированной информационной системы для оценки функциональной безопасности // Вопросы радиоэлектроники. 2012. Т. 3. № 1. С. 75–82.

3. Бударин Э. А., Васюков Д. Ю., Дементьев В. Е., Колбасова Г. С., Краснов В. А., Лепешкин О. М., Лаута О. С., Митрофанов М. В., Худайназаров Ю. К. Обеспечение защиты информации в локальных вычислительных сетях; Военная академия связи им. Маршала Советского Союза С. М. Буденного. Санкт-Петербург, 2013.

4. Лепешкин О. М., Карпов А. В., Шостак Р. К. Актуальность осуществления сетевого контроля защищенности информационных сетей // Радиолокация, навигация, связь. Сборник трудов XXIII Международной научно-технической конференции. В 3-х томах. 2017. С. 1198.

5. Акинин П. В., Блинников В. А., Братков В. В., Гундарь О. Н., Медведев Н. П., Сергодеева Е. А., Снимщикова Е. В., Арискина А. В., Бабин И. А., Копытов В. В., Косов Г. В., Кузьмин Д. С., Росенко А. П., Шульга М. М., Лепешкин О. М., Бурым Ю. В. Угрозы безопасности Росии на Северном Кавказе; Ставрополь, 2004.

6. Иванов Д. А., Коцыняк М. А., Лаута О. С., Нечепуренко А. П. Модель распределения факторов информационного воздействия по элементам информационно-телекоммуникационной сети // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2017). VI Международная научно-техническая и научно-методическая конференция: сборник научных сетей : в 4 т. 2017. С. 420–425.

7. Коцыняк М. А., Иванов Д. А., Лаута О. С., Нечепуренко А. П. Методика оценки защищенности информационно-телекоммуникационной сети в условиях информационного противодействия // Радиолокация, навигация, связь. Сборник трудов XXIII Международной научно- технической конференции. В 3-х томах. 2017. С. 83–89.

УДК 681.5.391.21

СПОСОБ СЕТЕВОГО МОНИТОРИНГА ОБЪЕКТОВ И СИСТЕМ СВЯЗИ

А. В. Карпов, О. М. Лепешкин, П. А. Новиков, Р. К. Шостак

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

В статье рассмотрены вопросы мониторинга объектов и систем связи и управления в целях обеспечения их доступности, надежности и работоспособности. При существующих принципах построения систем управления и сетей связи подвижного сегмента для их функционального взаимодействия в едином информационном пространстве и выполнения задач по обеспечению устойчивого информационного обмена, необходим новый подход к мониторингу подвижных объектов связи.

мониторинг; доступность; надежность; работоспособность; подвижный сегмент; единое информационное пространство; устойчивый информационный обмен; подвижные объекты связи.

Современные сети и коммуникации должны оперативно реагировать на атаки, сохраняя свою доступность, надежность и работоспособность. Во многих отношениях целью процесса обеспечения безопасности является повышение отказоустойчивости сетей [1].

При существующих принципах построения систем управления и сетей связи подвижного сегмента для их функционального взаимодействия в едином информационном пространстве и выполнения задач по обеспечению устойчивого информационного обмена, необходим новый подход к мониторингу подвижных объектов связи, который обеспечивал бы выполнение следующих функций:

– предварительно задавать вид и уровень опасности неисправностей подсистем и систем в целом, соответствующие им пороговые значения параметров технического состояния, допустимые значения функциональных параметров, разрешенные режимы функционирования и допустимые значения параметров регламентного состояния сетей связи [2];

– диагностировать параметры технического состояния контролируемого объекта при помощи расположенных на них компьютерных средств мониторинга и диагностики регламентного состояния;

– формировать управляющее воздействие по ближайшим неотложным действиям, направленным на устранение неисправностей и нарушений в режимах работы, недопущение развития уровня опасности и снижение влияния неисправностей и нарушений на безопасность объекта и системы в целом;

– формировать сводную диагностическую информацию о регламентном состоянии контролируемой системы;

– автоматически формировать сводную информацию о нарушениях установленных режимов функционирования;

– отображать результаты контроля на экране средства мониторинга;

– сравнивать измеренные значения параметров регламентного состояния с предварительно заданными значениями [3];

– оценивать техническое состояние узлов, агрегатов, подсистем и объекта в целом;

– фиксировать нарушения предварительно заданных разрешенных режимов функционирования;

– автоматически определять вид и уровень опасности неисправностей и нарушений установленных регламентных состояний;

– автоматически формировать управляющий сигнал (воздействие) по ближайшим неотложным действиям, направленным на определение неисправного элемента, узла, агрегата, недопущение развития уровня опасности неисправности и снижения влияния неисправности на безопасность объекта [4].

С целью представления сетевого мониторинга объектов и систем связи используем разложение Хевисайда (1). Суть разложения Хевисайда заключается в том, что исследуется не система, а процесс, который она реализует. Сложный процесс декомпозируется на элементарные процессы, каждый из которых характеризуется функцией распределения, средним временем и его дисперсией [5].

$$h(s)=\sum_{k-1}^{n}\frac{f(s_k)}{\varphi'(s_k)}\cdot\frac{1}{s-s_k}=\sum_{k=1}^{5}\frac{w\cdot m\cdot l\cdot P_n\cdot d\cdot(z+s_k)}{5s_k^4+4A\cdot s_k^3+3B\cdot s_k^2+2C\cdot s_k+D}\cdot\frac{1}{s-s_k}, \quad (1)$$

где w – возможность обнаружения объекта мониторинга; m – возможность выявления изменения состояния; d – возможность воздействия на объект мониторинга; l – возможность отличить один объект от другого; z – возможность распознавания назначения объекта, тогда:

$$h(t)=L^{-1}\{h(s)\}=\sum_{k=1}^{5}\frac{w\cdot m\cdot l\cdot P_n\cdot d\cdot(z+s_k)}{5s_k^4+4A\cdot s_k^3+3B\cdot s_k^2+2C\cdot s_k+D}\cdot\exp[s_k t]. \quad (2)$$

Полученное выражение (2) является функцией плотности вероятностей, поэтому искомая интегральная функция распределения вероятностей определяется так:

$$F(t)=\int_0^t h(t)dt=\sum_{k=1}^{5}\frac{w\cdot m\cdot l\cdot P_n\cdot d\cdot(z+s_k)}{5s_k^4+4A\cdot s_k^3+3B\cdot s_k^2+2C\cdot s_k+D}\cdot\frac{1-\exp[s_k t]}{-s_k}, \quad (3)$$

а среднее время T чувствительности к деструктивным воздействиям (ТСР) определится так:

$$\overline{T}=\int_0^\infty t\cdot h(t)dt=\sum_{k=1}^{5}\frac{w\cdot m\cdot l\cdot P_n\cdot d\cdot(z+s_k)}{5s_k^4+4A\cdot s_k^3+3B\cdot s_k^2+2C\cdot s_k+D}\cdot\frac{1}{(-s_k)^2}, \quad (4)$$

Зависимости $F(t)$ (3) и T (4) представлены на рисунке. В качестве исходных данных используются следующие значения времени и вероятности, соответствующие профильной модели сетевого мониторинга:

t_w = 7 мин., t_m = 5 мин., t_d = 18 мин., t_l = 5 мин., t_z = 5 мин.
D_n = 0,1…..0,9

Анализ представленной зависимости показывает, что совокупность приведенных факторов позволит обеспечить возможность повышения оперативности предупреждения развития инцидентов безопасности; повышения объективности контроля; повышения оперативности реакции системы мониторинга на инциденты безопасности; повышения оперативности для своевременного предотвращения инцидентов безопасности; обеспечение

возможности прогнозирования и анализа изменений состояния динамических объектов мониторинга и адаптации системы защиты.

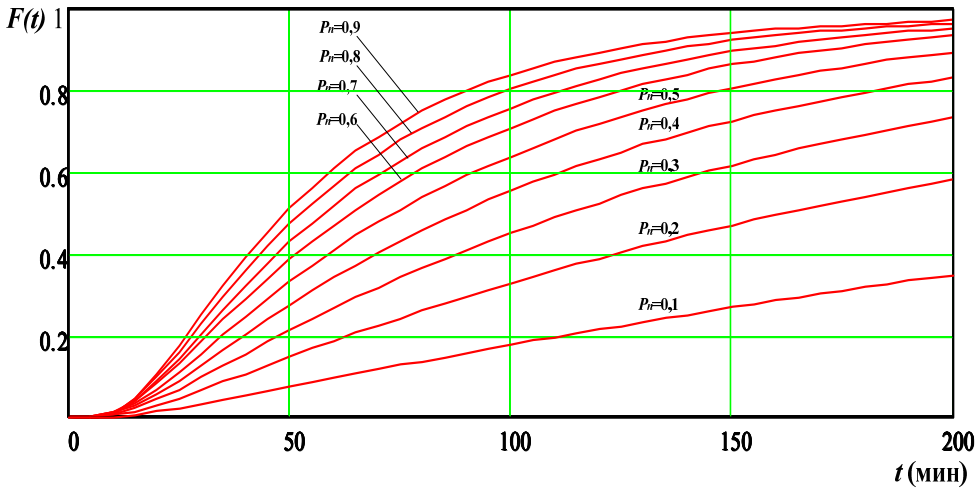


Рисунок. Зависимость интегральной функции распределения вероятности от времени осуществления сетевого мониторинга

Список используемых источников

1. Лепешкин О. М., Карпов А. В., Шостак Р. К. Актуальность осуществления сетевого контроля защищенности информационных сетей // Радиолокация, навигация, связь. Сборник трудов XXIII Международной научно-технической конференции. В 3-х томах. 2017. С. 1198.

2. Лепешкин О. М., Корсунский А. С. Оптимизация структуры комплекса информационно-технических средств в автоматизированных системах управления. Автоматизация процессов управления. 2011. № 4. С. 76–81.

3. Бударин Э. А., Васюков Д. Ю., Дементьев В. Е., Колбасова Г. С., Краснов В. А., Лепешкин О. М., Лаута О. С., Митрофанов М. В., Худайназаров Ю. К. Обеспечение защиты информации в локальных вычислительных сетях; Военная академия связи им. Маршала Советского Союза С. М. Буденного. Санкт-Петербург, 2013. 138 с.

4. Карпов А. В., Лепешкин О. М., Попов Н. А. Структура электромагнитного поля при нелинейной радиолокации // Радиолокация, навигация, связь. Сборник трудов XXIII Международной научно-технической конференции. В 3-х томах. 2017. С. 1118.

5. Коцыняк М. А., Иванов Д. А., Лаута О. С., Нечепуренко А. П. Методика оценки защищенности информационно-телекоммуникационной сети в условиях информационного противодействия // Радиолокация, навигация, связь. Сборник трудов XXIII Международной научно-технической конференции. В 3-х томах. 2017. С. 83–89.

УДК 004.056

РАЗРАБОТКА ПРОЕКТА МОДЕРНИЗАЦИИ СЕТИ ПРОВАЙДЕРА С ВНЕДРЕНИЕМ СЕРВИСОВ НА БАЗЕ MPLS

П. В. Карельский, М. М. Ковцур, К. С. Рязанцев

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

Технология MPLS активно используется при построении новых сетей сервис-провайдеров. Однако возникает необходимость предоставления MPLS-сервисов поверх существующих сетей, что приводит к частичной модернизацию сети. В рамках доклада определяются количественные характеристики, играющие важную роль при выборе оборудования для предоставления сервисов MPLS L2/L3 VPN.

многопротокольная коммутация по меткам, MPLS, L2/L3 VPN, характеристики оборудования, защита сервисов MPLS.

В настоящее время в сетях операторов связи при предоставлении услуг широко применяются сервисы L2/L3 VPN на базе технологии MPLS. Однако в некоторых случаях имеющееся оборудование оператора не поддерживает эту технологию. В этом случае – возникает потребность в обновлении парка устройств. Рассмотрим сеть, в которой необходимо реализовать предоставление сервисов на базе MPLS. Анализ имеющегося оборудования показал, что не все оборудование поддерживает MPLS и требуется модернизация сети.

Однако при обновлении оборудования возникает пара вопросов:

– На что обращать свое внимание при выборе оборудования?
– Какие характеристики являются наиболее значимыми?

Анализ представленных на рынке решений показал, что в основном производители уделяют внимание цене и описанию характеристик, нежели количественным параметрам оборудования. В ходе работы была составлена таблица 1 с характеристиками оборудования нескольких производителей [1, 2, 3].

В результате исследования механизмов работы MPLS технологии, а также L2/L3 VPN сервисов на ее основе, были выделены следующие, наиболее важные характеристики оборудования, представленные в таблице 2.

ТАБЛИЦА 1. Пример характеристик оборудования различных вендоров

Характеристика	Juniper EX4550	Raisecom iTN8800	Juniper MX-104	Juniper QFX5100	Cisco ASR 9K
Количество MAC адресов	32K	32K	512K	288K	512K
Емкость таблицы FIB IPv4	14 K	16K	4M	100K	128K
Емкость таблицы RIB	10K	–	21M	–	–
Max Pseudo Wires	–	4K	16K	–	4K
Max L2VPN (Kompella)	–	–	2K	–	–
VRF	254	1K	2K	1K	4K
MPLS Labels	125	–	–	16K	16K
Цена, тыс. руб.	от 150	от 400	от 500	от 800	от 900

ТАБЛИЦА 2. Взаимосвязь характеристики оборудования и сервисов

L2VPN сервис	Количество LDP соседей	Количество VSI	Количество PW	
L3VPN сервис	Количество FIB/RIB	Количество сессий BGP	Количество IGP соседей	Количество VRF
Общее для сервисов	Количество MAC адресов	Количество LSP	MPLS Labels	

Для модернизации сети необходимо выбрать наиболее оптимальное оборудование. В рамках статьи выполнен расчет для L2 VPN сервиса с топологией точка-точка (рис. 1). Задачей данного расчета является определение нехватки ресурсов оборудования.

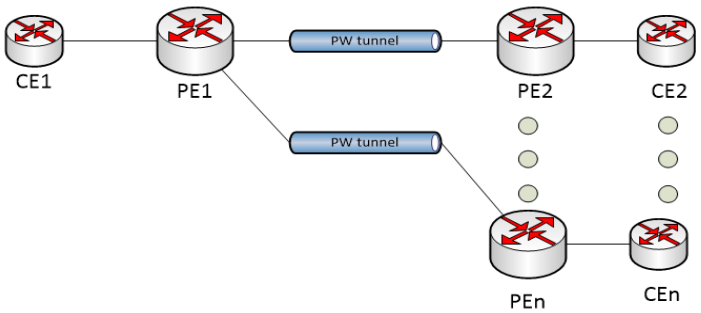


Рис. 1. Топология точка-точка

Введем допущение, что выбираемое для сети оборудование будет иметь следующие характеристики:

M = 30900 – количество максимально поддерживаемых MAC адресов;

MLN = 30 – количество максимально поддерживаемых LDP соседей;

MPL = 8000 – количество максимально поддерживаемых MPLS меток;

Расчет выполнен с учетом следующих характеристик решения:

D = 30, 100 – количество устройств на сети оператора;

NoC – число клиентов, подключенных к одному устройству;

MpC = 100 – число MAC адресов на одного клиента.

Необходимо оценить процент использования ресурсов оборудования исходя из технических характеристик MPLS устройств, числа возможных клиентов, а также параметров клиента.

Определим расход MAC адресов на число клиентов – MpC. Эта характеристика показывает, какое количество MAC адресов будет приходиться на одного клиента при равномерном распределении адресов. Используем отношение:

$$MpC = \frac{M}{NoC},$$

где M – количество MAC адресов, поддерживаемых оборудованием, NoC – число подключенных клиентов.

Рис. 2. Расход MAC адресов

Из рис. 1 видно, что с ростом числа клиентов меньшее число адресов приходится на одного клиента, при равном распределении адресов.

Далее выполним оценку использования таких характеристик как процент использования MAC адресов (MAC *Usage*), LDP соседей (LDPN *Usage*), меток (Label *Usage*) для разного количества устройств:

$$MAC\ Usage = \frac{MpC*NoC+D*MpD}{M},$$

$$LDPN\ Usage = \begin{cases} \frac{NoC}{MLN}, \text{при } NoC \le MLN \text{ и } NoC < D \\ \frac{D}{MLN}, \text{при } NoC \le MLN \text{ и } NoC \ge D \\ \frac{D}{MLN}, \text{при } NoC > MLN \text{ и } D \le MLN \\ 1 \text{ при } NoC > MLN \text{ и } D > MLN \end{cases},$$

$$Label\ Usage = \frac{NoC+D}{MPL},$$

где MpC – число MAC адресов на одного клиента, NoC – число клиентов, подключенных к одному устройству, D – количество устройств на сети клиента, MpD – количество MAC адресов на устройство, M – количество MAC адресов, MLN – количество максимально поддерживаемых LDP соседей, MPL – количество максимально поддерживаемых MPLS меток.

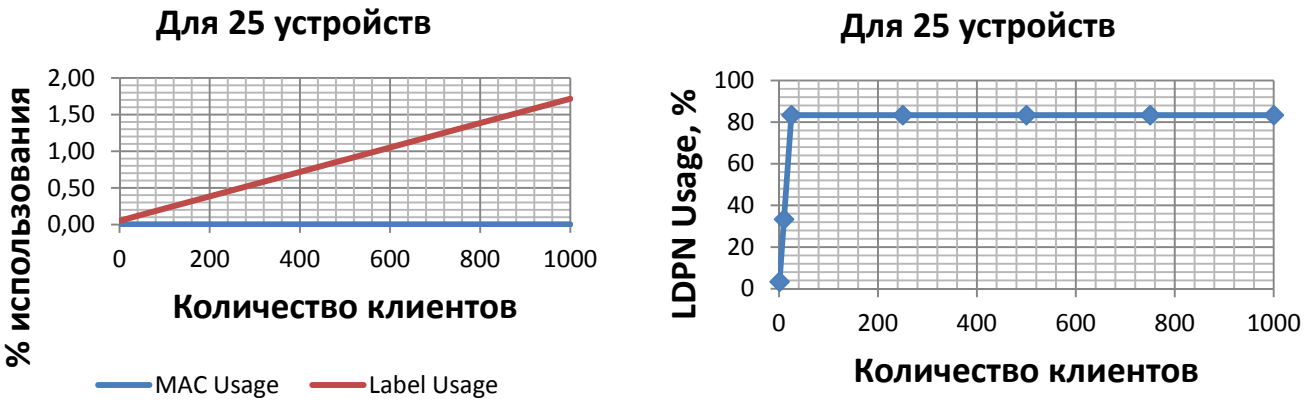


Рис. 3. График и расхода характеристик для 25 устройств

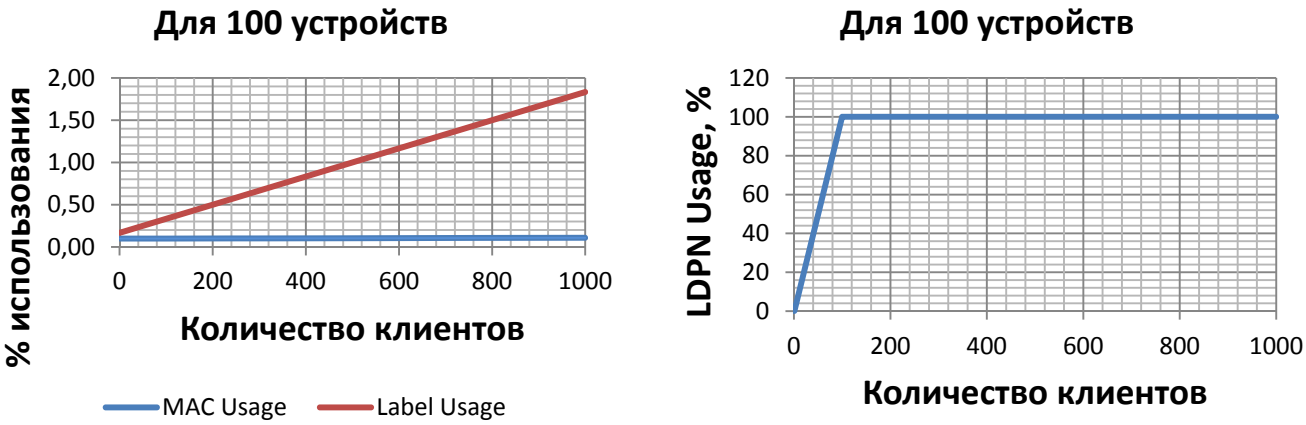


Рис. 4. Графики расхода характеристик для 100 устройств

Из рис. 3–4 видно, что с ростом количества устройств использование характеристик увеличивается. Можно сделать вывод, что для выбранной топологии и оборудования наиболее значимой характеристикой является количество соседей LDP. При числе клиентов более MLN, подключенных к одному MPLS-устройству и терминирующихся в других несовпадающих устройствах, требуется использовать функционал H-VPLS [4].

С точки зрения сетевой безопасности, технологии MPLS L2/L3 VPN предлагают новый уровень защиты сетевого трафика. Несмотря на то, что пакеты передаются по одной и той же опорной сети, трафик каждого клиента внутри L2VPN получается изолированным [5]. Однако для обеспечения информационной безопасности (ИБ) решения требуется активировать механизмы ИБ на плоскости данных, плоскости управления трафиком и плоскости управления устройством на каждом из элементов сети [6, 7].

В статье рассмотрены особенности, которые стоит учитывать при выборе оборудования для модернизации сети. Произведен расчет масштабируемости и выявлен наиболее значимый показатель при построении L2 VPN по топологии точка-точка.

Список используемых источников

1. IP-MPLS PE and Pre-Aggregation System [Электронный ресурс] // Режим доступа: https://www.raisecom.com/
2. MPLS: Layer 2 VPNs, Configuration Guide [Электронный ресурс] // Режим доступа: https://cisco.com/
3. TechLibrary [Электронный ресурс] // Режим к доступу: https://www.juniper.net/
4. Ковцур М. М. Исследование непересекающихся маршрутов глобальной сети // Наука вчера, сегодня, завтра. № 6 (6): сб. ст. по материалам VI международной научно-практической конференции. – Новосибирск : СибАК, 2013. С. 19–24.
5. Бухарин В. В., Липатников В. А., Сахаров Д. В. Метод управления информационной безопасностью организации на основе процессного подхода // Информационные системы и технологии. 2013. № 3 (77). С. 102–109.
6. Алейников А. А., Билятдинов К. З., Красов А. В., Левин М. В. Контроль, измерение и интеллектуальное управление трафиком: монография. СПб. : Центр «Астерон», 2016. 92 с. ISBN 978-5-00045-385-8.
7. Service Provider Security. URL: https://www.cisco.com/c/en/us/about/security-center/service-provider-infrastructure-security.html

УДК 004.733

РАЗРАБОТКА МОДЕЛЕЙ И МЕТОДОВ ВЗАИМОДЕЙСТВИЯ БЕСПИЛОТНЫХ АВТОМОБИЛЕЙ В УМНЫХ ГОРОДАХ И ПОСЕЛЕНИЯХ

Р. В. Киричек, А. В. Шкляева

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

За последние годы возрос интерес производства и использования беспилотных автомобилей. Это часть будущего, где «умные» автомобили будут транспортировать нас в различные места без водителей. Для этого необходимо разработать инфраструктуру, которая позволит беспилотному автомобилю взаимодействовать 24 часа в сутки со всеми участниками дорожного движения при помощи сетевых технологий при минимальных задержках.

беспилотный автомобиль, сетевые технологии, инфраструктура, V2V, V2I, интеллектуальная транспортная система.

В наше время автомобильная индустрия претерпевает значительные изменения. За последние несколько лет многие мировые компании инвестируют свои денежные средства в производство беспилотных автомобилей. Развитие беспилотного транспорта должно подкрепляться готовностью инфраструктуры: выделенными полосами движения, специальной разметкой, дорожными знаками и светофорами. Кроме того, беспилотное транспортное средство должно быть подключено к сети связи в режиме реального времени 24/7, чтобы обеспечить его полной картиной о дорожной ситуации и возможных проблемах, а также иметь возможность отправлять данные о состоянии автомобилей и пассажиров на выделенные серверы. В будущем такой транспорт станет массовым и вполне привычным явлением, но перед этим необходимо проработать телекоммуникационную составляющую инфраструктуры беспилотных автомобилей в умных городах с конкретными параметрами движения и интернетом.

Общие принципы работы беспилотных автомобилей

Все беспилотные автомобили базируются на одном принципе работы, который включает в себя следующие функции [1]: цифровая обработка данных с датчиков; построение модели дороги; построение карты местоположения автомобиля; выбор стратегии управления; распознавание участников дорожного движения; моделирование поведения объектов на дороге.

Рассмотрим на примере автомобиля Toyota Prius от Google (рис. 1) [2].

Рис. 1. Модель беспилотного автомобиля с используемыми датчиками

Датчики, установленные на автомобиле, собирают информацию о самом автомобиле и окружающей обстановке (наличие препятствий, пешеходов, дорожных знаков и светофоров). Программное обеспечение обрабатывает полученные данные и определяет дальнейшие маршруты.

Все беспилотные автомобили имеют несколько камер, которые смотрят в разных направлениях. Это помогает определить наличие других машин, людей и животных, а также распознать разметку на проезжей части и знаки дорожного движения. Для того чтобы установить расстояние до предметов, на машине присутствуют стереокамеры.

Для более точного определения расстояний до объектов, окружающих автомобиль, составляется трёхмерная карта при помощи лидара (рис. 2). Данная технология получает и обрабатывает информацию с помощью оптических систем.

Помимо лидара и камер, используются показания с радара. С его помощью расстояние до объектов определяется с помощью радиоволн. Радар позволяет «видеть» на более дальние расстояния, чем лидар, за счет более узкого угла обзора, что очень важно при высоких скоростях движения.

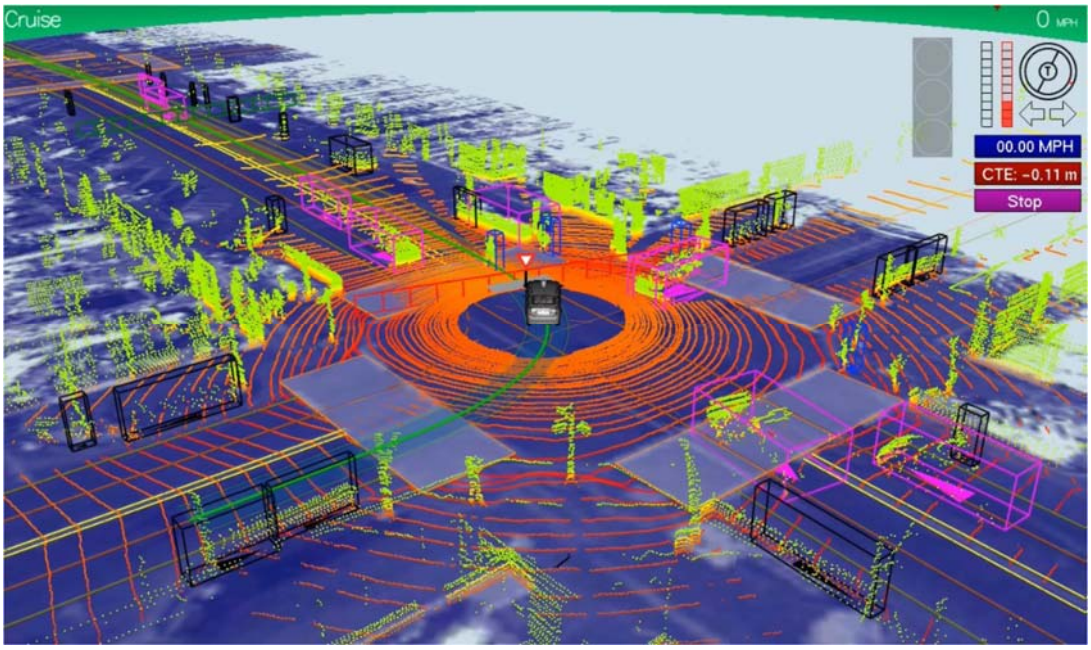


Рис. 2. 3D-карта окружающего пространства, построенная при помощи лидара

Приемники GPS/GLONASS определяют местоположение, направление и скорость передвижения [3].

Интеллектуальная транспортная система

Разработкой интеллектуальной транспортной системы (ITS) [4] с большим спектром возможностей занимаются такие крупные организации,

как ETSI, IEEE, 3GPP и т. д. Современные ITS применяются для помощи водителю транспортного средства. Данные системы оповещают об опасности на дорогах, предупреждают о возможном столкновении, о проведении дорожных работ и пр. Децентрализованные базы данных смогут информировать об опасных зонах, о дорожной обстановке, погодных условиях.

Безопасное и эффективное дорожное движение беспилотников будет возможно при обмене информацией между автомобилями по средствам V2V-систем, а также вместе с получением информации о ситуации на дорогах и актуальных цифровых карт дорог через V2I-системы.

Система V2V (*vehicle-to-vehicle*) – «транспортное средство – транспортное средство», благодаря обмену данными между автомобилями обеспечивает безопасное вождение на участках дорог с плохой видимостью. Такая система может предотвращать столкновения, оповещать о неполадках автомобиля, предоставлять полную картину дорожной обстановки. Например, две машины, которые двигаются по перекрестку, но не видны друг другу, обмениваются между собой своими координатами и скоростью движения через V2V-систему и избегают столкновения.

Система V2I (*vehicle-to-infrastructure*) – «транспортное средство – придорожная инфраструктура» обеспечивает передачу данных между автомобилем и придорожным оборудованием (сенсоры, базы данных, сервера) посредством радиосвязи. Например, на перекрестке произошла авария, придорожные датчики это обнаружат и передадут информацию приближающимся автомобилям о дорожной обстановке и о том, что необходимо снизить скорость движения или изменить маршрут следования. Это будет возможно благодаря V2I-системам.

Как уже говорилось ранее, в автомобиль встраивается очень много различным сенсоров. Передача данных телематических и телеметрических систем предполагает использование сотовой связи и технологии Wi-Fi. Поэтому в «беспилотнике» необходим еще один датчик для применения этих технологий. Автомобиль сможет взаимодействовать не только с другим транспортом и придорожной инфраструктурой, но и с различными гаджетами человека (рис. 3). Так может появится система V2X (*vehicle-to-everything*) – «транспортное средство, подключенное ко всему», которая получит наибольшее распространение за счет использования радиотехнологий в автомобилях для обеспечения безопасности на дорогах [5].

На пути к переходу к беспилотным автомобилям еще предстоит решить множество технологических задач. Но одна из самых главных – это обеспечение автомобилей высокоскоростным сетевым подключением. Максимально оперативно получать информацию и обмениваться ею с другими автомобилями и придорожной инфраструктурой будет возможно в сетях пятого поколения. В сетях 5G ожидаются минимальные задержки. Предпола-

гается, что средняя скорость скачивания в 5G-сетях для пользователей составит 100 Мбит/с, при этом время ожидания не превысит 4 мс (для 4G LTE этот значение составляет около 20 мс). Такие данные предполагает первая версия спецификации Международного Союза Электросвязи.

Рис. 3. Взаимодействие беспилотных автомобилей
со всеми участниками «умного» города

Актуальную информацию о дорожном движении необходимо доставлять беспилотному автомобилю с минимальной задержкой (около 1–10 мс). Для обеспечения такой задержки сети необходимо разработать типовую архитектуру телекоммуникационной инфраструктуры, которая будет обеспечивать непрерывную связь между беспилотными автомобилями и удаленными серверами с минимальными задержками [6].

Список используемых источников

1. Jarasuniene A. Research into Intelligent Transport Systems (ITS) Technologies and Efficiency // Transport. 2007. Vol. 22. pp. 61–67.

2. Автопилот. Беспилотный автомобиль. URL: http://www.tadviser.ru/index.php/

3. Man L., Yuhe Z., and Wenjia W. Analysis of congestion points based on probe car data // in IEEE Int. Conf. on Intell. Transp. Syst., Missouri, USA, 2009, pp. 1–5.

4. The National ITS Architecture U.S. Department of Transportation. URL: http://www.iteris.com/itsarch/index.htm

5. Driverless Cars Are Further Away Than You Think. URL: https://www.technologyreview.com/s/520431/driverless-cars-are-further-away-than-you-think/

6. ISO 26262-1:2011. Road vehicles – Functional safety – Part 1: Vocabulary. URL: https://www.iso.org/standard/43464.html

УДК 004.9

IOT-ПЛАТФОРМА ДЛЯ УПРАВЛЕНИЯ ЖИЛИЩНО-КОММУНАЛЬНЫМ ХОЗЯЙСТВОМ КАК PAAS-ПРОДУКТ ОПЕРАТОРА СВЯЗИ

С. В. Кисляков, Н. Э. Краснов

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

В статье описывается модель комплексного PaaS (Platform as a Service) решения по автоматизации жилищно-коммунального хозяйства (ЖКХ) с использованием технологии Интернета вещей. Предлагаемое решение предназначено для контроля и учёта расхода различного рода ресурсов со стороны служб ЖКХ, а также для управления и поддержки эксплуатации телекоммуникационного и оконечного оборудования со стороны оператора связи.

OSS/BSS, NRI, PaaS, IoT, Умный дом.

Концепция Интернет вещей (IoT) с момента своего появления привлекала внимание операторов связи своим потенциалом с точки зрения разработки новых услуг их последующей монетизации [1]. На сегодняшний день существует довольно много известных платформ [2]. Анализ показал, что в текущей рыночной ситуации наиболее экономически оправданным решением для оператора связи будет создание решения на базе уже существующего ИТ-ландшафта, а не покупка или разработка новой платформы. Оператор связи, особенно крупный, уже имеет сформированный OSS-ландшафт, состоящий из множества систем. Анализ функциональных требований к решению позволил выявить те системы в ИТ-ландшафте оператора, которые должны быть задействованы в разрабатываемом решении [1, 3, 4]. Так же стало ясно, какие именно из эксплуатационных задач – технического учёта, исследования сети (*discovering*), биллинга, мониторинга [1, 3] – должны поддерживаться решением.

В статье описывается решение в последовательности «выбор бизнес-модели» – формирование функциональных требований – описание архитектуры решения.

Описание бизнес-модели

Предоставление любой услуги невозможно без разработки бизнес-модели, она необходима для четкого понимая взаимодействия всех участников деятельности.

Экосистема IoT подразумевает несколько бизнес-ролей. Каждый участник деятельности играет как минимум одну бизнес-роль, однако ролей может быть и больше [5] (рис. 1).

Рис. 1. Связь между ролями в экосистеме IoT

Рассмотрим бизнес-модель выбранную на основе рекомендации Y.2060 ITU-T (рис. 2).

Рис. 2 Бизнес-модель для оператора связи для решения по автоматизации ЖКХ на основе IoT

Используя предложенную стандартную модель, конкретизируем роли оператора и управляющей компании в решении. Поставщиком платформы является оператор, который на базе своей сети предоставляет решение управляющей компании. Соответственно, управляющая компания будет выступать в роли абонента приложений. Сами по себе устройства IoT должны будут устанавливаться управляющей компанией, которая и будет отвечать за их тарификацию и обслуживание.

Функциональные требования к IT-ландшафту оператора связи

Современные методы построения IT-ландшафта оператора связи основаны на концепции Frameworx, TMForum [6, 7, 8], которая определяет, как наиболее грамотно и рационально проектировать и внедрять новые услуги и сервисы в IT-ландшафт оператора.

Для решения по автоматизации жилищно-коммунальных хозяйств необходимо определить основные бизнес-процессы [6] и бизнес-приложения [7] карт eTOM (*Enhanced Telecom Operations Map*) и TAM (*Telecom Application Map*).

Бизнес-процессы, поддерживаемые решением, следующие:

– Обеспечение и поддержка готовности процессов уровня услуг.
– Конфигурация и активация услуг.
– Управление решением проблем на уровне услуг.
– Поддержка и обеспечение готовности ресурсов.
– Управление людскими ресурсами.
– Обеспечение услуги ресурсами.
– Учёт использования ресурсов.
– Сбор и предоставление информации от ресурсов.

Выделим конкретные стандартные (на основе карты TAM) программные приложения, отвечающие за поддержку этих бизнес-процессов:

– развитие ресурсов и управление ими (*Resource management*);
– управление учетом ресурсов (*Resource inventory management*);
– управление заявками на предоставление ресурсов (*Resource order management*);
– управление учетом услуг (*Service inventory management*);
– управление заявками на предоставление услуг (*Service order management*);
– управление людскими ресурсами (*Workforce management*).

Описание технической реализации решения

В перечень технических средств решения входят следующие (рис. 3):

– базовая станция – выступает в роли агрегатора и контроллера для интернет-вещей;

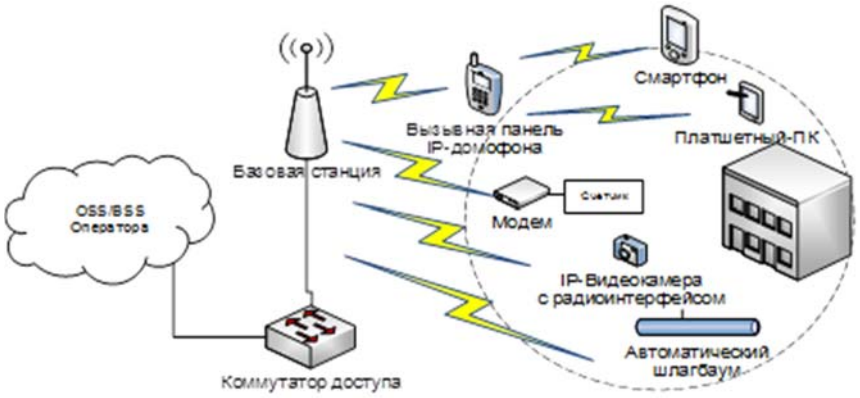


Рис. 3. Визуализация технического решения

– коммутатор доступа – необходим для доступа в сеть оператора;
– IP-Домофон – устройство для вызовов на смартфон пользователя;
– IP-Камера – устройство для видеосъемки на парковках и у подъездов;

– автоматический шлагбаум – устройство контролирующее доступ во двор посредством распознавания номера автомобиля.

– счетчик с установленным на нём модемом – комплексное устройство для автоматизации поверки показаний счетчиков газа/воды/электричества.

Заключение

Предложенное решение не требует больших финансовых вложений от оператора, так как хорошо встраивается в уже существующую ИТ-инфраструктуру. Можно утверждать, что требуемые технические доработки ИТ-систем, задействованных в решении, тоже будут не значительны. При этом предложенное решение позволяет оператору занять своё конкретное место на рынке IoT продуктов.

Список используемых источников

1. Самуйлов К. Е., Чукарин А. В., Яркина Н. В. Бизнес-процессы и информационные технологии в управлении современной инфокоммуникационной компанией. М. : РУДН, 2009. 442 с.
2. Pathirana D., Sonnadara S., Hettiarachchi M., Siriwardana H., Silva C. WireMe – IoT Development Platform for Everyone // 2017 Moratuwa Engineering Research Conference (MERCon), pp.93–98.
3. Кучерявый А. Е. Интернет Вещей // Электросвязь. 2013. № 1. С. 21–24.
4. Соколов Н. А. Сценарии реализации концепции «Интернет вещей» // Первая миля 2016. № 4. С. 50–54.
5. Рекомендация ITU-T Y.2060 «Обзор интернета вещей» 06.2012.
6. GB921 Business Process Framework (eTOM) R17.5.0 TM Forum, 2018.
7. GB929 Application Framework R17.5.0 TM Forum 2018.
8. GB922 Information Framework (SID) R17.5.0 TM Forum, 2018.

УДК 65.011.56

АНАЛИЗ ТОЧЕК УПРАВЛЯЮЩЕГО ВОЗДЕЙСТВИЯ СО СТОРОНЫ OSS-МОДУЛЯ НА ПРОГРАММНО-КОНФИГУРИРУЕМУЮ СЕТЬ

С. В. Кисляков, Н. С. Плетнева

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

В статье рассматривается базовая модель интеграции OSS/BSS среды и сетей SDN, функциональные требования и подход к построению OSS на сети SDN. Выделены основные проблемы, связанные с переходом к сетям SDN. Актуальность данной темы

обусловлена стремительным ростом популярности сетей SDN, главным достоинством которой является экономичность и независимость от производителя.

программно-конфигурируемая сеть, SDN, контроллер, оператор связи.

Сегодняшняя архитектура OSS/BSS построена на прочном, но стареющем фундаменте, разработанном в течение нескольких десятилетий для телекоммуникационных услуг, которые были относительно статичны и предсказуемы. Концепция SDN (*Software-defined Networking*, также программно-определяемая сеть) характеризуется рядом ощутимых преимуществ: сервисы будут распределены по общей базовой инфраструктуре и организованы гибко и динамично – что также положительно влияет на управление сетью.

Для операторов связи внедрение новых виртуализированных сервисов в гибридной среде требует не только трансформации существующей OSS/BSS, но и поддержки новых дополнительных возможностей и услуг, предоставляемых NFV (Виртуализацией сетевых функций).

Для автоматизации новых возможностей в новых OSS необходимо реализовать [1]:

– управление виртуальными сетевыми ресурсами в режиме реального времени;

– динамическое управление состоянием сети в режиме реального времени (управляемое контроллерами SDN);

– операции на основе API с расширенной автоматизацией;

– возможность моделирования новых типов ресурсов и поддержки новых интерфейсов.

Трансформацию OSS/BSS традиционно определяют рабочие группы аналитиков и разработчиков компаний, входящих в состав членов организации TM Forum. Их наработки отражаются в документах TM Forum и служат стандартами «де факто» для разработки OSS/BSS [2].

Анализ карты eTOM под влиянием SDN/NFV

Анализируя релиз карты eTOM (18.0) можно отследить изменения в сторону SDN/NFV. В частности, появились шаблоны общих процессов, имеющих дело с каталогами продуктов и услуг и ёмкостью. Появились шаблоны, регулирующие определение и использование ёмкости и ёмкости по требованию.

В процессах стратегии, инфраструктуры и продукта добавилось управление торговой маркой, исследование рынка, управление маркетинговой кампанией, что означает продвижение продуктов и услуг через различные среды, включая телевидение, СМИ, интернет, в целях выхода на рынок и привлечения клиентов [3].

Анализ TAM под влиянием внедрения SDN/NFV

Домен «Клиент» (*Customer Domain*) с введением SDN Customer Domain становится частью более широкой концепции, связанной со всеми внешними сторонами (Поставщиком, Партнером, Заказчиком), участвующими в структуре.

Изменения предусматривают расширение возможности самообслуживания для клиентов – фактически, архитектура решения должна предусматривать доступ ко всем функциям, ориентированным на клиента. Так же предусмотрена реализация процессов настройки домашней сети и выбора тарифного плана в зависимости от количества и типа устройств в домашней сети.

Домен «Продукт» обогащается функциями управления жизненным циклом для виртуальных компонентов и виртуальных сетевых функций – планирования, разработки, тестирования, запуска, выполнения, обновления, обеспечения и выставления счетов [3].

Анализ требований для реализации OSS для SDN

В рамках управления заказами CRM и остальные задействованные OSS должны будут работать с контроллерами SDN, чтобы управлять согласованными правилами упорядочения заказов в нескольких физических и виртуализированных доменах. Каталоги виртуальных функций необходимо реализовывать на уровне управления заказами.

Инвентаризация услуг должна основываться на правилах пересылки динамических данных. При этом необходимы новые модели ресурсов и их отношения в OSS.

Необходимо расширить автоматизацию (*planing*) планирования до виртуальной инфраструктуры и VNF. Инструменты сетевого планирования с использованием моделирования и аналитики должны иметь возможность использовать VNF и функциональные возможности SDN вместе с физическими сетями [4, 5].

Инвентаризация ресурсов как процесс потребует мгновенной реакции на изменения и синхронизации с системами NRI.

Необходимо реализовать возможность гибкого управления пропускной способностью, включая переподписку на основе шаблонов использования и SLA. При этом потребуется реализовать бесшовное управление конфигурациями VNF с физическими настройками и правилами управления операциями [4, 5].

Неотъемлемой частью новых разработок являются изменения в подходах к безопасности. Однако более подробно эти вопросы будут рассмотрены в других работах.

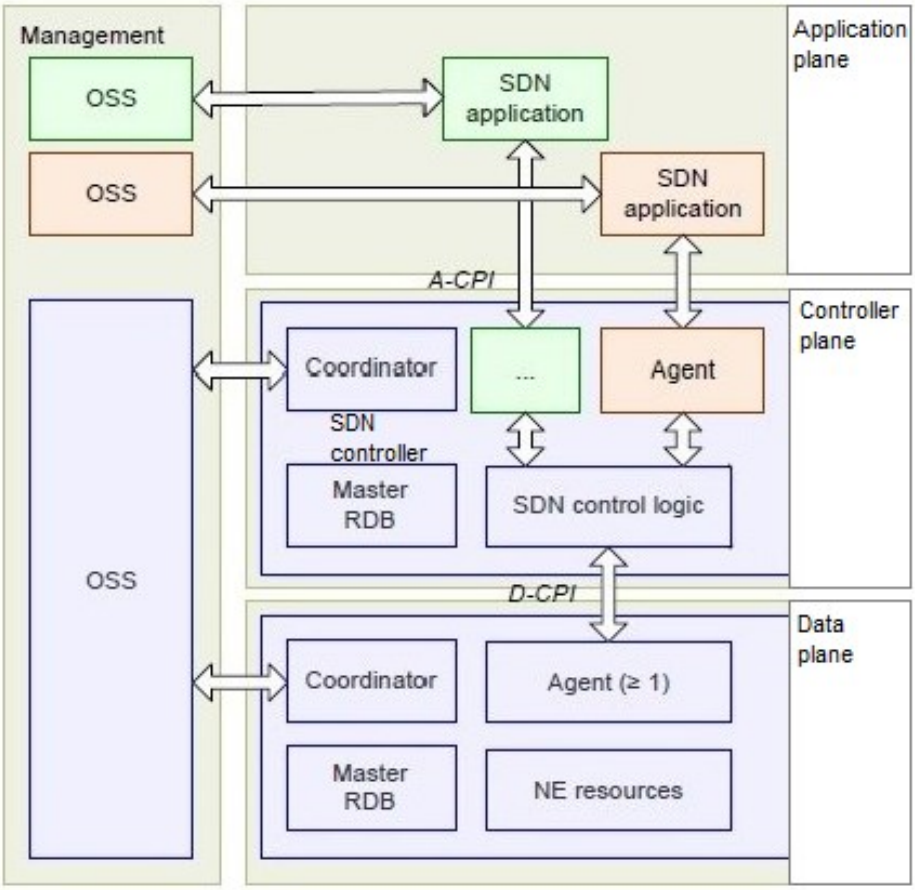


Рисунок. Модель управления сетью SDN

Список используемых источников

1. Impact of SDN and NFV on OSS/BSS // ONF Solution Brief, 2016.

2. Джон Райли, Мартин Кринер NGOSS: построение эффективной системы поддержки и эксплуатации сетей для операторов связи. М. : Альпина Бизнес Букс, 2007. 192 с.

3. SDN-NFV Reference Architecture [Электронный ресурс]. Режим доступа: /http://innovation.verizon.com/content/dam/vic/PDF/Verizon_SDN-NFV_Reference_Architecture.pdf (дата обращения 13.02.2018).

4. Самуйлов К. Е., Серебренникова Н. В., Чукарин А. В., Яркина Н. В. Системы следующего поколения для поддержки операционной деятельности инфокоммуникационной компании: учеб. Пособие. М. : РУДН, 2008. 123 с.

5. Виртуализация функций оператора: NFV & OSS [Электронный ресурс]. Режим доступа: http://www.tssonline.ru/articles2/fix-op/virtualizatsiya-funktsiy-operatora-nfv-oss/ (дата обращения 10.03.2018).

УДК 654.1

ОСОБЕННОСТИ ВНЕДРЕНИЯ И ИСПОЛЬЗОВАНИЯ OSS-СИСТЕМЫ ВЗАИМОДЕЙСТВИЯ ДЛЯ ЗАДАЧ ИССЛЕДОВАНИЯ И ТЕСТИРОВАНИЯ СЕТИ

С. В. Кисляков, Д. И. Рязанов

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

В статье описывается опыт внедрения системы «АРГУС СИРИУС» на сети СПбГУТ для проведения исследования сети и тестирования сетевого оборудования. Система входит в состав установленного OSS-комплекса систем поддержки эксплуатации сетевой инфраструктуры, разработанного НТЦ АРГУС.

OSS/BSS, исследование сети, автоматизация бизнес-процессов.

Введение

Оказание услуг связи неразрывно связано с вопросами комплексного управления сетями связи. Цель управления – обеспечение заданного уровня качества оказания услуг и функционирования сетей связи. Основной задачей управления сетью является реализация целенаправленного воздействия (исследование сети, контроль, администрирование) на оборудование связи с помощью средств автоматизации и информатизации [1].

Большую роль в сети оператора играют OSS/BSS комплексы. Они позволяют автоматизировать бизнес – процессы оператора связи. Большая часть эксплуатационных задач, таких как мониторинг и исследование сети, активация оборудования, требуют наличия систем специального класса, обеспечивающих взаимодействие с оборудованием оператора. Подобные системы сложны как в разработке, так и в первичной настройке и эксплуатации, т. к. каждая сеть имеет свои особенности. Поэтому настройка системы рассматривается как серьёзная самостоятельная задача.

OSS-комплекс лаборатории систем поддержки эксплуатации в СПбГУТ

В Санкт-Петербургском государственном университете телекоммуникаций им. проф. М. А. Бонч-Бруевича (СПбГУТ) создана лаборатория для задач исследования бизнес – процессов оператора связи, которая состоит из нескольких систем, которые мы можем видеть на рис. 1. Система «СИРИУС» – представляет собой программно-аппаратный комплекс, с по-

мощью которого любое другое приложение класса OSS может получить доступ к управлению сетевым оборудованием или отдельным технологическим доменом [2].

Рис. 1. ИТ-ландшафт лаборатории

Место задачи исследования сети (discovering)

Весь комплекс задач оператора стандартизирован организацией TMForum и аккумулирован в карте eTOM (*Enhanced Telecom Operations Map*) – расширенной карте процессов деятельности телекоммуникационной компании (рис. 2.).

Те группировки бизнес-функций, которые автоматизирует обсуждаемая система, отмечены на карте красным цветом.

1. SM&O Support & Readiness (Обеспечение и поддержка готовности процессов уровня услуг);
2. Service Configuration & Activation (Конфигурация и активация услуг);
3. Service Problem Management (Управление решением проблем на уровне услуг);
4. Resource Data Collection & Distribution (Сбор и предоставление информации от ресурсов);
5. Resource Trouble Management (Управление неисправностями на уровне ресурсов);
6. Resource Performance Management (Управление производительностью ресурсов);

7. Resource Mediation & Reporting (Учёт использования ресурсов) – возможности СИРИУС позволяют данной системе вести учет использования ресурсов оператора [3].

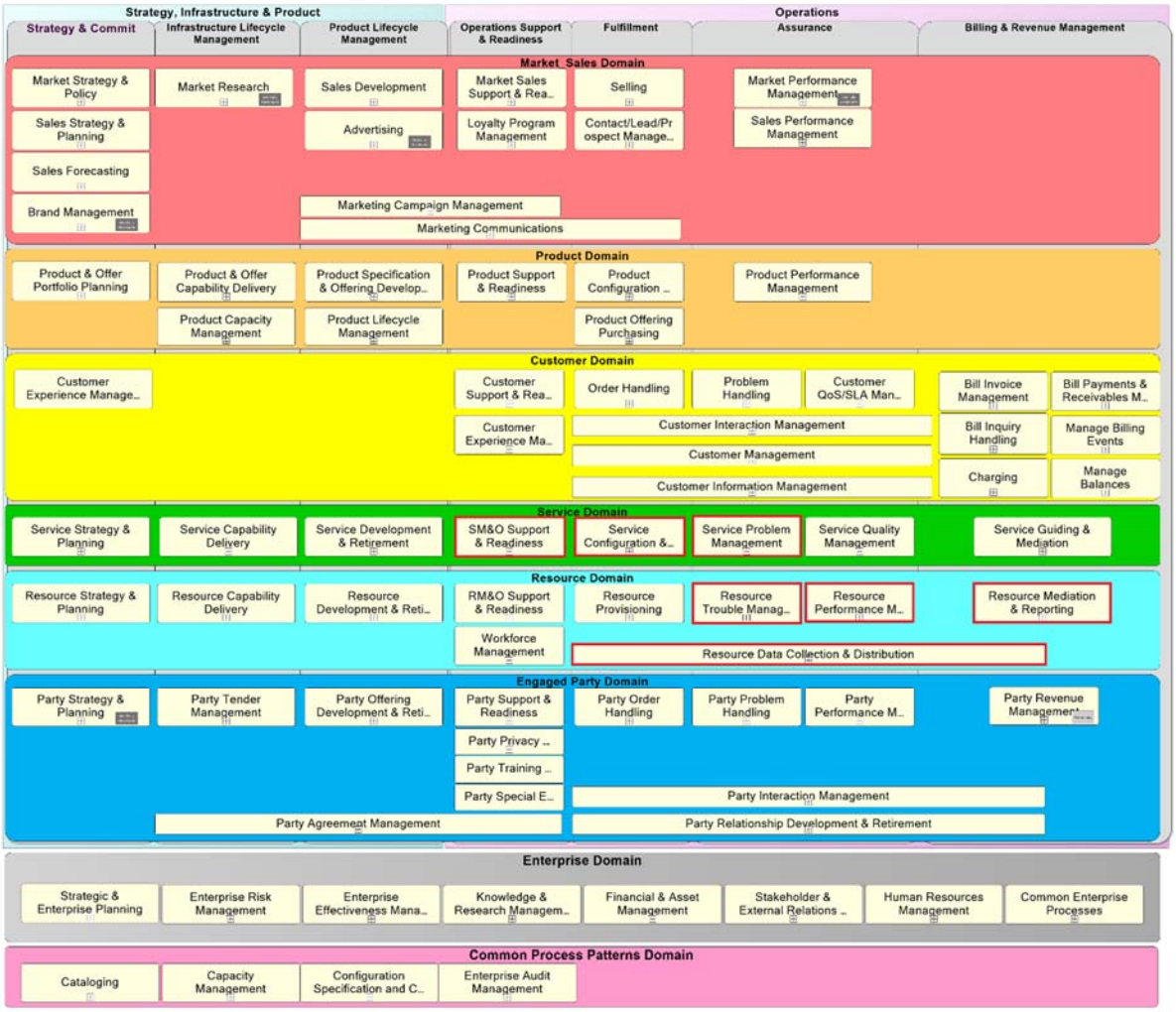


Рис. 2. Карта eTOM (релиз 17.5)

Чтобы вести речь о исследовании сети, нужно понять, как происходит общение на сети в данной ситуации, а общение между серверами СИРИУС и оборудованием на сети оператора связи происходит непосредственно по протоколам SNMP, Telnet и SSH как на рис. 3.

Основной прикладной задачей исследования сети является автоматизация процесса первичного наполнения и дальнейшая актуализация базы данных технического учета информацией об оборудовании на сети оператора. На основании полученной информации, система обеспечивает построение и отображение топологии существующей сети на логическом и физическом уровнях исследуемой сети протокола Интернет.

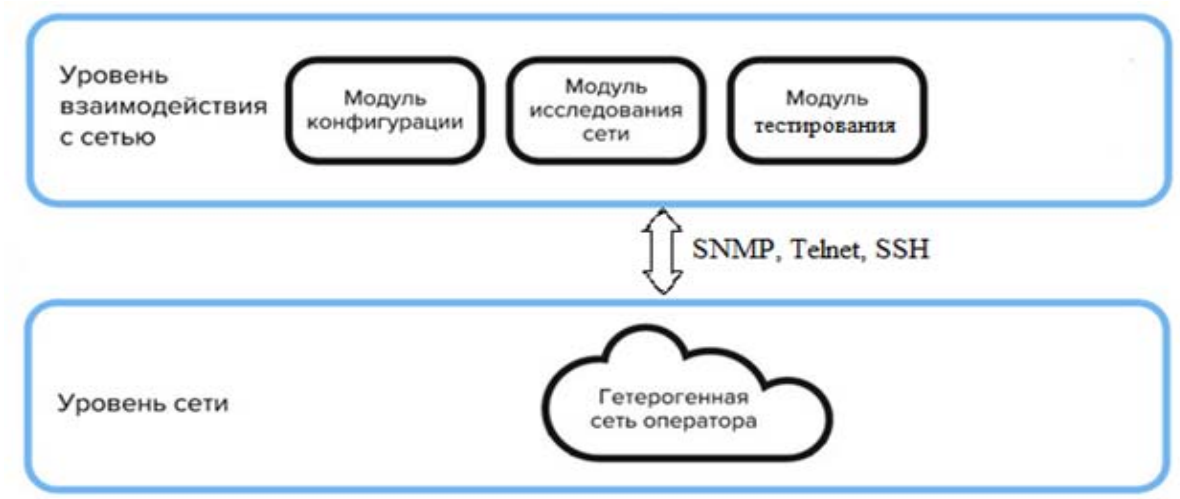


Рис. 3. Взаимодействие системы СИРИУС с оборудованием оператора

Исследование сети

В процессе выполнения исследования IP-подсети, сервер СИРИУС проводит поиск устройств в сети. Следующим этапом производится сравнение информации об устройствах сети, полученной сервером СИРИУС, с информацией об этой сети в системе инвентаризации (ТУ). Если найденное СИРИУСом устройство отсутствует в системе инвентаризации, либо информация об атрибутах устройства не соответствует аналогичным данным в ТУ, в детальной информации о процессе исследования в журнале исследования сети (ЖИС) появляется сообщение типа CONFLICT. Таким образом, для каждого устройства, информации о котором нет в ТУ, либо не актуальной информации, создается CONFLICT.

Исследование сети может проводится как на сетевом, так и на канальном уровнях модели OSI и строить на базе этой информации схемы. Система может обновлять данные в двух режимах: «ручном» и в автоматическом. Таким образом, система намного облегчает работу оператора связи благодаря автоматизации, процесс построения схемы сети делается просто и быстро.

Пример схемы построения сети канального можно увидеть на рис. 4.

Практическая часть

На данный момент реализация разработки полигона для задач исследования и тестирования сети продвигается вперед. На начальном этапе нашей работы при исследовании сети было обнаружено одно устройство ZyXel и построена сеть с одним доступным устройством. Проверена полная работоспособность системы, ведется работа над слиянием оборудования на сети, которое есть в университете, с системой СИРИУС для дальнейшей работы.

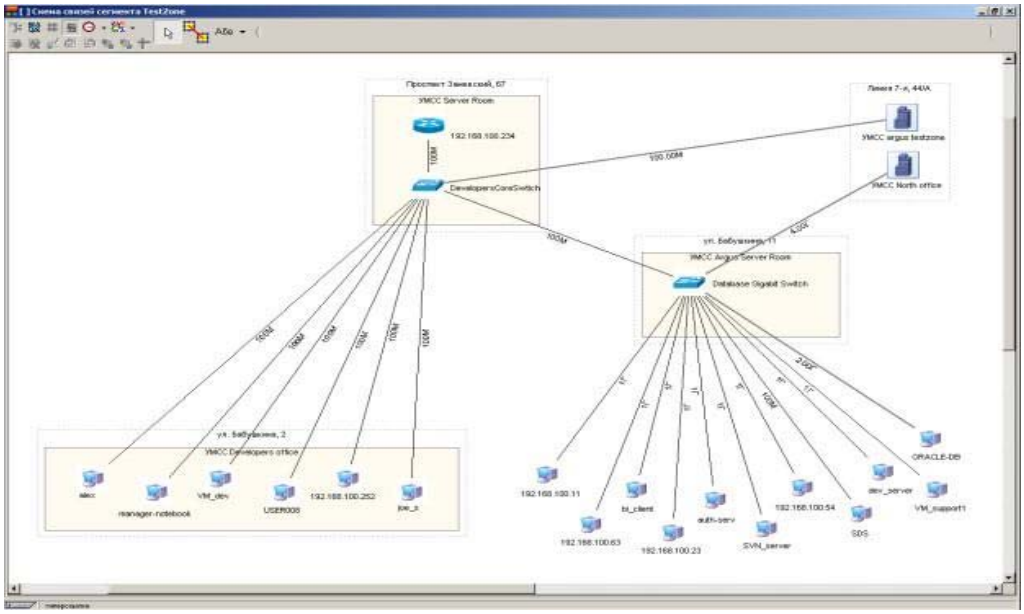


Рис. 4. Пример схемы построения сети второго уровня модели OSI

Список используемых источников

1. Гребешков А. Ю. Управление сетями электросвязи по стандарту TMN: учеб. пособие. М. : Радио и связь, 2004. 155 с.
2. http://argustelecom.ru/produktyi/vzaimodejstvie-s-oborudovaniem.html

УДК 004.056

ИССЛЕДОВАНИЕ МЕХАНИЗМА АВТОРИЗАЦИИ ПОЛЬЗОВАТЕЛЕЙ ДЛЯ ДОСТУПА К IP–ТВ СЕРВИСАМ С ПРИМЕНЕНИЕМ RADIUS–СЕРВЕРА

М. М. Ковцур, А. В. Поляничева

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

В современном мире доступом к сети Internet обладает большинство устройств. Кроме доступа в интернет, сервис провайдеры предлагают пользователям дополнительные возможности, среди которых IP-телевидение. При предоставлении данной услуги операторы используют различные механизмы контроля доступа пользователей к услуге. RADIUS сервера повсеместно используются для реализации AAA сервисов. В рамках данной статьи рассмотрен сценарий применения RADIUS-сервера для решения задачи авторизации пользователей при запросе доступа к сервису IP-телевидения.

авторизация, IPTV, IGMP, multicast.

Безопасность является одним из важнейших аспектов при передаче трафика. Для обеспечения контролируемого доступа к сети часто используют авторизацию и аутентификацию пользователей с помощью AAA сервера. В данном исследовании рассмотрена авторизации клиентов для доступа к услуге IP-TV с использованием RADIUS сервера [1].

IPTV – технология (стандарт) цифрового телевидения в сетях передачи данных по протоколу IP, новое поколение телевидения.

Как правило, при организации IPTV вещания по сетям с коммутацией пакетов используют многоадресную рассылку. Multicast трафик [2] (групповая передача пакетов) используется для передачи потокового видео. Multicast доставляет видео-контент неограниченному числу абонентов, не перегружая сеть. При организации услуги, каждый канал представляется в виде отдельной мультикаст-группы. Для просмотра контента пользователь должен подписаться на группу, а при завершении просмотра – выйти из группы.

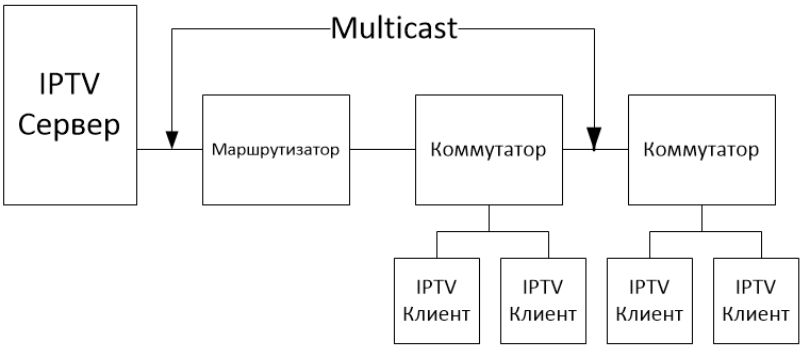


Рис. 1. Модель сети для предоставления услуги IPTV

Для присоединения или выхода из группы используется протокол IGMP (*Internet Group Membership Protocol*). Модель сети представлена на рис. 1.

Основные правила работы протокола IGMP [2] следующие:

– IPTVклиент посылает пакет IGMP типа «report» для запуска процесса подключения к группе рассылки;

– узел посылает пакет Leave при отключении от группы рассылки;

– маршрутизатор или коммутатор с поддержкой multicast посылает в сеть запросы IGMP general query через определенные временные интервалы. Эти запросы позволяют определить текущее состояние групп рассылки;

– IPTV клиент отвечает на IGMP general query с указанием адресов просматриваемых каналов.

Одним из важных аспектов при организации IPTV является авторизация пользователей при запросе канала. Для этой задачи можно использовать списки доступа IGMP, однако такой подход требует обновления списков

на оборудовании при смене тарифного плана клиента. Наиболее популярные подходы – использование шифрования медиаданных и операторских порталов, а также применение RADIUS-авторизации для multicast [3]. При использовании операторских порталов – оператор загружает специализированное программное обеспечение на оборудование клиента, однако такой подход сокращает число поддерживаемого оборудования. В случае RADIUS авторизации – пользователь может использовать практически любое программное обеспечение для просмотра IPTV.

При внедрении RADIUS-сервера возникают дополнительные временные затраты, вызванные необходимостью коммутатора запросить разрешение для подключения в группу каждого отдельного клиента. Эти задержки влияют на время переключения канала. Исследование посвящено оценке влияния параметров канала связи на скорость предоставления доступа к услуге IP-TV (рис. 2.).

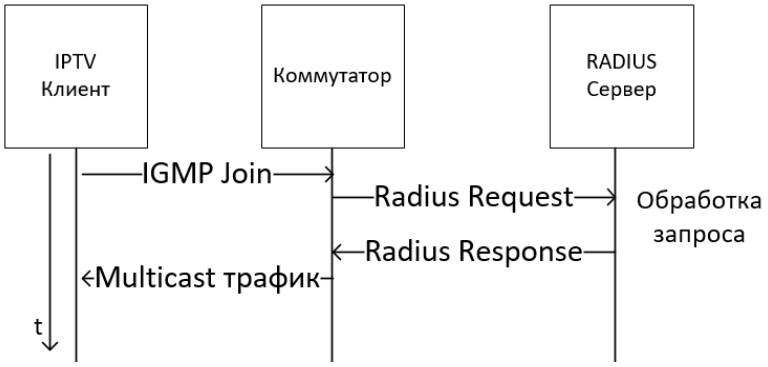


Рис. 2. Модель процесса авторизации клиента при доступе к услуге IPTV

Пусть используется канал связи со следующими параметрами – задержка D_{dist} = 0.001, 0.002 .. 0.4 мс, битовая ошибка P_0 =10^{-7}, 10^{-6} .. 0.1, скорость C_{dist} = 100 Мбит/с.

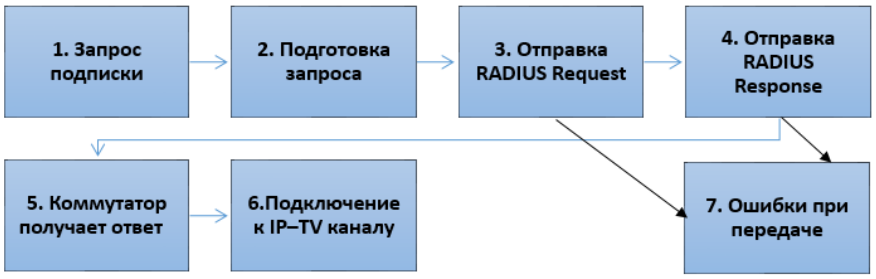


Рис. 3. Модель процесса авторизации клиента

Модель авторизации пользователя представлена на рис. 3 [4]. Для оценки временных характеристик используются следующие параметры модели:

– время передачи от клиента от клиента до порта коммутатора провайдера – T_{12} (мс);

– время обработки, зависит от оборудования – T_{23} – 10 мс;

– задержка в канале связи – *Ddist* (мс);

– время доставки multicast-пакета от порта коммутатора до пользователя– T_{56} (мс);

– время кэширования T_{cash} = 100 мс;

– N_{rqr} – размер пакета *AccessRequest* – 1024 бит;

– N_{rqi} – размер пакета IGMP – 368 бит;

– N_{rs} – размер пакета AccessResponse – 592 бит;

– N_m – размер пакета Multicast – 300 бит;

– C_{dist} – скорость канала – 100 Мбит/с

Составим вероятностный граф, описывающий процесс авторизации пользователей для доступа к услуге IPTV [4]. Граф представлен на рис. 4, где каждая ветвь соответствует переходу из одного состояния в другое согласно модели, рис. 3. Нумерация вершин графа соответствует нумерации узлов рис. 3. Переходы 3–4, 4–6 соответствуют успешному завершению процесса авторизации, когда ветви 3–7 и 4–7 означают возникновение ошибки. Вероятность успешной передачи запроса авторизации коммутатора к RADIUS-серверу [3] будет иметь вид:

$$p_{34} = (1 - P_0)^{N_{rqr}},$$

где N_{rqr} – размер сообщения в битах [5], P_0 – вероятность битовой ошибке в канале связи.

Тогда производящая функция ветви H_{34} имеет вид:

$$H_{34} = p_{34} \times x^{T_{34}}$$

где:

$$T_{34} = D_{dist} + \frac{N_{rqr}}{C_{dist}}.$$

Другие производящие функции определяются по аналогии.

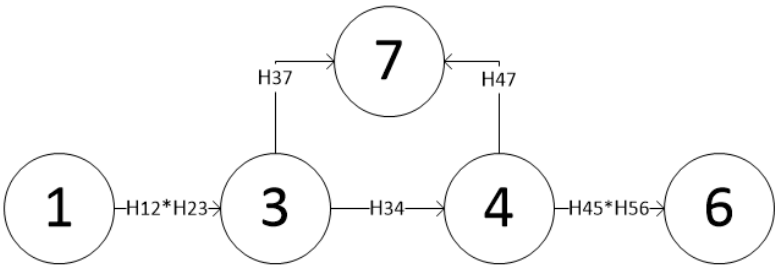


Рис. 4. Граф процесса авторизации

Ветвь неуспешного завершения процесса авторизации будет иметь вид:
$H_A = H_{12} * H_{23} * (H_{37} + H_{34} * H_{47})$.

Ветвь успешного завершения процесса *Tsuccess* авторизации будет иметь вид [5]:

$H_B = H_{12} * H_{23} (H_{34} * H_{46})$.

Вычислим производящую функцию ветви успешного завершения протокола.

Время успешного завершения *Tsuccess* будет иметь вид:

$$Tsuccess = \frac{d}{dx} H_B(x).$$

Вероятность успешной авторизации пользователя для доступа к услуге IPTV будет иметь вид:

$$P_d = H_b\,(x = 1).$$

Итоговые графики представлены на рисунках 5 и 6.

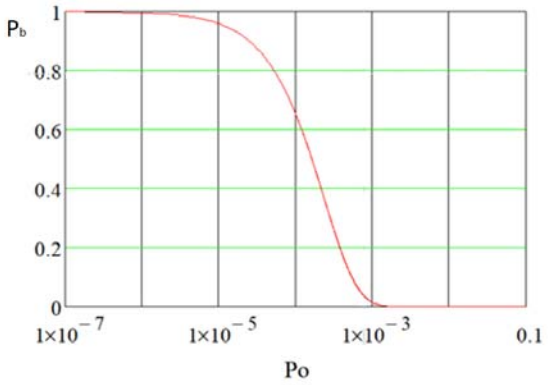


Рис. 5. Зависимость вероятности успешной авторизации пользователя для доступа к услуге от вероятности ошибки в канале связи

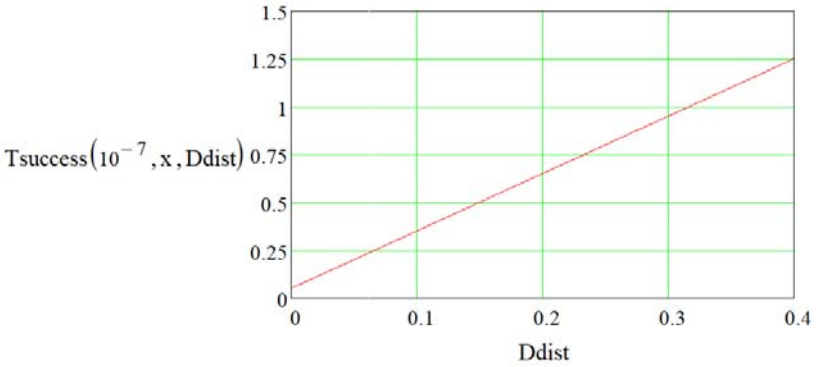


Рис. 6. Оценка времени доступа к услуге IPTV

При битовой ошибке меньшей 10^{-5} вероятность успешного завершения передачи велика.

При использовании RADIUS-авторизации для многоадресной рассылки задержка в канале связи оказывает значительное влияние на время предоставления услуги, как между пользователем и коммутатором оператора, так и между коммутатором и RADIUS сервером. Для минимизации временных затрат на доступ к услуге IPTV целесообразно сокращать эту задержку.

Список используемых источников

1. RFC 2865: Remote Authentication Dial In User Service (RADIUS) [Электронный ресурс]. Режим доступа // http://www.rfc-base.org/rfc-2865.html/ (дата обращений 16.03.2018).

2. RFC 3376: Internet Group Management Protocol, Version 3 [Электронный ресурс]. Режим доступа // https://tools.ietf.org/html/rfc3376/ (дата обращений 16.03.2018).

3. Гольдштейн Б. С., Елагин В. С., Сенченко Ю. Л. Протоколы AAA: RADIUS и DIAMETER. Серия «Телекоммуникационные протоколы». Книга 9. СПб. : БХВ-Петербург, 2014.

4. Никитин В. Н., Юркин Д. В. Улучшение способов аутентификации для каналов связи с ошибками // Информационно-управляющие системы. 2010. № 6. С. 42–46.

5. Ковцур М. М., Никитин В. Н., Юркин Д. В. Оценка вероятностно-временных характеристик защищенной IP-телефонии // Защита информации. Инсайд. 2012. № 4. С. 64.

УДК 510.6

ИДЕНТИФИКАЦИЯ ОБЪЕКТОВ РАДИОМОНИТОРИНГА В МНОГОУРОВНЕВЫХ СТРУКТУРАХ УПРАВЛЕНИЯ ПРИ ПРИМЕНЕНИИ АЛГОРИТМА ОЦЕНКИ КОРРЕЛЯЦИОННЫХ ХАРАКТЕРИСТИК

С. Ю. Козлов, В. В. Кузьмин, Н. П. Удальцов

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

В статье приведен алгоритм, позволяющий определять структурное построение организации в пространстве и принадлежность ее объектов к уровням управления в многоуровневых структурах. При моделировании структуры организации в пространстве использование представленного алгоритма позволяет принимать альтернативное решение при построении структуры организации и определять ее принадлежность к уровню управления.

алгоритм, структура, организация, объект.

Системы связи являются составной частью управления эвентуальной организацией, режимы их работы отражают состояние и деятельность объектов, входящих в ее структуру. Основную часть времени функционирование средств связи подчинено состояниям деятельности многих организаций, их распределение в пространстве отражает плотность построения системы управления организации. На основании вышеизложенного формируется вывод о том, что плотность размещения средств связи в пространстве адекватно отображает структуру построения конкретных организаций в многоуровневых системах. В системном представлении организации важное место занимает их структурное описание. Структурное описание системы включает данные о количестве элементов системы и данные их взаимосвязей [1].

В интересах моделирования деятельности объектов необходимо учитывать факторы, влияющие на их размещение: объект занимает определенный район, обеспечивающий ему выполнение поставленной задачи; объект стремится к сохранению коммуникабельности, т. е. способности управлять подчиненными элементами и быть управляемым, что естественно выражается в сохранении определенных взаимных удалений между объектами [2].

Цель работы – разработать алгоритм оценки корреляционных характеристик для определения структурного построения организации в пространстве, и установления принадлежности включающих в них объектов к уровню управления в многоуровневых системах.

В зависимости от выбранных размеров β_i-й окрестности взаимосвязанность районов размещения i-го и j-го объектов характеризуется следующим образом: размещение i-го объекта в определённом районе предполагает обязательное размещение в пределах β_i-й окрестности j-го объекта $P_{\beta_i}(O_j/O_i) = 1$, $d_{ij} \le R_{\beta_i}$; размещение i-го объекта исключает возможность размещения в пределах β_i-й окрестности *j-го* объекта $P_{\beta_i}(O_j/O_i) = 0$, $d_{ij} > R_{\beta_i}$; в β_i-й окрестности i-го объекта размещение j-го объекта носит вероятностный характер $0 < P_{\beta_i}(O_j/O_i) < 1$.

При моделировании i-го и j-го объектов, их местоположение описывается координатами $X = \{x_i, x_j\}$, $Y = \{y_i, y_j\}$. При следующих допущениях: исходя из множества факторов, влияющих на размещение объектов, в том числе и случайного характера, определяются, что флуктуации величин x_i и x_j, y_i и y_j подчинены нормальному закону распределения с математическими ожиданиями m_{xi}, m_{xj}, m_{yi}, m_{yj} и дисперсиями σ_{xi}^2, σ_{xj}^2, σ_{yi}^2, σ_{yj}^2, соответственно, величины X и Y – независимы.

Тогда плотность вероятности величин разноса объектов по оси абсцисс ΔX и оси ординат ΔY будет определяться, как композиция нормальных законов (1.1–1.2) соответствующих случайных величин [3, 4].

$$f(\Delta X) = \frac{exp\left(-\frac{(\Delta X - m_{\Delta x})^2}{2\ \sigma_{\Delta x}^{\ 2}}\right)}{\sqrt{2\pi}\ \sigma_{\Delta x}}, \quad (1.1)$$

$$f(\Delta Y) = \frac{exp\left(-\frac{(\Delta Y - m_{\Delta y})^2}{2\ \sigma_{\Delta y}^{\ 2}}\right)}{\sqrt{2\pi}\ \sigma_{\Delta y}}. \quad (1.2)$$

С практической точки зрения разнос объектов оценивается путём непосредственного определения возможных расстояний между ними – R_{ij}. Значение величины R_{ij} определяется многими факторами, в том числе и случайного характера, и поэтому описывается [5] нормальным усечённым законом распределения (2):

$$f(R) = \frac{A \cdot exp\left(-\frac{(R - m_R)^2}{2\ \sigma_{\Delta R}^{\ 2}}\right)}{\sqrt{2\pi}\ \sigma_R}, \quad A = \frac{1}{F\left(\frac{R_{max} - m_R}{\sigma_R}\right) - F\left(\frac{R_{min} - m_R}{\sigma_R}\right)} \quad (2)$$

где $F(\cdot)$ – функция Лапласа, R_{min}, R_{max} – максимальное и минимальное удаление объектов друг от друга.

Кроме расстояния между объектами информативными признаками выступает взаимная ориентация их относительно друг друга. Характеристики ориентации размещения объектов указывают возможное направление размещения j-го объекта относительно i-го объекта и наоборот. Размещение объектов друг относительно друга представляются значениями азимутов с i-го объекта на j-й объект. В этом случае ориентация размещения объектов описывается равномерным или нормальным законами распределения (3, 4), где Θ_{ij} – значения азимутов:

$$f_{равнм.з}(\Theta) = \frac{1}{\Theta_{max} - \Theta_{min}}, \quad (3)$$

$$f_{норм.з}(\Theta) = \frac{exp\left(-\frac{(\Theta - m_\Theta)^2}{2\ \sigma_{\Delta\Theta}^{\ 2}}\right)}{\sqrt{2\pi}\ \sigma_\Theta}. \quad (4)$$

В целом, взаимосвязанность размещения объектов определяется двумерной функцией плотности вероятности, отражающей зависимость размещения, исходя из их удалённости друг от друга и взаимной ориентации. Потому как случайные величины R и Θ независимы, то их совместная плотность распределения определяется как произведение соответствующих функций распределения (5):

$$f(R,\Theta)=\frac{A\cdot exp\left(-\frac{(R-m_R)^2}{2\ \sigma_{\Delta R}^{\ 2}}\right)}{\sqrt{2\pi}\ \sigma_R(\Theta_{max}-\Theta_{min})}. \qquad (5)$$

Графическая интерпретация характеристик взаимосвязанности размещения объектов представлена на рис. 1.

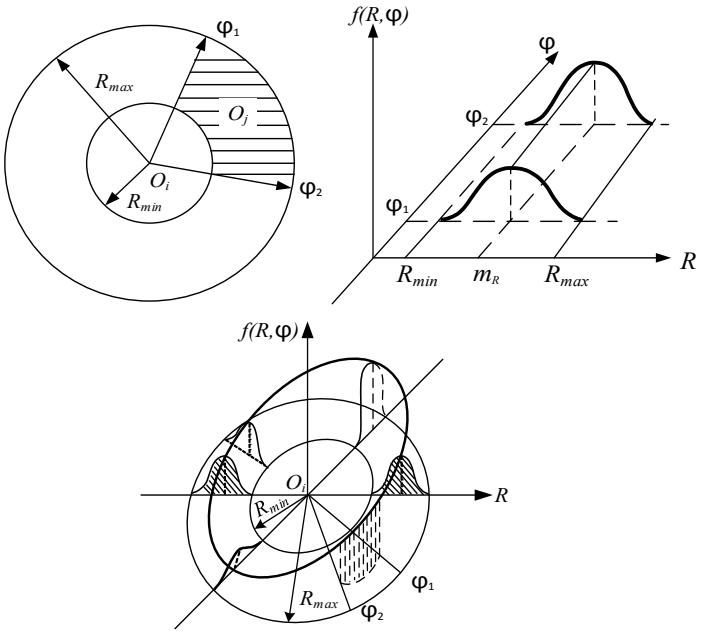


Рис. 1. Графическое отображение взаимосвязанности размещения объектов

Исследования показывают, что при существующих погрешностях измерения пространственных характеристик размещения объектов средствами наблюдения (10...15 % от дальности) и ограниченных объёмах статистических данных с достаточной для практических расчётов точностью функции распределения значений расстояний между объектами и направлений их размещения аппроксимируются равномерными законами распределения, что значительно упрощает расчёты.

Входным элементом представленного алгоритма является результирующая таблица минимальных и максимальных расстояний и азимутов, кото-

рая находит свое применение при составлении алгоритма оценки корреляционных характеристик объектов и установление их принадлежности к уровню управления в иерархических системах (рис. 2).

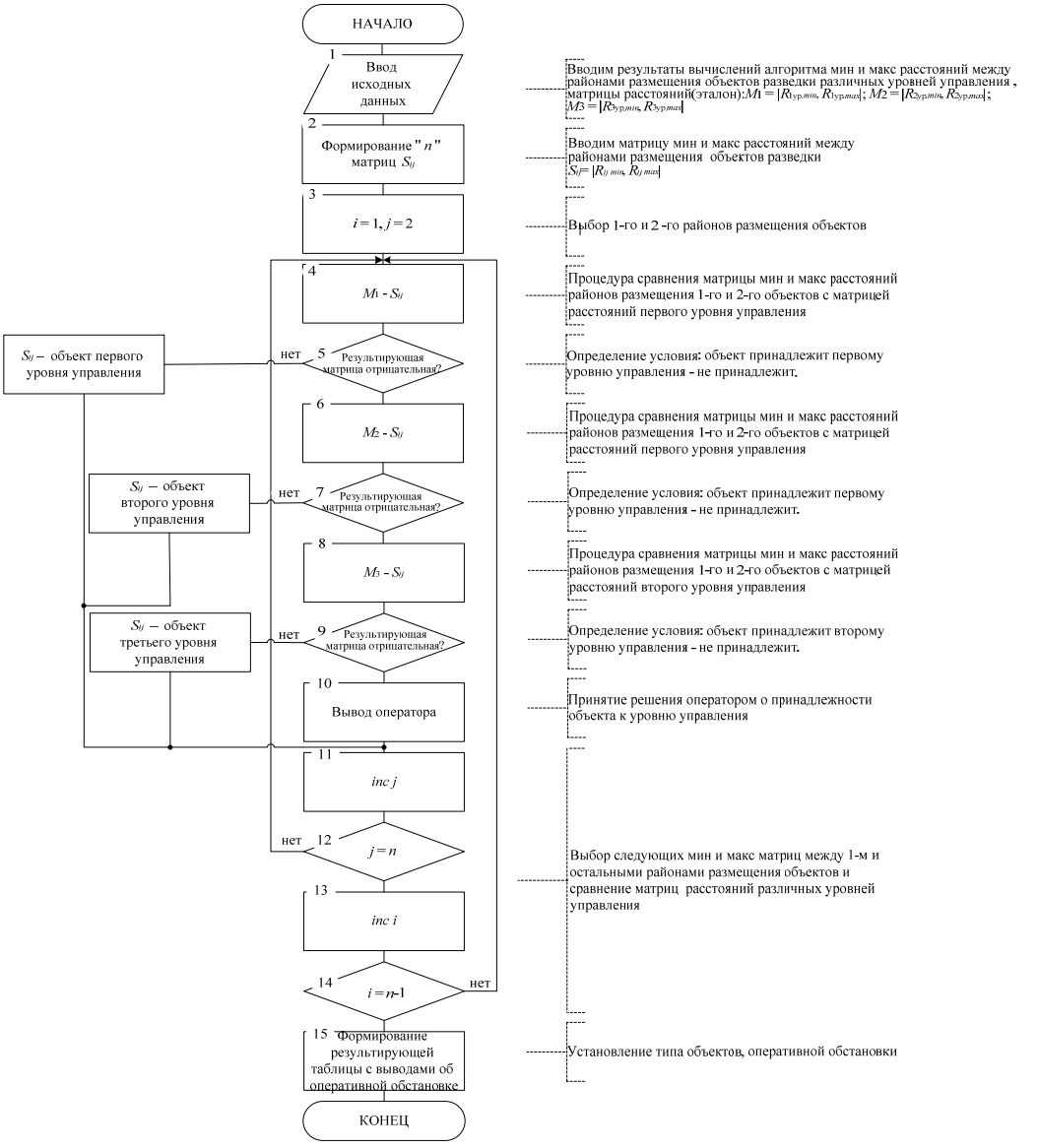


Рис. 2. Алгоритм оценки корреляционных характеристик объектов и установление их принадлежности к уровню управления в многоуровневых системах

Заключение

Вышеуказанные корреляционные характеристики получаются при условии, что динамика прогнозирования поведения действий объектов позволяет им находиться в пределах некоторых районов, размеры и взаимное расположение которых учитывается при расчётах. Однако в настоящее время, учитывается динамичность развития современных действий, следует

отметить, что такая ситуация возможна только в течение некоторого интервала времени. Чем выше динамичность действий, тем короче временной интервал.

Таким образом, знание корреляционных характеристик размещения позволит получать специальную информацию об одних объектах на основе данных от других, что особенно важно в условиях ограниченных возможностей по установлению непосредственного контакта с объектами.

Список используемых источников

1. Денисов А. А., Колесников Д. Н. Теория больших систем управления. Л. : Энергоиздат. 1982. 216 с.
2. Акимова Т. А. Теория организации: учебное пособие для вузов. М., 2003. 367 с.
3. Вентцель Е. С. Теория вероятностей. М. : Издательский центр «Академия». 2005. 576 с.
4. Гнеденко Б. В., Хинчин А. Я. Элементарное введение в теорию вероятностей. М. : Наука. 1982. 160 с.
5. Вадзинский Р. Н. Справочник по вероятностным распределениям. СПб. : Наука, 2001. 287 с.

УДК 654.025.8

СРАВНЕНИЕ АКТИВНОГО ОБОРУДОВАНИЯ GPON КЛАССОВ B+ и C+

А. А. Козырев, Г. А. Широков, П. П. Шумаков

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

В статье проводится сравнительный анализ характеристик широко применяемого на сегодняшний день активного оборудования класса B+ для развертывания пассивных оптических сетей доступа GPON и недавно появившегося на рынке аналогичного оборудования класса C+. Приводятся расчеты, наглядно демонстрирующие преимущества использования оборудования класса C+ вместо оборудования класса B+. Также в докладе отражены пути решения проблемы наращивания потенциала уже имеющейся пассивной оптической сети, а также возможности совместного использования оборудования класса B+ и C+ в различных вариациях.

сети доступа, последняя миля, GPON, оптический бюджет.

Наиболее важными элементами пассивной волоконно-оптической сети доступа являются два активных ее элемента: OLT – оптический линейный терминал, устанавливаемый в помещении оператора связи (провайдера)

на узле агрегации траффика и ONT – оптический сетевой терминал, устанавливаемый в помещении пользователя [1].

По своей сути, что OLT, что ONT являются оптическими приемопередатчиками, наиболее важными параметрами которых являются средняя выходная мощность передатчика и чувствительность приемника. От этих параметров напрямую зависит оптический бюджет проектируемой волоконно-оптической сети доступа, речь о котором пойдет дальше в данной статье. От оптического бюджета зависят два самых важных конфигурационных параметра сети доступа: расстояние от абонента до узла агрегации (расстояние OLT-ONT) и коэффициент ветвления дерева PON. Эти конфигурационные параметры не важны пользователю, однако они сильно важны оператору связи, предоставляющему услуги пользователям, ведь от этих параметров напрямую зависят затраты оператора и его выручка.

Средняя выходная мощность передатчика и чувствительность приемника являются величинами, нормируемыми в соответствии с классом оборудования технологии GPON и определены МСЭ. До недавнего времени при проектировании волоконно-оптической сети доступа на базе технологии GPON повсеместно применялось оборудование OLT и ONT класса B+, но буквально недавно на рынке появилось оборудование класса C+, что по своей сути стало новым витком в развитии сетей GPON, важность которого трудно переоценить. В таблице, представленной ниже, приведена сравнительная характеристика оборудования GPON классов B+ и C+.

ТАБЛИЦА. Сравнительная характеристика оборудования GPON классов B+ и C+

	Оборудование класса B+	Оборудование класса C+
Рабочая длина волны передатчика, нм	1490 / 1310	1490 / 1310
Рабочая длина волны приемника, нм	1490 / 1310	1490 / 1310
Тип инкапсулятора волокна	SFP модуль	SFP модуль
Скорость передачи, Мбит/с	2488	2488
Тип оптоволокна	Одномодовое	Одномодовое
Тип разъема	SC/APC	SC/APC
Средняя выходная мощность передатчика, дБм	+5	+10
Чувствительность приемника, дБм	–28	–32

Как видно из таблицы, большинство показателей в оборудовании класса C+ остались неизменны, но два наиболее важных при проектирова-

нии волоконно-оптической сети доступа показателя существенно изменились: возросла средняя выходная мощность передатчика, а приемник стал более чувствительным. Далее посмотрим какие конструктивные преимущества появились после изменения этих показателей.

Для начала, необходимо рассчитать бюджет оптической мощности при использовании оборудования классов B+ и C+. Оптический бюджет определяется как разность мощности передатчика и чувствительности приемника [2]. После произведения линейных расчетов видно, что оптический бюджет ВОСС, построенной на оборудовании класса B+ составляет 33 дБ, в то время как оптический бюджет ВОСС, построенной на оборудовании класса C+ составляет 42 дБ. Очевидно, что оптический бюджет при использовании оборудования класса C+ заметно больше, чем при использовании аналогичного оборудования класса B+.

Бюджет оптической мощности показывает, какое затухание может претерпеть оптический сигнал при передаче по оптоволокну от коммутатора, расположенного на узле агрегации, до входа абонентского оптического терминала, чтобы быть распознанным фотоприемным устройством. Сигнал претерпевает затухание вследствие распространения по самому оптоволокну, вследствие прохождения множества разъемных и неразъемных соединений (сварок оптоволокна), а также вследствие прохождения через сплиттер. Затухание на каждом пассивном элементе сети GPON также нормируется, и при монтажных работах четко контролируется проверяющими организациями [3]. Потеря бюджета оптической мощности без учета магистрального участка сети доступа при коэффициенте ветвления дерева PON 1:64 является известной величиной, и составляет (28+/–0,5) дБ [4].

С оптическим бюджетом оборудования класса B+ на магистральный участок остается всего лишь 5 дБ, в то время как оптический бюджет магистрального участка при использовании оборудования класса C+ составит 14 дБ.

После произведения расчетов начинают быть видны конструктивные преимущества оборудования класса C+: с 5 дБ максимальная протяженность магистрального участка составит 11 км (с учетом строительной длины волоконного кабеля в 2 км, используемой при методе пневмозадувки, 5 сварных соединений). С 14 дБ максимальная протяженность магистрального участка составит уже 30 км (с учетом строительной длины волоконного кабеля в 2 км, используемой при методе пневмозадувки, 13 сварных соединений). Так как располагать узлы агрегации целесообразно рядом с уже имеющимися объектами связи, такими как здания автоматических телефонных станций и т. д., данное расстояние играет огромную роль при прокладке сети доступа в микрорайоны новой застройки без развитой инфраструктуры или при прокладке сети доступа в загородные поселки частной застройки, что сейчас становится очень популярным.

Также с таким запасом по децибелам можно ввести третий уровень ветвления сигнала, тем самым увеличив коэффициент ветвления одного оптоволокна с 1:64 до 1:128, сократив количество оптических волокон в магистральном кабеле, а, следовательно, снизив его цену, или, не сокращая количество волокон в кабеле, увеличить коэффициент резервирования системы.

В случае, если не требуется прокладывать магистральный участок сети доступа на большие расстояния и не требуется введение третьего уровня ветвления, есть возможность совместного использования оборудования классов B+ и C+, например, при использовании станционного оборудования класса C+ и абонентского оборудования класса B+ оптический бюджет удается увеличить с 33 дБ до 37 дБ, тем самым увеличив длину магистрального участка сети доступа до 20 км.

Список используемых источников

1. Гольдштейн Б. С., Соколов Н. А., Яновский Г. Г. Сети связи: учебник для вузов. СПб. : БХВ-Санкт-Петербург, 2010. 400 с.

2. Сычев К. И. Математические модели процессов функционирования узлов коммутации мультисервисных сетей связи // Электросвязь. 2008. № 2. С. 24-29.

3. Былина М. С., Глаголев С. Ф., Иванов В. С., Смирнов Г. М. Современные технологии проектирования, строительства и эксплуатации направляющих систем электросвязи: методические указания к курсовому проектированию (спец. 210404) / ГОУВПО СПбГУТ. – СПб., 2007.

4. Иванов А. Б. Волоконная оптика: компоненты, системы передачи, измерения. М.: Компания Сайрус Системс, 1999. 663 с.

УДК 004.056.53

МЕТОДЫ ЧЕЛОВЕКО-МАШИННОГО ВЗАИМОДЕЙСТВИЯ ДЛЯ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ ПРИНЯТИЯ РЕШЕНИЙ В ПРОЦЕССАХ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

М. В. Коломеец[1,2], А. А. Чечулин[1,2], И. В. Котенко[1,2]

[1]Санкт-Петербургский институт информатики и автоматизации Российской академии наук
[2]Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

В виду постоянного роста количества и сложности данных информационной безопасности, необходимо развивать технологии управления информацией и, в частности,

разрабатывать новые методы человеко-машинного взаимодействия. Большой потенциал имеют решения, основанные на использовании нестандартных способов представления и ввода информации: голосовые ассистенты, сенсорные мультитач-экраны, технологии виртуальной и дополненной реальности и системы компьютерного зрения. Но, несмотря на доступность устройств, системы на основе данных технологий не находят широкого применения. Это связано с неразвитостью принципов взаимодействия пользователя и данных для указанных типов технологий. В работе рассматриваются основные принципы построения систем человеко-машинного взаимодействия, а также потенциал их использования в системах информационной безопасности.

человеко-машинное взаимодействие, информационная безопасность, принятие решений.

Проблема эффективного управления системами информационной безопасности на основе данных является актуальной задачей в виду увеличения объема видов и количества информации [1].

Данная проблема особенно актуальна для систем, в которых отдельные процессы управления невозможно или сложно автоматизировать. К таким случаям можно отнести принятие решений в ситуационных центрах безопасности, принятие решений с высокой степенью влияния контекста информации и случаи, когда решение должно принципиально приниматься человеком, который будет нести за него ответственность.

Наиболее эффективным инструментом для оперативного анализа данных является визуализация [2], но для управления визуальным отображением и манипуляцией информацией, специалистам необходимы эффективные инструменты взаимодействия с данными. Можно выделить три основные причины, которые обуславливают необходимость в развитии технологий управления данными.

Во-первых, рост данных порождает неуправляемость. Сегодняшний мир движется к четвертой промышленной революции [3], темпы роста IoT рынка составляют 42 % в год [4], а компании и страны стремятся к тотальной информатизации всех процессов. Из-за роста количества источников данных, объема данных и их гетерогенности, анализ данных сильно усложняется, а людям необходимы инструменты для эффективного извлечения знаний.

Во-вторых, новые данные, которые становятся доступны, дают новые возможности управления. Новые возможности систем позволяют принимать более качественные решения, но скорость принятия решений уменьшается, а сложность увеличивается. При этом когнитивные способности человека остаются прежними.

В-третьих, в современных системах человек становиться «бутылочным горлышком», являясь самым медленным элементом системы и тормозящим остальные процессы.

Для решения данных проблем необходимо развивать технологии управления информацией и, в частности, разрабатывать новые методы человеко-машинного взаимодействия.

Большой потенциал имеют решения, основанные на использовании нестандартных способов представления и ввода информации: голосовые ассистенты, сенсорные мультитач-экраны, технологии виртуальной и дополненной реальности и системы компьютерного зрения.

Но, несмотря на доступность устройств, системы на основе данных технологий не находят широкого применения. С одной стороны, это связано с неразвитостью принципов взаимодействия пользователя и данных для указанных типов технологий, а с другой – с неготовностью аппаратной части.

Например, массовое использование виртуальной реальности в обучении пока не предоставляется возможным вследствие большой стоимости устройств. На 2018-й год самым бюджетным вариантом является использование мобильных телефонов вместе с cardboard [5], но стоимость телефонов с поддержкой виртуальной реальности остается высокой, в то время как само устройство устаревает за два–три года.

Также необходимо отметить, что на маломощных устройствах задержки в рендеринге изображения влияют на состояние здоровья (могут вызывать головную боль и чувство тошноты).

Использование дополненной реальности в визуальной аналитике на сегодняшний день также маловероятно. Одним из самых успешных устройств дополненной реальности с точки зрения эргономики являются очки Microsoft HoloLens [6], но даже в них оператору сложно проводить много времени.

Несмотря на очевидное несовершенство аппаратной части в практическом применении, существующие устройства позволяют определить принципы взаимодействия человека и данных, которые можно будет применить в будущих поколениях устройств.

Создание систем человеко-машинного взаимодействия должно происходить на четырех уровнях.

1) Исследования человека и его возможностей [7]. Так как новые технологии ввода и вывода информации значительно отличаются от возможностей мыши и монитора, необходимо определить сильные и слабые стороны используемого устройств в контексте возможностей человека. Например, при разработке сложных систем управления на основе сенсорных экранов необходимо изучить какие жесты удобны для человека и какие комбинации жестов интуитивно понятны. При разработке решений на основе дополненной реальности необходимо определить, какие физические параметры объектов могут быть точнее интерпретированы пользователем (такие как цвет, объем объекта, движение в пространстве и т. д.).

2) Исследования аппаратной части. Необходимо определить, какие ограничения несут определенные физические параметры используемых устройств. Например, в виртуальной реальности крайне важной является эргономика, так как человеку может быть необходимо находится в очках виртуальной реальности достаточно длительное время.

3) Исследования программной части. Аппаратные решения позволяют лишь считывать физические действия пользователей, но не интерпретировать их. Важной частью исследований является построение программных алгоритмов и методов интерпретации действий пользователя. Например, в системах на основе сенсорных экранов необходимо разрабатывать точные алгоритмы определения жестов, включая их отдельные параметры, такие как скорость движения, направление и т. п.

4) Исследование визуальной части. Для новых способов взаимодействия необходимы способы визуализации, которые будут их поддерживать. Например, при использовании дополненной реальности не имеет смысла отрисовывать двумерные диаграммы, которые можно более эффективно воспринимать на экране.

Развитие технологий человеко-машинного взаимодействия позволит усовершенствовать многие области информационной безопасности. Так технологии виртуальной реальности очевидно окажут влияние на процессы обучения. Например, виртуальную реальность можно использовать при изучении методов обеспечения физической безопасности.

Сенсорные экраны можно использовать для анализа данных, представленных большими и многоуровневыми графами, таких как компьютерные сети, социальные сети, онтологические базы и т. д. Технологии дополненной реальности имеют потенциал при анализе киберфизической безопасности. Например, системы на основе дополненной реальности можно использовать для визуализации состояния отдельных элементов предприятия, когда информация об объекте может отображаться поверх самого объекта.

Таким образом, можно заключить, что в целом текущее состояние технологий позволяет производить исследования возможностей применения новых способов человека машинного взаимодействия в информационной безопасности.

Работа выполнена при поддержке РФФИ (16-29-09482, 18-07-01488) и при частичной поддержке бюджетной темы № АААА-А16-116033110102-5.

Список используемых источников

1. Коломеец М. В., Котенко И. В., Чечулин А. А. Использование виртуальной и дополненной реальности для визуализации данных кибербезопасности // Защита информации. Инсайд. 2017. №. 5. С. 58–63.

2. Novikova E., Kotenko I. Analytical Visualization Techniques for Security Information and Event Management // Proceedings of the 2013 21st Euromicro International Conference on Parallel, Distributed, and Network-Based Processing, PDP 2013. IEEE, 2013. P. 519–525.

3. Кобяков А. Вызовы XXI века: как меняет мир четвертая промышленная революция // РБК. Опубл. 2016. Т. 12.

4. Technavio Inc., Global Telecom IoT Market 2016-2020 // Technavio report, 2016.

5. Powell W. et al. Getting around in google cardboard–exploring navigation preferences with low-cost mobile VR // Everyday Virtual Reality (WEVR), 2016 IEEE 2nd Workshop on. IEEE, 2016. P. 5–8.

6. Garon M. et al. Real-time high resolution 3D data on the HoloLens // Mixed and Augmented Reality, 2016 IEEE International Symposium on. IEEE, 2016. P. 189–191.

7. Коломеец М. В. Использование когнитивных особенностей человека для визуализации данных безопасности // Информационные технологии в управлении. 2016. С. 723–728.

УДК 004.056.5

ПРОБЛЕМЫ ОБНАРУЖЕНИЯ ЦЕЛЕНАПРАВЛЕННЫХ АТАК (APT) НА КРИТИЧЕСКИ ВАЖНЫЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ

Н. А. Комашинский, И. В. Котенко

Санкт-Петербургский институт информатики и автоматизации Российской академии наук

В работе приведены трудности при обнаружении целевых компьютерных атак на критически важные объекты, рассмотрены инструменты для обнаружения и реагирования для данного типа атак, выработаны рекомендации и методика для предотвращения таких атак. Знание основных принципов организации и проведения целевых атак, а также использование результатов данного анализа позволит выявлять сложные компьютерные атаки на начальном этапе, предотвращая глобальные последствия заражений вредоносным программным обеспечением и попыток несанкционированного доступа к ресурсам критически важных инфраструктур.

целенаправленная атака, критически важная информационная система, компьютерная разведка, вредоносное программное обеспечение, киберпреступность.

В наше время компьютерная безопасность критически важных информационных систем – это забота каждого сотрудника, начиная от обычных пользователей и администраторов, до руководителей. В любой IT-сфере приоритетной задачей является повышение информационной безопасности организации и центров обработки данных. На протяжении многих лет киберпреступники получали более продвинутые и эффективные средства

для достижения своих целей. Они организовывали целые команды высококвалифицированных хакеров и превратили эту деятельность в крупный бизнес.

Важно соблюдать меры безопасности, чтобы защитить информацию, исключить утечку ценных данных и предотвратить целевые атаки. Для этого необходимо понимать, что из себя представляют компьютерные атаки и изучать способы их предотвращения [1].

Следует отметить, какие информационные системы относятся к критическим.

Признаки критически важных информационных систем:

(1) управление потенциально опасными производствами или технологическими процессами;

(2) обеспечение функционирования опасных объектов, осуществляющих управление (или информационное обеспечение управления) чувствительными (важными) для государства процессами.

Целевые атаки на критические информационные системы обычно тщательно спланированы и разбиты на четыре обязательные фазы:

(1) вторжение,

(2) разведка (скрытый аудит),

(3) захват,

(4) добыча информации.

В каждой фазе могут использоваться различные методы для достижения необходимых целей [2].

Вторжение. В целенаправленных атаках хакеры обычно получают доступ в сеть организации, используя социальную инженерию, уязвимости нулевого дня, SQL-инъекции, целевое вредоносное программное обеспечение и другие творческие методы. Основное отличие целенаправленных атак заключается в том, что, в то время как обычные атаки нацелены на краткосрочные одноразовые результаты «найти уязвимость и тут же ее использовать», целевые атаки предназначены для создания скрытого канала управления, чтобы запускать конкретные команды в течение длительного периода и добывать ценную информацию.

Разведка (скрытый аудит). На следующем этапе, после внедрения в информационную систему, злоумышленник строит карту сети с помощью специальных инструментов, сканирует конфиденциальные ресурсы. На этом этапе нужно обнаружить незащищенные данные и сети, уязвимости программного и аппаратного обеспечения, открытые учетные данные и пути к дополнительным ресурсам или точкам доступа. При этом строго соблюдаются методичность и определенная длительность, чтобы избежать обнаружения. В некоторых случаях намеренно используются признаки для обнаружения псевдо-атаки для отвлечения внимания от настоящей цепочки событий целенаправленной атаки.

Захват. В фазе захвата устанавливается доступ к открытым данным, хранящимся в незащищенных системах. Кроме того, руткиты могут быть тайно установлены в целевых системах и точках доступа к сети для сбора данных и инструкций по мере их прохождения через сеть организации.

Добыча информации. Как только злоумышленники захватят контроль над целевыми системами, они могут продолжить кражу интеллектуальной собственности или других конфиденциальных данных. После получения обратных сигналов управления, собранные данные могут быть отправлены на базовую станцию атакующего, например, через почту, либо с помощью зашифрованных пакетов или сжатых файлов с парольной защитой. В то время как происходит утечка ценной информации зачастую эти данные подвергаются ручному анализу специалистами, для извлечения коммерческой тайны, прогнозирования конкурентных действий и планирования маневров.

Для локализации воздействия целевых атак и снижения подверженности критически важных систем различным уязвимостям предлагаются следующие рекомендации [3]:

пограничные брандмауэры и интернет-шлюзы – устанавливают защиту периметра сети, в частности веб-прокси, веб-фильтрацию, проверку содержимого и политики брандмауэра, чтобы обнаруживать и блокировать загружаемые файлы, блокировать доступ к известным вредоносным доменам и не разрешать компьютерам пользователей напрямую общаться с Интернетом;

защита от вредоносных программ – создание и поддержка защиты от вредоносных программ для обнаружения и реагирования на известные сигнатуры атаки;

своевременно обновление программного обеспечения – исправление известных уязвимостей с последней версией программного обеспечения для предотвращения атак, которые используют ошибки программного обеспечения;

управление белым списком и контроль исполнения файлов – предотвращение возможности запуска или установки неизвестного программного обеспечения, включая AutoRun на USB и CD-приводах;

безопасная конфигурация – ограничить функциональность каждого устройства, операционной системы и приложения до минимума, необходимого для функционирования информационной системы;

парольная политика – соблюдение соответствующих требований к сложности и частоте смены паролей;

контроль доступа пользователей – включает ограничение прав доступа обычных пользователей и соблюдение принципа наименьших привилегий.

Опираясь на рассмотренные модели организации целевых компьютерных атак, помимо выполнения рекомендаций, предлагается использовать

методику распределенного анализа событий для выявления целевых компьютерных атак. В связи с большим количеством обрабатываемых событий в современных системах обнаружения атак, главной целью методики является интеграция технологий Snort и Hadoop.

Для анализа пакетов используется Hadoop. В схеме (рис.) входящие пакеты собираются с помощью Snort в режиме регистрации пакетов. Каждый пакет содержит определенные признаки, такие как временная метка, протокол, IP-адрес источника, IP-адрес узла назначения, номера портов, тип пакета и другие поля, характеризующие входящий пакет. Когда на локальном диске будет записано большое количество пакетов, файлы будут либо в формате tcpdump, либо в двоичном формате. Поэтому необходимо выполнить некоторую предварительную обработку, чтобы превратить их в читаемый формат. Это делается с помощью подходящих команд Snort. Для анализа в Hadoop эти файлы должны быть загружены в файловую систему HDFS. Здесь работает MapReduce, преобразовывая пакеты и извлекая из них такую важную информацию, как IP-адрес источника, IP-адрес узла назначения, номера портов, тип пакета и др. Также он определяет количество пакетов от определенного источника до адресата определенного типа.

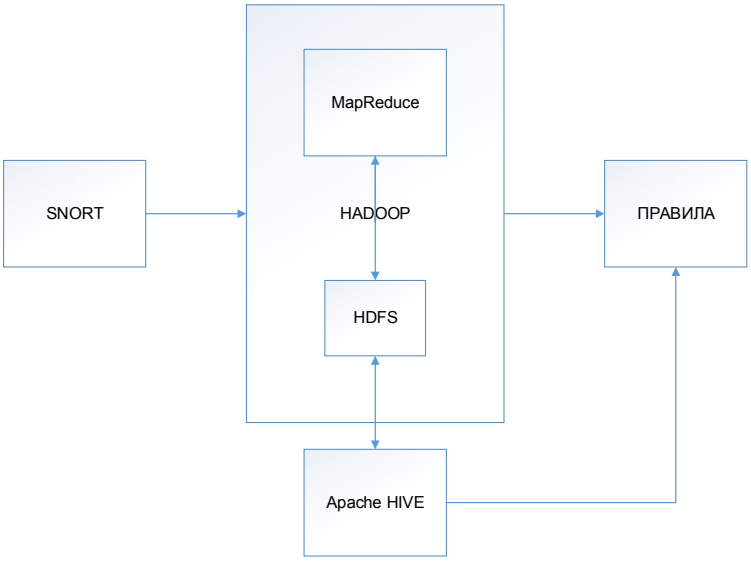


Рисунок. Предлагаемая архитектура обработки данных

Для управления базами данных на основе платформы Hadoop используется Apache Hive. Данная система позволяет выполнять запросы, агрегировать и анализировать данные, хранящиеся в Hadoop. Даже после обработки в Hadoop файл может быть очень большим. Таким образом, для достижения лучших результатов пользователь может выполнить запрос и в течение очень короткого промежутка времени получить информацию о необходимых деталях. После идентификации IP-адреса источника и IP-

адреса узла назначения, могут быть сгенерированы новые правила Snort, если на конкретный узел поступает большое количество пакетов.

В данной реализации главной задачей Hive является максимально упростить SQL-запросы. Создаются таблицы, в которых хранятся ключевые данные от MapReduce и результаты анализа загружаются из HDFS в Hive. Выбранные запросы с условиями будут выполнены как задача Mapreduce и результаты будут отображаться вместе с указанием времени выполнения задания. Вывод запроса может быть записан в файлы.

Особенность методики заключается в том, что для обнаружения аномалий в Snort должны добавляться соответствующие правила, чтобы при будущей аналогичной атаке предпринять соответствующие меры. Необходимо постоянно обновлять и добавлять новые правила для Snort, на основе анализа событий, поступающих в систему. Таким образом, Snort будет способен находить новые атаки, добавляя соответствующие правила и сигнализировать пользователю о потенциальной вредоносной активности.

В заключении следует отметить что, несмотря на многочисленность методов и средств обнаружения компьютерных атак в больших информационных системах, проблема остается до конца не решенной и актуальной. Данные рекомендации помогут лишь уменьшить вероятность получения несанкционированного доступа к защищаемой информации.

В настоящее время авторы работы участвуют в разработке комплекса программно-инструментальных средств для автоматизированной поддержки данной методики [4, 5, 6, 7, 8, 9].

Работа выполняется при поддержке РФФИ (16-29-09482, 18-07-01488) и при частичной поддержке бюджетной темы № АААА-А16-116033110102-5.

Список используемых источников

1. Baddar S. A.-H., Merlo A., Migliardi M. Anomaly Detection in Computer Networks: A State-of-the-Art Review // Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 2014, Vol. 5, No. 4. P.29–64.

2. Govindarajan M., Chandrasekaran R.M. Intrusion Detection Using an Ensemble of Classification Methods // Proc. of the World Congress on Engineering and Computer Science. 2012, Vol. 1. P. 459–464.

3. Oracle White Paper. Anatomy of a Cyber Attack. December 2017. P. 3–7.

4. Котенко И. В., Саенко И. Б. К новому поколению систем мониторинга и управления безопасностью // Вестник Российской академии наук. 2014. Т. 84. № 11. С. 993–1001.

5. Браницкий А. А., Котенко И. В. Анализ и классификация методов обнаружения сетевых атак // Труды СПИИРАН. 2016. Вып. 45. С. 207–244.

6. Котенко И. В., Полубелова О. В., Саенко И. Б., Чечулин А. А. Применение онтологий и логического вывода для управления информацией и событиями безопасности // Системы высокой доступности2012. № 2. С. 100–108.

7. 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.

8. Котенко И. В., Саенко И. Б. SIEM-системы для управления информацией и событиями безопасности // Защита информации. Инсайд 2012. № 5. С. 54–65.

9. Igor Kotenko, Igor Saenko, Alexey Kushnerevich. Parallel big data processing system for security monitoring in Internet of Things networks // Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), Vol. 8, No. 4 (December 2017). P. 60–74.

УДК 004.056

ИССЛЕДОВАНИЕ ДАТЧИКА СЛУЧАЙНЫХ ЧИСЕЛ НА ОСНОВЕ МАГНИТОМЕТРА

В. Д. Корпусов, О. О. Ольховой, В. А. Яковлев

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

Разработан алгоритм и программа для операционной системы Android, позволяющая осуществлять вывод данных магнитометра смартфона на внешний носитель. Рассмотрен принцип построения генератора случайных чисел на основе магнитометра. Исследованы статистические характеристики ГСЧМ по графическим и оценочным тестам. Проверена возможность применения ГСЧМ для криптографических приложений по группе тестов NIST STS.

генераторы случайных чисел, магнитометрические данные, статистические тесты.

Генераторы случайных чисел находят широкое применение в криптографии [1]. В первую очередь они необходимы для генерации случайных последовательностей (ключей) и стартовых векторов в алгоритмах симметричного шифрования и хэширования. Они необходимы для формирования случайных чисел при генерации закрытых ключей в алгоритмах цифровой подписи и шифрования с открытыми ключами. Также случайные последовательности применяются в протоколах аутентификации и распределения ключей и многих других аспектах защиты информации.

Качественные генераторы истинно случайных последовательностей основываются на различных физических процессах и явлениях, имеющих случайную природу. Многие способы получения настоящих случайных чисел не могут быть реализованы на практике, так как используемый в крип-

тографических целях генератор должен быть компактным, быстрым (генерировать числа в реальном времени), независящим от внешних факторов и условий окружающей среды.

Применительно к криптографическим приложениям в области средств вычислительной техники и связи могут быть использованы генераторы случайных чисел (ГСЧ), основанные на измерении флюктуационных шумов электронных приборов, времени доступа к оперативной памяти, времени отклика периферийных приборов, погрешностей счетчиков времени, на основе фиксации прерываний, использовании квантовых эффектов и другие [2]. Главное требование, предъявляемое к ГСЧ, – равномерность и независимость распределения генерируемых символов.

В последнее время интерес исследователей привлекли генераторы случайных чисел на основе магнитометров, встроенных в смартфоны [3], что позволяет решить ряд задач защиты информации в сотовой связи криптографическими методами.

Магнитометр представляет собой устройство для измерения интенсивности одной или нескольких составляющих магнитного поля.

Магнитометры могут быть построены на разных физических принципах. В мобильных устройствах применяются магнитометры на эффекте Холла [4].

Малый размер датчика Холла вместе с другими присущими ему преимущественными характеристиками способствует его встраиванию в корпус смартфона. Датчик Холла обеспечивает линейность, достаточную чувствительность, динамический диапазон для ручных устройств с функциями детектирования геомагнитного поля. В некоторых применениях другие типы магнитных датчиков обеспечивают более высокую чувствительность, что используется для более точных измерений относительно слабого магнитного поля Земли. Но сотовые телефоны часто подвержены воздействию сильных магнитных полей и возмущений, которые могут легко насытить высокочувствительный датчик, который вдобавок может быть весьма чувствителен к шумам. В связи с этим датчик Холла является оптимальным решением для эффективных измерений геомагнитного поля и компенсацией внешних полей и возмущений.

Напряженность магнитного поля не стабильная и неоднородная величина. Имеют место частые возмущения и магнитные бури, изменяющие локально напряженность поля на 100–500 nТл. Магнитные бури вызываются возмущением токов, распространяющихся в ионосфере под влиянием солнечного ветра. Нестабильность напряженности магнитного поля и обусловливает случайность магнитометрических данных.

Целью исследования является анализ возможности применения магнитометра в качестве датчика случайных чисел для криптографических при-

ложений. Для этого необходимо в первую очередь получить последовательность чисел от такого датчика и проверить ее статистические характеристики.

Для анализа было выбрано устройство (*Huawei MediaPad* X1), на котором установлен магнитометр MAG3110 семейства Xtrinsic компании Freescale [4].

Xtrinsic MAG3110 – трехосевой малогабаритный магнитометр с малым энергопотреблением для измерения геомагнитных полей земли. Магнитометр Xtrinsic MAG3110 включает три датчика магнитного поля, ориентированных по осям X (ось направлена на геомагнитный север), Y (на восток) и Z (вверх) и интегральную схему для обработки сигналов, обмена по интерфейсу I²C (последовательная асимметричная шина для связи между интегральными схемами внутри электронных приборов) и реализации других функциональных возможностей. Для упрощения синхронизации магнитометра с внешними устройствами используется сигнал прерывания INT1, который является индикатором наличия новой порции данных на его выходе. Данная функциональность повышает эффективность мобильных устройств, значительно увеличивая срок жизни батарей.

Основные технические характеристики магнитометра MAG3110:

- динамический диапазон: +/– 1,000 мкТл;
- высокое разрешение в полном динамическом диапазоне;
- максимальная частота выборки 80 Гц;
- интерфейс I²C с частотой 400 кГц;
- напряжение питания: 1,95–3,6 В;
- наличие драйвера для ОС;
- механизм прерываний для синхронизации данных;
- ультрамалогабаритный 2×2×0,8 мм 10-ти выводной DFN корпус;
- Диапазон рабочих температур: от –45 до +85 °C.

Для вывода магнитометрических данных разработан алгоритм и написано приложение «Магнитометр-1» в программе Android Studio на языке Java [5].

Приложение позволяет: получить доступ к датчику (*geomagnetic field sensor*), вывести значения датчика на экран, записать значения датчика на определенном отрезке времени и сохранить показания в файловую систему смартфона.

Статистические свойства последовательностей генератора случайных чисел на основе магнитометра (ГСЧМ) были предварительно оценены с использованием двух графических тестов: гистограммы распределения элементов последовательности и распределения на плоскости для магнитометрических данных, полученных по трем осям измерений: X, Y, Z (рис. 1).

В таблице приведены значения математического ожидания и дисперсии полученных последовательностей.

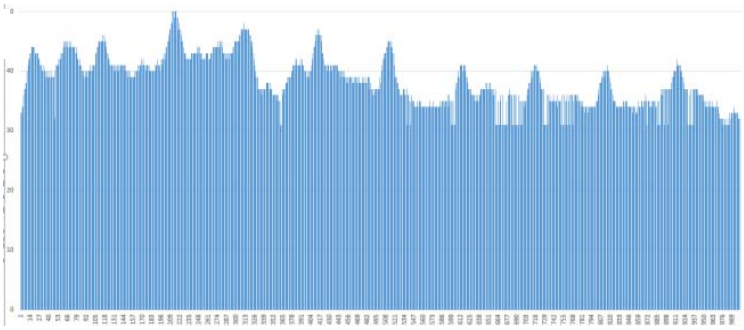
ТАБЛИЦА. Математическое ожидание и дисперсия

	X	Y	Z
Мат. ожидание	38,477	47,75	39,067
Дисперсия	17,372	850,10	3,474

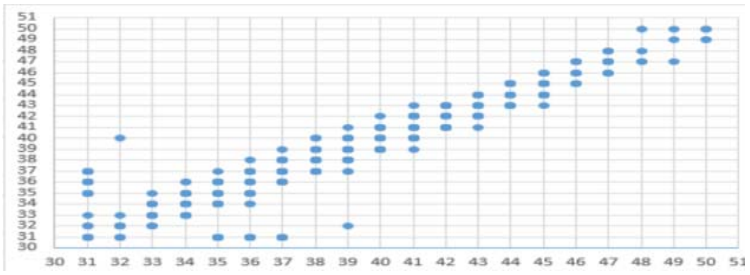
Видно, что только по оси Y обеспечивается равномерность и независимость генерируемой последовательности. Эта же последовательность имеет большую дисперсию, что свидетельствует о ее случайности. Поэтому эта последовательность была выбрана для дальнейших исследований. Обозначим ее ***B***.

Для получения двоичной последовательности, проведено сначала центрирование последовательности ***B***, путем вычитания из каждого значения величины математического ожидания. После этого проведено квантование последовательности ***B***: если $B_i \geq 0$, то в ячейку памяти записывается 1, если $B_i < 0$, записывается 0. Двоичную последовательность обозначим – ***B2.***

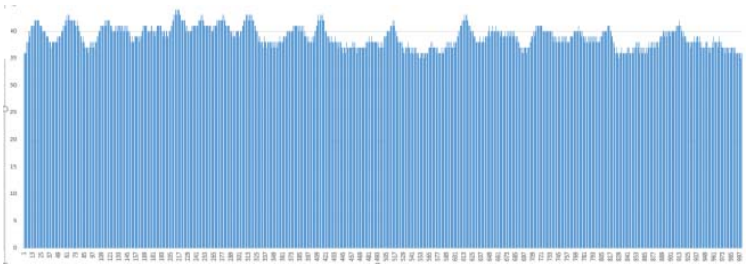
а) X



б)



в) Y



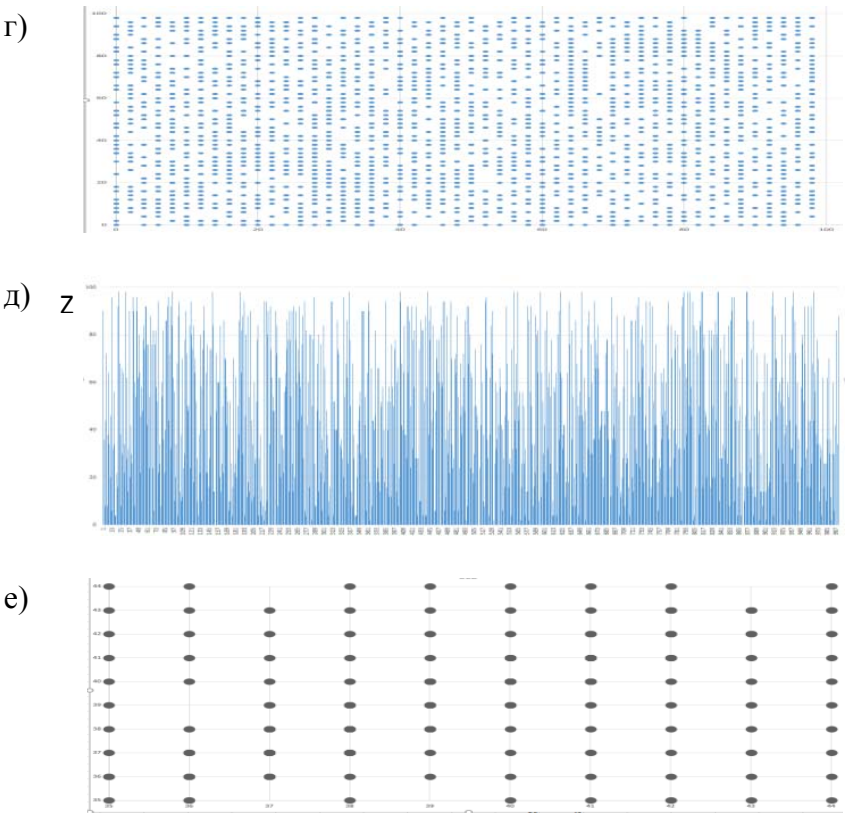


Рисунок. Гистограммы распределения элементов последовательности (а, в, д), результаты теста распределения на плоскости (б, г, е) по осям X, Y, Z

Статистические свойства последовательности $\boldsymbol{B2}$ были оценены по совокупности тестов NIST STS [6, 7]. В состав пакета NIST STS входят 15 статистических тестов, целью которых является определение меры случайности бинарных последовательностей, порождённых либо аппаратными, либо программными генераторами случайных чисел. Эти тесты основаны на различных особенностях, присущих только неслучайным последовательностям. Проверка проводилась на 10 последовательностях длиной 25000 бит каждая.

Тестируемый ГСМЧ показал положительный результат на всех тестах, за исключением теста Runs Test. В этом тесте анализируется количества появлений «блоков» – подпоследовательностей, состоящих из одних единиц, и «дырок» – подпоследовательностей, состоящих из одних нулей.

Для улучшения характеристик ГСЧ была получена новая последовательность путем сложения значений магнитометрических данных по всем координатам $\boldsymbol{B = B_X + B_Y + B_Z}$ магнитометра. После центрирования и квантования этой последовательности получена новая двоичная последовательность B'_2. Анализ статистических свойств $\boldsymbol{B'_2}$ по критериям НИСТ показал отличный результат на всех 15 тестах. Это позволяет сделать вывод о том, что случайные последовательности на основе магнитометрических

данных обладают хорошими статистическими свойствами и могут быть использованы в различных криптографических приложениях.

Авторы видят свою задачу в улучшении производительности ГСМЧ и оценке влияния внешних факторов: температура, снижение заряда аккумуляторной батареи, ориентация смартфона в пространстве на качество генерируемой последовательности.

Список использованных источников

1. Чугунков И. В., Иванов М. А. Теория применение и оценка качества генераторов псевдослучайных последовательностей. М. : Издательство КУДИЦ-ОБРАЗ, 2003. 240 с. ISBN 5-93378-056-1.

2. Агафьин С. С. Построение ДСЧ на основе измерения времени доступа к оперативной памяти. Проблемы информационной безопасности. Компьютерные системы. СПб. : Изд. Политехн. университета. 2015. № 4. С. 90–95.

3. Jin R., Shi L., Zeng K., Pande A., Mohapatra P. MagPairing: Pairing smartphones in close proximity using magnetometers // IEEE Transactions on information forensics and security, June 2016, pp. 1304–1319.

4. Xtrinsic MAG3110 Three-Axis, Digital Magnetometr [Электронный ресурс] // URL: http://www.nxp.com/

5. Установка Android Studio, создание эмулятора [Электронный ресурс] // URL: https://android-school.ru/

6. Статические тесты NIST [Электронный ресурс] // URL: http://csrc.nist.gov/

7. Статистическая проверка случайности двоичных последовательностей методами NIST [Электронный ресурс] // URL: https://habrahabr.ru/

УДК 004.056.2

МЕХАНИЗМЫ ОБЕСПЕЧЕНИЯ ЦЕЛОСТНОСТИ ДАННЫХ И ВЫЧИСЛИТЕЛЬНОЙ ЦЕЛОСТНОСТИ В ОБЛАЧНЫХ СИСТЕМАХ

И. В. Котенко, Е. С. Меркушев

Санкт-Петербургский институт информатики и автоматизации Российской академии наук

В статье проводится систематизация механизмов обеспечения целостности данных и вычислительной целостности в облачных системах: выделяются наиболее распространенные угрозы, обсуждаются стратегии защиты, формулируются перспективные направления исследований в этой области.

облачные системы, целостность данных, вычислительная целостность.

Одними из важнейших механизмов защиты информации являются механизмы обеспечения целостности [1]. Понятие целостность применительно к облачным системам (ОС) подразумевает, что провайдер должен добросовестно хранить доверенные ему данные, а вычислительные задачи пользователей не должны подвергаться каким-либо воздействиям со стороны вредоносных утилит, других пользователей или самого облачного провайдера, причем любые нарушения при хранении данных в облаке (потеря, изменение, компрометация), а также любые некорректные вычисления должны быть обнаружены. Целостность остается одним из наиболее актуальных аспектов в сфере облачных технологий, поскольку в этом случае пользовательские данные и их вычислительные задачи хранятся удаленно на подконтрольных потенциально ненадежным провайдерам серверах, а традиционные механизмы обеспечения целостности зачастую оказываются неприменимы.

Основные угрозы целостности в облачных окружениях принято разделять в соответствии с определением, данным выше. Во-первых, это потеря, изменение или компрометация данных. На серверах провайдера хранится значительное количество информации пользователей. Часть данных может быть повреждена злонамеренно или случайно. Известны случаи [2], когда ошибки администраторов при резервном копировании, восстановлении или миграции приводили к потере данных. Кроме того, атаки различного рода со стороны третьих лиц так же могут привести к утечке, порче или потере данных. Во-вторых, некорректные облачные вычисления. Поскольку вычисления производятся на удаленных ресурсах провайдеров, механизмы вычислений недостаточно прозрачны для клиентов облака. Серверы могут работать некорректно и возвращать ошибочный результат по различным причинам, среди которых можно назвать неправильное конфигурирование провайдером программной или аппаратной части, наличие устаревшего и (или) уязвимого кода, присутствие зараженных вычислительных узлов.

Ввиду увеличения объема хранимой в облачных системах информации, традиционные методы, требующие вычисления хэша целого файла на стороне провайдера, становятся недоступными. Неоправданным оказывается и механизм, при котором необходимо скачивать файл с сервера, а затем самостоятельно выполнять проверку целостности, поскольку это влечет за собой большие вычислительные расходы и требует высокой пропускной способности.

Для проверки целостности данных, хранимых на удаленных серверах, предлагаются различные *протоколы доказательства обладания данными* (*Proof of Data Possession,* PDP) [2].

Оригинальная PDP-модель предполагает наличие на стороне клиента метаданных, которые должны быть сформированы перед загрузкой информации на удаленный сервер [2]. Для проверки целостности файла клиенту

необходимо отправить запрос на сервер, который, в свою очередь, должен ответить сообщением, основанным на интересующем клиента файле. Сопоставляя ответ сервера с имеющимися у клиента метаданными, можно судить о доступности файла в его первоначальном виде. Описанная модель позволяет достичь высокой вероятности определения некорректной работы сервера при незначительных вычислительных расходах и издержках на хранение информации, однако она применима только для файлов, которые не изменяются после загрузки на сервер.

Другой механизм проверки целостности данных – *доказательство извлечения* (*Proof of retrievability,* POR) [3], т. е. того, что файл - в наличии и может быть извлечен. Эта модель предназначена для минимизации как объемов хранения данных (как на стороне клиента, так и на сервере), так и сложности выполнения проверки и числа блоков данных, к которым необходимо обращаться при проверке. Пользователь хранит только ключ, использующийся для шифрования исходного файла *F* в *F'*, причем в *F'* внедряется набор контрольных значений. Сервер хранит зашифрованный файл *F'*, не зная, где именно расположены контрольные значения, поскольку они неотличимы от обычных блоков данных. Для проверки целостности файла серверу необходимо вернуть некоторое подмножество контрольных значений *F'*. Если *F'* изменен или удален, велика вероятность того, что необходимые контрольные значения также испорчены или потеряны. Из-за ограниченного количества контрольных значений, при незначительных повреждениях файла предлагаемый протокол может возвращать ошибочное подтверждение целостности данных. Как оригинальную PDP-модель, так и POR-модель можно использовать только для статичных файлов, что снижает их применимость в облаках, поскольку последним свойственна динамическая обработка данных.

Динамическая PDP-модель [4] обладает полной поддержкой операций добавления, изменения, вставки и удаления. Результаты экспериментов показывают, что, несмотря на рост вычислительных затрат, модель оказывается эффективной. Например, для проверки целостности файла размером 1Гб, динамической модели необходимо сгенерировать всего 415 Кб данных и потратить 30 мс на вычислительные расходы. Протокол рассматриваемой PDP-модели имеет три новые операции: «подготовить изменение», «применить изменение», «проверить изменение». Первая запускается клиентом для подготовки запроса на обновление данных (изменить блок *i*, удалить блок *j* и т. д.). Вторая запускается сервером для фактического обновления файла, после чего возвращает доказательство изменения клиенту, который, в свою очередь, проверяет поведение сервера во время изменения данных.

Модель слоя высокой доступности и целостности для облачного хранения (*High-Availability and Integrity Layer,* HAIL) [5] отличается от упомя-

нутых выше, поскольку предлагает распределенное окружение, при котором клиент должен загружать файл сразу на несколько серверов с резервированием и хранить только небольшое неизменное состояние на локальном устройстве.

Вместо предоставления пользователям возможности самостоятельно проверять целостность данных, поставщик услуг может делегировать эту задачу третьим лицам, которым доверяет как клиент, так и провайдер облака [6]. Сторонний аудитор в таком случае должен гарантировать эффективную проверку целостности данных без локальной копии информации, отсутствие новых уязвимостей для конфиденциальности пользовательских данных.

Проверка корректности удаленных облачных вычислений – задача более трудоемкая и актуальная. Традиционные стратегии проверки делятся на 4 категории: повторное вычисление, репликация, аудит, доверенные вычисления.

Повторное вычисление: необходимо еще раз произвести вычисления локально и сравнить с полученными ранее результатами. Стратегия гарантирует 100 %-ю точность определения ошибки, не требует доверия к облачному поставщику. Однако стоимость оказывается значительной, поскольку каждая проверка требует, как минимум, столько же времени, сколько потрачено на удаленное вычисление. По этой причине клиенты не используют рассматриваемую стратегию в чистом виде. Разновидность повторного вычисления – *выборочное вычисление* [7], которое предоставляет вероятностные гарантии обнаружения ошибок, зависящие от выборки. Выборочное повторное вычисление жертвует точностью ради эффективности.

Репликация назначает одно задание нескольким устройствам, затем сравнивает результаты. Относительное большинство совпадающих результатов позволяет судить о правильности вычислений. Репликация предполагает наличие некоторого доверия к поставщику облака, поскольку вычисления и проверка правильности производятся удаленно. Злоумышленник, контролирующий определенную часть машин, может обойти проверку корректности результата с помощью репликации, возвращая с подконтрольных ему устройств некорректный результат, аналогичный полученному ранее.

Аудит [8] обычно применяют совместно с журналированием. Во время выполнения вычислений отдельный компонент записывает все критические события в журнал, который отправляется одному или нескольким аудиторам для проверки. Аудит – типичный подход для криминалистической проверки. Один из недостатков аудита заключается в том, что злоумышленник лучше, чем проверяющий, разбирается в вычислениях, что позволяет ему оставаться незамеченным, изменяя некоторые данные.

Доверенные вычисления [9, 10, 11, 12] обеспечивают единообразное заранее известное поведение аппаратной и программной частей устройств.

Ключевым методом проверки целостности является удаленная аттестация: оборудование генерирует сертификат, содержащий подробные сведения о том, какое программное обеспечение запущено. Данный сертификат отправляется проверяющему для подтверждения того, что программное обеспечение не было изменено. Предположение, на котором основывается метод доверительных вычислений, заключается в том, что некоторые компоненты, например, аппаратная часть и гипервизор не изменены злоумышленником.

Некоторые методы проверки вычислительной целостности зависят от сферы использования. Например, в [13] используя теорему двойственности линейного программирования и получая условия, которым должно удовлетворять решение, механизм проверки увеличивает стоимость вычислений, как для сервера, так и для клиентов, на величину близкую к нулю. Алгоритм, предложенный в [14], проверяет умножение квадратных матриц порядка m за $O(m^2)$.

Касательно целостности данных в облачных системах выделяют две основные проблемы: (1) значительные объемы данных исключают использование обычных алгоритмов хэширования; (2) проверка целостности может быть применена только после реализации дополнительных требований, которые увеличивают сложность. Например, поддержка динамических операций над данными из облака с применением механизмов проверки целостности – нетривиальная задача. Однако реализация механизмов обеспечения вычислительной целостности – значительно более трудоемкий процесс. Главной проблемой является недостаток информации о внутренних вычислениях. Правильно спроектированные методы проверки должны удовлетворять следующим условиям: нагрузка локальных вычислений для проверки целостности должна быть меньше, чем для исходного удаленного вычисления; должна иметься возможность производить проверку на любой из составных частей для обеспечения отказоустойчивости.

Авторами в настоящее время ведутся исследования по защите информации при реализации облачных технологий больших данных для мониторинга безопасности [15, 16].

Работа выполняется при финансовой поддержке РФФИ (проекты 16-29-09482 и 18-07-01488) и бюджетной темы АААА-А16-116033110102-5.

Список используемых источников

1. Котенко И. В., Юсупов Р. М. Перспективные направления исследований в области компьютерной безопасности // Защита информации.Инсайд. 2006. № 2. С. 46–57.

2. Ateniese G., Burns R., Curtmola R., Herring J., Kissner L., Peterson Z., Song D. Provable data possession at untrusted stores // ACM conference on Computer and communications security, ACM, 2007. P. 598–609.

3. Juels A., Kaliski B. S. PORs: Proofs of retrievability for large files // ACM conference on Computer and communications security. ACM, 2007. P. 584–597.

4. Erway C., Küpçü A., Papamanthou C., Tamassia R. Dynamic provable data possession // ACM conference on Computer and communications security. 2009. P. 213–222.

5. Bowers K. D., Juels A., Oprea A. HAIL: A high-availability and integrity layer for cloud storage // ACM conference on Computer and communications security, 2009. P. 187–198.

6. Wang C., Wang Q., Ren K., Lou W. Privacy-preserving public auditing for data storage security in cloud computing // IEEE INFOCOM 2010, IEEE, 2010. P. 1–9.

7. Xiao Z., Xiao Y. Accountable MapReduce in Cloud Computing // IEEE Conference on Computer Communications Workshops. IEEE, 2011. P. 1082–1087.

8. Haeberlen A., Kuznetsov P., Druschel P. PeerReview: Practical accountability for distributed systems // ACM Symposium on Operating Systems Principles. 2007. P. 175–188.

9. Santos N., Gummadi K. P., Rodrigues R. Towards trusted cloud computing // Conference on hot topics in cloud computing. USENIX Association Berkeley, 2009.

10. Десницкий В. А., Котенко И. В. Защита программного обеспечения на основе механизма «удаленного доверия» // Изв. вузов. Приборостроение 2008. Т. 51, № 11. С. 26–30.

11. Десницкий В. А., Котенко И. В. Методы защиты программного обеспечения на основе принципа удаленного доверия // Защита информации. Инсайд. 2009. № 6. С. 57–61.

12. Котенко И. В., Десницкий В. А. Аспектно-ориентированная реализация модели защиты программ на основе «удаленного доверия» // Информационные технологии и вычислительные системы. 2009. № 4. С. 67–76.

13. Wang C., Ren K., Wang J. Secure and Practical Outsourcing of Linear Programming in Cloud Computing // IEEE Trans. Cloud Computing: IEEE, 2011. P. 820–828.

14. Monrose F., Wyckoff P., Rubin A. D. Distributed execution with remote audit // Network and Distributed System Security Symposium. ISOC, 1999.

15. Novikova E., Kotenko I. Analytical Visualization Techniques for Security Information and Event Management // Proceedings of the 2013 21st Euromicro International Conference on Parallel, Distributed, and Network-Based Processing, PDP 2013. P. 519–525.

16. Котенко И. В., Полубелова О. В., Саенко И. Б., Чечулин А. А. Применение онтологий и логического вывода для управления информацией и событиями безопасности // Системы высокой доступности. 2012. Т. 8. № 2. С. 100–108.

УДК 004.056.53

МОДЕЛИ NOSQL БАЗ ДАННЫХ ДЛЯ МОНИТОРИНГА КИБЕРБЕЗОПАСНОСТИ

И. В. Котенко[1], И. А. Ушаков[2]

[1]Санкт-Петербургский институт информатики и автоматизации Российской академии наук
[2]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье приведены основные модели NoSQL баз данных, включающие в себя модели БД вида ключ-значение, документные БД, БД семейства столбцов, графовые БД.

Проводится сравнительный анализ существующих моделей и делается вывод о целесообразности использования существующих моделей данных для мониторинга кибербезопасности.

большие данные, NoSQL базы данных, информационная безопасность, мониторинг.

Реляционные базы данных, широко используемые в настоящее время для хранения информации многими организациями, хорошо зарекомендовали себя в случае хранения ограниченного набора данных [1]. Хранение огромных массивов информации становится неэффективным в реляционных базах данных. Это обусловливает актуальность появления отличных от реляционных баз данных – NoSQL.

NoSQL базы данных можно разделить на четыре категории [2, 3, 4]:

1. Ключ-значение (*Key-Value*) – базы данных NoSQL, рассчитанные на нагрузки с большим количеством операций чтения (например, социальные сети, игры, сервисы обмена мультимедийными материалами и порталы вопросов и ответов) или нагрузки с повышенными требованиями к вычислительной мощности (например, сервисы рекомендаций). Кэширование в памяти позволяет увеличить производительность приложений за счет сохранения критически важных блоков данных в памяти для последующего доступа к ним с минимальными задержками. Примерами баз данных (БД) являются: BerkeleyDB, LevelDB, Redis, Riak.

2. Документные базы данных (*Document Databases*) используются для хранения частично структурированных данных в виде документов, обычно в формате JSON или XML. В отличие от традиционных реляционных баз данных, каждый из нереляционных (NoSQL) документов может обладать собственной схемой, что предоставляет большую гибкость организации и хранении данных приложения, а также сокращает объем хранилища для необязательных значений. Примерами БД являются: CouchDB, MongoDB, OrienDB, RavenDB.

3. Базы данных семейства столбцов (*Column-Family Stores*) – рассчитаны на чтение и запись данных в виде столбцов, а не строк. Столбчатый подход к хранению таблиц баз данных имеет важное значение для производительности аналитических запросов, поскольку он значительно снижает общие требования к операциям дискового ввода-вывода и снижает объем данных, которые требуется загружать с диска [3]. Примерами БД являются: Cassandra (рис. 1), HBase, Hypertable, Amazon SimpleDB.

4. Графовые базы данных (*Graph Databases*) хранят вершины и направленные связи, называемые ребрами (рис. 2) [3]. Графы могут быть построены с использованием реляционных (SQL) и нереляционных баз данных (NoSQL). Каждая вершина или ребро может обладать набором собственных свойств. Примерами БД являются: FlockDB, HyperGraphDB, OrientDB.

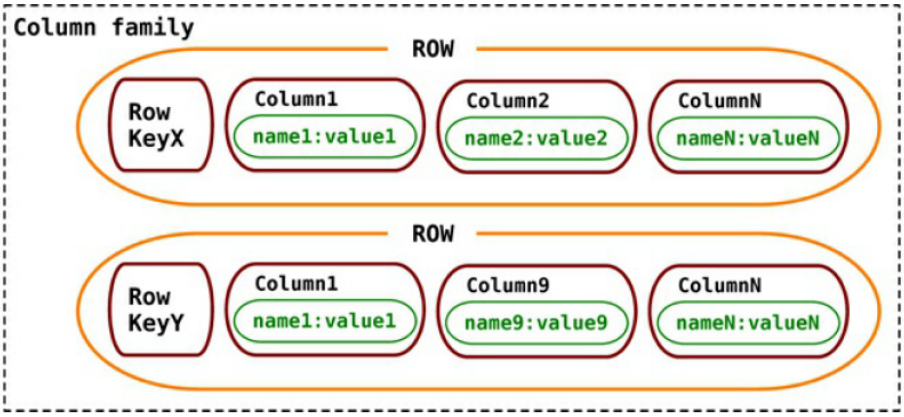


Рис. 1. Структура базы данных Cassandra на основе семейства столбцов

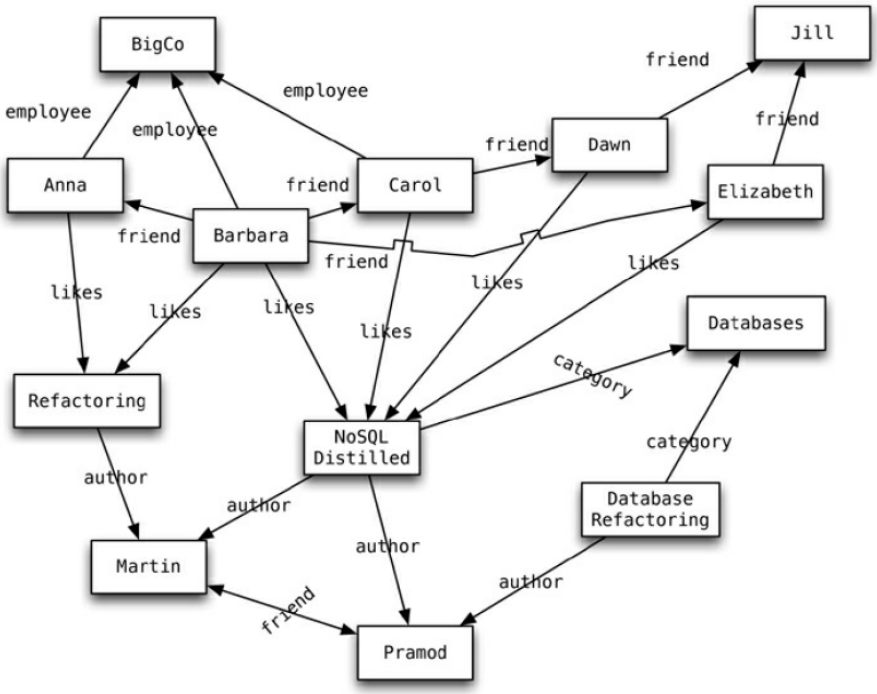


Рис. 2. Пример структуры графовой базы данных

Для решения задач мониторинга кибербезопасности наиболее подходящими категориями являются БД семейства столбцов, обеспечивая горизонтальную масштабируемость. Поэтому они подходят для задач, связанных с большими данными, когда база размещается в кластере из десятков, сотен, а то и тысяч узлов [5, 6].

Также для решения задач мониторинга кибербезопасности подходят документные базы данных, так как они подходят к решению задач с высокой степенью изменчивости.

Эти параметры являются критичными для мониторинга кибербезопасности, где важны такие параметры, как скорость обработки информации

и принятия решения, а также изменчивость поведения злоумышленника в компьютерной сети [7, 8].

Работа выполняется при поддержке РФФИ (16-29-09482, 18-07-01488) и при частичной поддержке бюджетной темы № АААА-А16-116033110102-5.

Список используемых источников

1. Tauro C. J. M, Aravindh S., Shreeharsha A. B. Comparative Study of the New Generation, Agile, Scalable, High Performance NOSQL Databases // International Journal of Computer Applications, Vol. 48, No. 20, June 2012.

2. Что такое NoSQL. URL: https://aws.amazon.com/ru/nosql/ (дата обращения 29.03.2017).

3. Sadalage P. J., Fowler M. NoSQL Distilled. A Brief Guide to the Emerging World of Polyglot Persistence. 2013. Pearson Education, Inc.

4. Редмонд Э., Уилсон Д. Р. Семь баз данных за семь недель. Введение в современные базы данных и идеологию NoSQL. М. : ДМК Пресс, 2013. 384 с.

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

6. Василишин Н. С., Ушаков И. А., Котенко И. В. Исследование алгоритмов анализа сетевого трафика с использованием технологий больших данных для обнаружения компьютерных атак // Информационные технологии в управлении (ИТУ-2016). Материалы 9-й конференции по проблемам управления. 2016. С. 670–675.

7. 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.

8. Котенко И. В., Саенко И. Б. SIEM-системы для управления информацией и событиями безопасности // Защита информации. Инсайд. 2012. № 5. С. 54–65.

УДК 004.056.53

МЕТОДИКИ ПОИСКА ИНСАЙДЕРОВ В КОМПЬЮТЕРНЫХ СЕТЯХ НА ОСНОВЕ ТЕХНОЛОГИЙ БОЛЬШИХ ДАННЫХ

И. В. Котенко[1], И. А. Ушаков[2]

[1]Санкт-Петербургский институт информатики и автоматизации Российской академии наук
[2]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Задача выявления инсайдеров в современных компьютерных сетях является одной из основных. Выявление инсайдеров в КС является трудновыполнимой задачей, в особен-

ности, с учетом огромного потока информации, который генерируется пользователями в КС. Необходимо из общего потока информации и событий выделить ту информацию, которая позволяет идентифицировать внутренних нарушителей. В статье проанализирован подход к защите от инсайдеров в компьютерных сетях, базирующийся на использовании платформы контроля безопасности корпоративных сетей Cisco ISE и ее интеграции с технологией обработки больших данных, реализуемой авторами.

большие данные, выявление инсайдеров, инсайдер, компьютерные сети.

В настоящее время задача выявления инсайдеров является крайне актуальной задачей [1, 2, 3]. Большинство исследований в области поиска инсайдеров в компьютерной сети основаны на использовании различных статистических методов выявления аномалий в деятельности сотрудников организации.

Инсайдерская атака – это злонамеренная атака, совершенная в сети или компьютерной системе персоной, имеющей доступ в эту сеть или систему. Инсайдер – сотрудник компании, имеющий доступ к конфиденциальным данным, размещенным в компьютерной сети предприятия. Инсайдерские атаки оказывают большую угрозу безопасности сети, поскольку злоумышленники, которые осуществляют эти атаки, имеют доступ к ресурсам системы и могут быть знакомы с архитектурой сети. Кроме того, многие организации основное внимание уделяют защите от внешних нападений и недостаточно заботятся о безопасности внутри сети.

Основные причины осуществления инсайдерских атак:

корпоративные политики не определены, либо определены, но не выполняются или определены не корректно;

используемое пользователями программное обеспечение не контролируется (применяется стороннее ПО, небезопасные Интернет-браузеры и т. д.);

у пользователей имеются повышенные привилегии.

Основной задачей защиты от инсайдерских атак является организация адекватного распределения полномочий доступа к корпоративным ресурсам. Компании должны осуществлять внутренний контроль, чтобы обнаруживать, и предотвращать доступ к закрытым ресурсам, разрешая его только тем людям, которым это необходимо для выполнения своей работы.

Чтобы защититься от инсайдерских атак в организации должен выполняться учет и контроль всех успешных и неудавшихся попыток доступа к закрытым ресурсам компании, которые должны быть зарегистрированы, проверены или рассмотрены на регулярной основе. Наряду с этим, все изменения производственных данных и систем должны быть зарегистрированы, чтобы производить учет измененных данных и автора изменений. Регистрация и контроль всех корпоративных процессов требует больших ресурсов и внимания, поэтому важно идентифицировать самые критические

активы компании и обеспечить грамотный и удобный учет и механизмы контроля этих активов.

Из коммерческих решений в этой области стоит отметить решение компании Cisco Systems – Identity Services Engine (ISE) [4, 5]. Cisco Identity Services Engine – это платформа контроля безопасности корпоративных сетей, содержащая сервисы аутентификации, авторизации и учета (AAA), профилирования, оценки состояния и управления гостевым доступом в одном решении.

Платформа Cisco ISE содержит заранее составленные шаблоны устройств, которые могут использоваться в корпоративной сети. Этими устройствами могут являться принтеры, IP-телефоны, смартфоны, IP-камеры и планшеты.

Cisco ISE получает информацию о функциях оконечных устройств при помощи сканирования этих устройств, выполнения программ сетевой телеметрии и обмена информацией с сенсорами устройств. Сканирование информации осуществляется при помощи десяти проб: NetFlow Probe, DHCP Probe, DHCP SPAN Probe, HTTP Probe, HTTP SPAN Probe, RADIUS Probe, Network Scan Probe, DNS Probe, SNMP Query Probe, SNMP Trap Probe.

Архитектура Cisco ISE позволяет предприятиям собирать контекстную информацию в реальном времени из сетей, пользователей и устройств. Администратор может использовать эту информацию, чтобы принимать различные решения управления, идентифицируя различные элементы сети, такие как коммутаторы доступа, беспроводные LAN-контроллеры (WLC), шлюзы виртуальных частных сетей (VPN) и коммутаторы дата-центра.

Cisco ISE использует следующие основные образы:

1. Образ администрирования. Этот образ выступает в качестве интерфейса для формирования и синхронизации политик. Этот образ является контролирующим центром в архитектуре Cisco ISE, он также обычно контролирует лицензирование и содержит пользовательский интерфейс. Образ администрирования в процессе распределенного внедрения ответственен за передачу настроек на другие узлы. Узлы, которые обрабатывают образ администрирования, обычно относят к узлам администрирования. Узлы администрирования выполняют следующие функции: лицензирование, администрирование аутентификации, администрирование авторизации, администрирование учета.

2. Образ сервисов политик. Этот образ является программой, которая создает решения политик. Этот образ обеспечивает обработку всех сетевых сообщений, включая DHCP, CDP, NetFlow и RADIUS. Узлы, которые обрабатывают образ сетевых политик, обычно относят к узлам сервисов политик. Узлы сервисов политик оценивают и создают условия политик для следующих функций: сетевой доступ, оценка состояния, гостевой доступ, профилирование, клиентское обеспечение.

3. Образ мониторинга. Этот образ выступает в качестве интерфейса для логирования и просмотра отчетных данных. Эта программа собирает логи и упорядочивает их. Также она используется для создания отчетов и уведомлений для системы Cisco ISE. Узлы, которые обрабатывают образ мониторинга, обычно относят к узлам мониторинга. Узлы мониторинга предназначены для сбора логов, упорядочивания событий и создания отчетов. Узлы мониторинга также могут передавать собранную информацию на удаленные базы данных.

4. Образ pxGrid [6]. Этот образ обеспечивает интеграцию систем безопасности с Cisco-платформой для передачи контекстной информации между устройствами.

Взаимодействие устройств в архитектуре Cisco ISE.

На схеме показано логическое взаимодействие различных узлов друг с другом (рис.):

1. Клиент (пользователь/устройство) пытается получить доступ.

2. Клиент подключается через Network Access Device (NAD), который может являться коммутатором, беспроводным контроллером или адаптивным устройством безопасности, таким как VPN концентратор.

3. Клиент проходит аутентификацию путем отправки запроса RUDIUS на узел сервисов политик.

4. Используя настройки, полученные от узла администрирования, узел сервисов политик обрабатывает учетные данные, предоставленные клиентом, и, основываясь на условиях политик, принимает решение авторизации.

5. Узел сервисов политик может запросить необходимые данные у внешнего сервера идентификационных данных, такого как Microsoft Active Directory, LDAP или токен сервера.

6. Узел сервисов политик возвращает для обработки свое решение на NAD. Это решение содержит такие функции, как присвоение VLAN, dACL или SGT.

7. Основываясь на этом решении, клиент получает возможность посылать свой трафик через NAD на запрашиваемый сетевой ресурс.

8. Всё логирование, такое как syslog от NAD, или данные об аутентификации RADIUS от узла сервисов политик могут быть отправлены на узел мониторинга для классификации и обработки.

9. Узел администрирования содержит графический интерфейс, который позволяет просматривать данные, собранные узлом мониторинга, а также просматривать и настраивать политики на узле сервисов политик.

Cisco ISE содержит большой выбор инструментов, позволяющих отслеживать доступ пользователей. Вся необходимая информация отображается в приборной панели. Она хранится в базах данных и может использоваться в целях мониторинга работы пользователей и обнаружения инсайдеров.

Рисунок. Схема взаимодействия устройств в архитектуре Cisco ISE

В последнее время все больше исследователей рассматривают методы поиска инсайдеров на основе технологий больших данных [7]. Данные исследования направлены на предобработку полученных данных с различных сенсоров телеметрии и последующее принятие решения о блокировке инсайдера на основании обработки полученных данных.

Несмотря на преимущества коммерческого проекта Cisco ISE, использование данного продукта без применения технологий потоковой обработки данных [8, 9] не позволяет в полной мере учитывать все действия злоумышленника в сети в различные моменты времени.

Решение pxGrid выступает в роли интегрированной платформы для объединения различных элементов сетевой безопасности и обладает возможностью комплексирования передаваемых данных между собой и требует отдельного анализа.

В настоящее время авторы разрабатывают собственную методику выявления инсайдеров с использованием механизмов потоковой обработки данных и платформы Cisco ISE [10, 11]. Методика основана на использовании программного обеспечения Elastic Stack.

Работа выполняется при поддержке РФФИ (16-29-09482, 18-07-01488) и при частичной поддержке бюджетной темы № АААА-А16-116033110102-5.

Список используемых источников

1. Грушо А. А., Забежайло М. И., Смирнов Д. В., Тимонина Е. Е. Модель множества информационных пространств в задаче поиска инсайдера // Информатика и ее применения. 2017. Т. 11, вып. 4. С. 65–69.

2. Anomaly Detection at Multiple Scales (ADAMS). – General Services Administration, 22.10.2010. URL: https://www.fbo.gov/download/2f6/2f6289e99a0c04942b bd89ccf242fb4c/DARPA-BAA-11-04ADAMS.pdf.

3. Senator T., Goldberg H. G., Memory A., et al. Detecting insider threats in a real corporate database of computer usage activity // 19th ACM SIGKDD Conference. (International) on Knowledge Discovery and Data Mining Proceedings. New York, NY, USA: ACM, 2013. P. 1393–1401.

4. 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. 2015. С. 310–313.

5. Woland A., Heary J. Cisco ISE for BYOD and Secure Unified Access, 2nd Edition. // Jun 16, 2017 by Cisco Press.

6. Технология Cisco PxGrid. URL: https://www.cisco.com/c/dam/global/ru_ru/about/brochures/assets/pdfs/white-paper-c11-735489.pdf. (дата обращения 29.03.2017).

7. Thuraisingham B., Mehedy M., Pallabi M., Latifur Khan P. Big Data Analytics with Applications in Insider Threat Detection // CRC Press by Taylor & Francis Group, LLC 2018.

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

9. Василишин Н. С., Ушаков И. А., Котенко И. В. Исследование алгоритмов анализа сетевого трафика с использованием технологий больших данных для обнаружения компьютерных атак // Информационные технологии в управлении (ИТУ-2016) Материалы 9-й конференции по проблемам управления. 2016. С. 670–675.

10. Котенко И. В., Кулешов А. А., Ушаков И. А. Система сбора, хранения и обработки информации и событий безопасности на основе средств Elastic Stack // Труды СПИИРАН. 2017. № 5 (54). С. 5–34.

11. Igor Kotenko, Artem Kuleshov and Igor Ushakov. Aggregation of Elastic Stack Instruments for Collecting, Storing and Processing of Security Information and Events // The 14th IEEE Conference on Advanced and Trusted Computing (ATC 2017). San Francisco, August 4-8, 2017, USA. Los Alamitos, California. IEEE Computer Society. 2017. P. 1550–1557.

УДК 004.414

РИСКИ ПРИ РЕАЛИЗАЦИИ ТЕХНОЛОГИИ BYOD В ОРГАНИЗАЦИЯХ И РЕШЕНИЯ ДЛЯ ИХ МИНИМИЗАЦИИ

А. В. Красов, А. Н. Рогова

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

В данной статье рассмотрены риски, которые могут возникать при реализации технологии BYOD в организациях. К таким рискам относятся нарушения безопасности и конфиденциальности. Были рассмотрены инструменты для их минимизации. Приведены практические решения для организаций для уменьшения описанных ранее рисков.

BYOD, риски, мобильные устройства, проблемы безопасности.

Сегодня, во времена, когда рабочее место можно организовать где угодно и когда угодно, устанавливать границы для программ BYOD становится сложнее.

Поскольку трудовые ресурсы становятся все более мобильными и доступными с помощью смартфонов, планшетов и ноутбуков, организации становится все более подверженными рискам безопасности и конфиденциальности.

Безопасность и конфиденциальность – те риски, с которыми сталкиваются как сами организации, так и сотрудники. Организации более обеспокоены безопасностью корпоративных данных и тем, как им угрожает поведение пользователей. Сотрудники больше озабочены конфиденциальностью своих личных данных, и какие права на них имеют работодатели.

Рассмотрим риски для безопасности, которым подвержены сотрудники и организации. Одним из неотъемлемых недостатков BYOD является потеря контроля и видимости данных предприятия, которые передаются, хранятся и обрабатываются на персональном устройстве. Отсюда вытекает риск потенциальной утечки данных или раскрытие данных предприятия с незащищенного устройства. Такие риски возникают и при физической потере или краже устройства.

Концепция BYOD восприимчива к атакам «человек-в-середине» и подслушиванию в общественных точках доступа Wi-Fi, которые часто используются удаленными работниками.

Устройства, которые используют сотрудники, также могут быть использованы – случайно или намеренно – третьей стороной, например, друзьями или семьей, что может привести к потере или компрометации конфиденциальных данных. При размещении личной и корпоративной информации на одном устройстве существует риск случайного удаления корпоративных данных при намеренном удалении какой-либо персональной информации.

Существенным риском является использование на личных устройствах таких процедур, как «Jailbreaking», «root» и «unlock» в целях удаления ограничений конфигурации поставщиков. Это делает устройства более уязвимыми для небезопасных приложений. Они могут иметь доступ к датчикам устройства (например, к микрофону, камере) или к конфиденциальным данным, хранящимся на устройстве, без ограничений [1].

Также устройства BYOD уязвимы для инсайдерских атак, которые трудно предотвратить, поскольку они происходят в локальной сети (LAN) организации, используя действительный профиль пользователя.

Проблемам конфиденциальности подвержены сотрудники компаний, использующие устройства BYOD. Поскольку эти устройства имеют доступ к серверам и сетям, компании так же имеют к ним доступ. Работодатели не столько заинтересованы в том, что делают сотрудники в свободное время,

сколько в том, может ли то, что они делают, каким-либо образом подорвать безопасность компании. Совершенно ясно, что есть тонкая грань, когда дело доходит до того, насколько глубоко организации могут, должны и должны вникать в личные данные.

Рабочие мобильные устройства могут подвергаться запросу на обнаружение в контексте судебного процесса, связанного с организацией. Это ставит под угрозу конфиденциальность личных данных пользователей.

У сотрудников есть риск потери личных данных. Внутри компании безопасность BYOD может основываться на программном обеспечении, которое не делает различия между личными и корпоративными данными. Таким образом, если есть предполагаемое нарушение безопасности, все на устройстве – персональном и корпоративном – может автоматически быть удалено (называется удаленной очисткой). Также ИТ-отдел компании может отслеживать физическое местоположение сотрудника в любое время и быть в курсе его онлайн-активности.

Рассмотрим технологии, которые способны минимизировать вышеперечисленные риски для безопасности и конфиденциальности данных.

Система управления мобильными устройствами (MDM) способна производить удаленную очистку всех данных с устройства и определять его местонахождение, если оно было утеряно. MDM также хорошо справляется с сегрегацией данных [2]. Например, совместная работа и личные контакты в одной адресной книге создают высокий риск утечки данных. Сотрудник может неправильно выбрать личный контакт в качестве получателя и случайно опубликовать конфиденциальную информацию о компании.

Управление мобильностью предприятия (EMM) схоже с MDM. Основное различие заключается в том, что MDM управляет функциями устройства, в то время как EMM управляет всем устройством [2].

Еще одним средством для снижения рисков для безопасности является контейнеризация виртуально-хостируемого рабочего стола (VHD). VHD создает полноценный образ рабочего стола, который включает операционную систему, все приложения и настройки. Любой компьютер может получить доступ к рабочему столу с обработкой и хранением на центральном сервере. Контейнер VHD помещает собственные приложения в безопасную зону на устройстве. Он эффективно изолирует и защищает их от определенных функций, таких как беспроводные сетевые соединения, порты USB или камеры устройства.

Управление доступом к сети (*Next Gen* NAC) аутентифицирует пользователей, реализует приложения безопасности и ограничивает доступность сетевых ресурсов конечным устройствам в соответствии с определенной политикой безопасности, особенно для мобильных устройств [3]. Администраторы могут создавать и автоматически применять строгие политики

доступа. С Next Gen NAC сеть распознает личность пользователя. Он позволяет им получать доступ к ресурсам, которые им необходимы, применяя строгие правила для роли пользователя. Он лучше всего работает с MDM, что позволяет организациям контролировать, управлять, защищать и применять политики безопасности на устройствах сотрудников.

Система предотвращения потери данных (DLP) направлена на то, чтобы конечные пользователи не отправляли потенциально чувствительную или критическую информацию вне корпоративной сети. По мере создания информации, инструменты DLP могут применять к ней политику использования, будь то файл, электронная почта или приложение. Система сначала прикрепляет ЦВЗ на конфиденциальные данные, затем, отслеживает, как, когда и кому эти данные будут доступны и/или переданы.

Метод удаленной очистки – это возможность удаленного удаления данных с устройства. Она включает перезапись сохраненных данных для предотвращения судебного восстановления и возврат устройства к исходным заводским настройкам. Поэтому любые данные, когда-либо сделанные на нем, будут недоступны для всех.

Комплексная стратегия, которую следует использовать организациям для снижения рисков BYOD, должна включать в себя такие решения, которые лучше всего работают при использовании в тандеме, таких как MDM и NAC.

Для наиболее успешного уменьшения рисков, компании могут придерживаться следующих решений. В первую очередь, организации должны понимать свои собственные требования к защите данных.

Компании должны регулярно обновлять операционные системы, браузеры и другие приложения с помощью последних исправлений безопасности.

На устройствах сотрудников, покидающих компанию, надлежащим образом должны быть уничтожены корпоративные данные. В противном случае, риск утечки любых данных, которые могут быть скомпрометированы, может оставаться и в будущем.

Следует ограничить доступ к корпоративным данным в зависимости от характера работы сотрудника. Разумное предоставление данных обеспечивает минимальный необходимый доступ к конфиденциальным данным.

Трассировка устройств. Решение заключается в том, чтобы компании применяли строгую политику отслеживания устройств. Таким образом, они всегда будут знать о местонахождении всех корпоративных устройств, независимо от того, используются они или нет. Еще одной хорошей практикой является внедрение системы наблюдения, которая может контролировать все устройства, входящие и выходящие из помещения компании [4].

Случается, что нарушения конфиденциальности данных связаны с человеческой ошибкой. Одним из решений является регулярное интенсивное обучение сотрудников всех ролей по вопросам безопасности.

Основная проблема, связанная с угрозами, присущими удаленной работе и BYOD, заключается в том, чтобы иметь сеть, которая контекстуально осведомлена. Контекстно-осведомленная сеть – это та сеть, которая может идентифицировать источник и характер трафика – по местоположению, типу устройства и поведению, например, обычное или подозрительное. Определяя потенциальные угрозы, система может принять разумное решение о том, как реагировать.

Список используемых источников

1. Риски BYOD [Электронный ресурс]. Режим доступа: https://www.itweek.ru/security/article/detail.php?ID=174433

2. Управление мобильными устройствами [Электронный ресурс]. Режим доступа: http://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:Mobile_Device_Management_(MDM)_%D0%A3%D0%BF%D1%80%D0%B0%D0%B2%D0%BB%D0%B5%D0%BD%D0%B8%D0%B5_%D0%BC%D0%BE%D0%B1%D0%B8%D0%BB%D1%8C%D0%BD%D1%8B%D0%BC%D0%B8_%D1%83%D1%81%D1%82%D1%80%D0%BE%D0%B9%D1%81%D1%82%D0%B2%D0%B0%D0%BC%D0%B8_Enterprise_Mobility_Management_(EMM)

3. Next Gen NAC is designed to facilitate BYOD [Электронный ресурс]. Режим доступа: https://www.networkworld.com/article/2173486/security/next-gen-nac-is-designed-to-facilitate-byod.html

4. Hayes Bob, Bring Your Own Device (BYOD) to Work. M. : Gardners Books, 2013.

УДК 003.26

ПРАКТИЧЕСКОЕ ПРИМЕНЕНИЕ СЕТЕВОЙ СТЕГАНОГРАФИИ НА ПРИМЕРЕ ПРОТОКОЛА ICMP

А. В. Красов, Е. И. Степанов

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

С наступлением эры перманентной прослушки трафика на стороне государств, провайдеров и компаний передача информации по сети перестала быть незаметной. При определенном стечении обстоятельств может понадобиться канал, о существовании которого не будет известно.

стеганография, сетевая стеганография, безопасность, icmp.

На данный момент информация является одним из самых ценных ресурсов. Так, информация, попадая в неправильные руки, может повлиять на финансы, экономику, жизни людей и т. д. Обычно такую информацию стараются зашифровать и/или отправить по шифрованному каналу, что уже является сигналом для злоумышленника, что информация имеет ценность, что данная информация может быть использована в своих целях третьими лицами. Несмотря на то, что информация зашифрована, злоумышленник может расшифровать данные приложив достаточные компьютерные мощности.

Наукой, изучающей способы и методы скрытия конфиденциальных сведений, называется стеганографией [1, 2]. Задачей стеганографии является скрытие самого факта существования секретных данных при их передаче, хранении или обработке.

Сетевая стеганография – вид стеганографии, в которой, в качестве носителей стеганограмм, используются протоколы сетевой модели открытых систем – OSI. Стеганограммой являются скрываемые данные. Термин «сетевая стеганография» ввели польские ученые W. Mazurczyk и K. Szcsypiorski [3].

В общем виде сетевая стеганография является семейством методов по модификации данных в заголовках сетевых протоколов и в полях полезной нагрузки пакетов, изменению структуры передачи пакетов и гибридных методов в том или ином сетевом протоколе [4].

Прикладным применением стеганографии чаще всего является защита авторского права. В случае данной работы главным применением является отправка стеганограмм посредством ничем непримечательного протокола ICMP – протокола межсетевых управляющих сообщений. Примером может послужить отправка инсайдерской информации.

Обычно протокол ICMP используется для передачи сообщений об ошибках и исключительных ситуациях, таких как недоступность хоста, маршрутизатора, истечение времени жизни дейтаграммы, либо недоступность запрашиваемой услуги [5].

Также протокол ICMP используется для проверки доступности конечного хоста или маршрутизатора, посредством ECHO – запросов и ECHO – ответов, которые в свою очередь используются в программном обеспечении – Ping.

Типичный размер полезной нагрузки ECHO пакета – 32 байт.

Для захвата и генерации пакетов используется популярная и распространенная библиотека libpcap. Библиотека разработана в лаборатории Беркли и поддерживается до сих пор. Используется в таком программном обеспечении как tcpdump, Wireshark, Nmap, McAfee, Symantec и так далее.

Реализован метод модификации полезной нагрузки ICMP – пакета на языке программирования Java. Вместо обычного тела пакета были отправлены данные состоящие из чисел с единичным инкрементом (рис. 1).

Рис. 1. Отправка ICMP – пакета

Таким образом можно отправить любые данные, прежде поделив их.

На принимающей стороне увидеть данные можно к примеру, с помощью анализатора сетевого трафика – tcpdump (рис. 2).

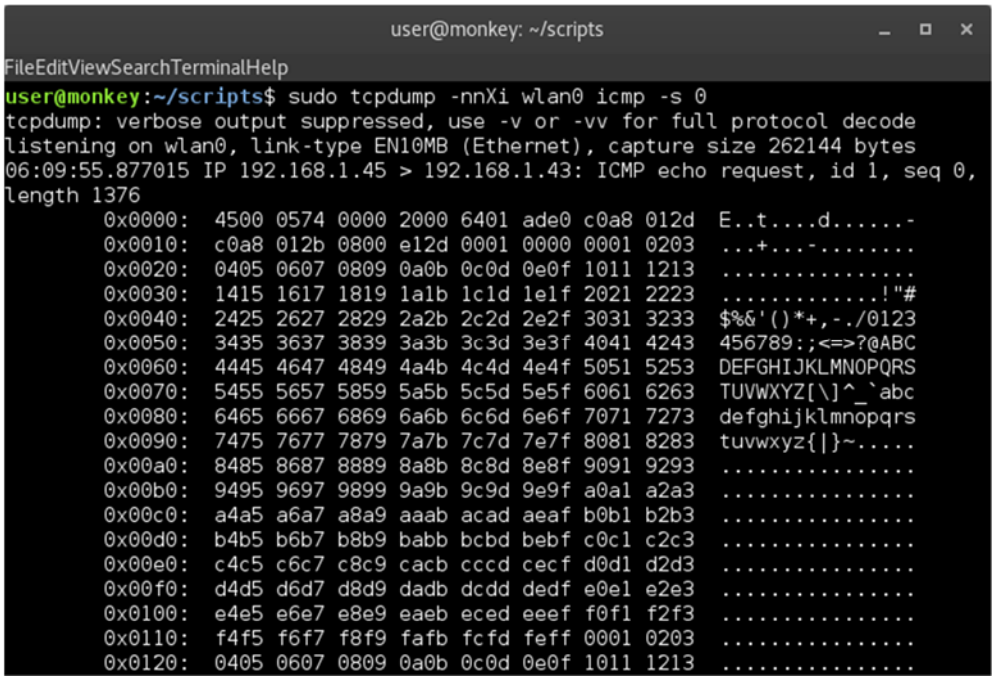


Рис. 2. Прием ICMP – пакета

Получены исходные данные, отправленные с первого хоста.

В работе был рассмотрен метод изменения полезной нагрузки ICMP – пакета для скрытой передачи через сеть. Данный метод сравнительно легко поддается статистическому анализу, который позволяет выявить данный канал связи и данные в нем. Утилита ping использует заданную полезную нагрузку, для противодействия достаточно будет сравнить принятый пакет с оригиналом.

Список используемых источников

1. Коржик В. И., Небаева К. А. Основы стеганографии : учебно-методическое пособие. Федер. агентство связи, С.-Петерб. гос. ун-т телекоммуникаций им. М. А. Бонч-Бруевича. СПб. : СПбГУТ, 2015. 20 с.

2. Коханович Г. Ф. Стеганография теория и практика. Киев. : МК-Пресс, 2006. 288 с. ISBN 966-8806-06-9

3. Пескова О. Ю., Халабурда Г. Ю. Применение сетевой стеганографии для защиты данных, передаваемых по открытым каналам Интернет // Интернет и современное общество : труды XV всерос. объединенной конф., Санкт-Петербург, 10–12 окт. 2012 г. СПб. : НИУ ИТМО, 2012. С. 348–354.

4. Mazurczyk W. Szczypiorski K. Steganography of VoIP Streams [Электронный ресурс] // On the Move to Meaningful Internet Systems : OTM Confederated International Conferences. Berlin: Springer, 2008. pp. 1001–1018. URL: https://arxiv.org/pdf/0805.2938.pdf (дата обращения 29.01.2018).

5. RFC 792. Internet Control Message Protocol [Электронный ресурс] // URL: https://tools.ietf.org/html/rfc792 (дата обращения 29.01.2018).

УДК 004.056.57

ИСПОЛЬЗОВАНИЕ И РАЗРАБОТКА МЕТОДОВ ОБНАРУЖЕНИЯ ВРЕДОНОСНОЙ АКТИВНОСТИ АВТОМАТИЗИРОВАННОГО ПОСТРОЕНИЯ БОТНЕТ-СЕТЕЙ

А. В. Красов, М. С. Сурмина

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

В данной статье изучена история возникновения, цели и архитектура построения ботнет-сетей. Изучены методы заражения конечных устройств, способы защиты от заражения, механизмы разрушения ботнет-сетей.

ботнет-сеть, сетевая стеганография, скрытые каналы, DDoS.

На сегодняшний день ботнет-сети широко распространены по всему миру. Сегодня они поставляются, как услуга. Ботнет-сеть нужна для DDoS-атаки, которая заказывается через полноценный веб-сервис. На таких сервисах можно встретить тарифы, которые могут включать сложные правительственные цели, различные источники атак (видеокамеры, сервера и т. п.), различные сценарии атаки [1] (табл.).

ТАБЛИЦА. Топ-10 худших стран с ботнетами на 31 декабря 2017 года

№	Страна	Кол-во ботов
1	Индия	1976502
2	Китай	1701210
3	Иран	814991
4	Вьетнам	719956
5	РФ	532106
6	Таиланд	521084
7	Турция	516305
8	Бразилия	466111
9	Индонезия	369709
10	Мексика	340976

В данной статье речь заходит об IRC – протокол прикладного уровня для обмена сообщениями в режиме реального времени. Разработан в основном для группового общения, также позволяет общаться через личные сообщения и обмениваться данными, в том числе файлами. Для управления каналами IRC были созданы специальные боты, т. к. администрирование каналов могло занимать много время.

Со временем боты стали использоваться с целью нанесения вреда. Использование ботов помогало скрыть инициатора атаки, т. к. ущерб был нанесен ботом, а не напрямую атакующим. С течением времени стали одновременно использовать группу ботов с различных устройств, объединяемых в ботнет. Для атаки крупных целей требовались большие сети ботов. Поэтому злоумышленники начали использовать троянские программы и другие скрытые методы, чтобы увеличить число зараженных компьютеров в сети.

Современные боты представляют собой различные гибриды угроз, интегрированных в систему управления и контроля. Они могут распространяться как черви, скрываться от операционной системы как большинство вирусов, а также включают в себя различные методы атак. Другая серьезная проблема заключается в том, что в создании современных ботов принимают участие сразу несколько человек. Таким образом, появляется несколько различных вариантов одного и того же бота, что затрудняет их распознавание антивирусными программами.

Итак, ботнет-сеть, которая состоит из некоторого количества конечных устройств, на которых установлен и запущен бот – автономное программное обеспечение. Используется чаще всего для отправки спама, брутфорсинга, DDoS-атак. Боты не являются вирусами, но они могут состоять из них вместе с программами для удаленного доступа и инструментами для скрытия

от ОС. В качестве архитектуры используются 2 модели: клиент-серверная (рис. 1) и децентрализованная (рис. 2). Первые ботнеты использовали клиент-серверную модель потому, что с ее помощью легче управлять хостами в сети.

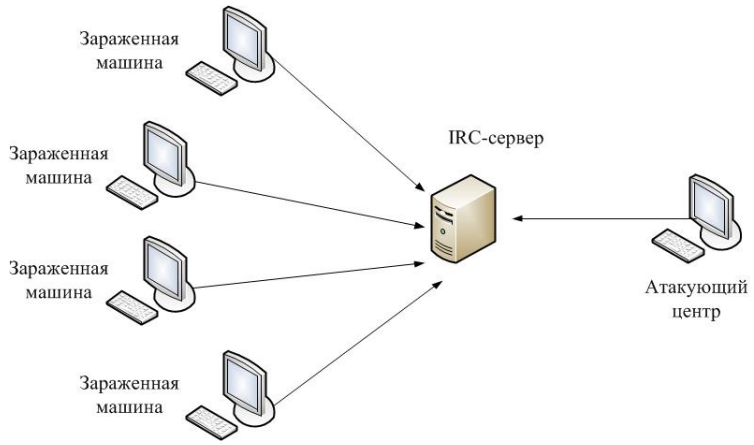


Рис. 1. Клиент-серверная модель ботнет

В централизованной сети боты подключаются к одному или нескольким серверам, а затем ждут управляющих команд от сервера. Управляющий компьютер посылает команды на серверы, а те в свою очередь отравляют их клиентам. Клиенты выполняют команды и посылают на сервер сообщение о результатах.

Такая модель имеет один существенный недостаток. В случае отказа сервера управляющий компьютер потеряет связь со своими ботами и не сможет ими управлять.

Рис. 2. Децентрализованная модель ботнет

Сегодня число одноранговых бот-сетей растёт всё больше. К примеру, в ботнет-сети "Peer-to-Peer" нет централизованного сервера, а боты подключены друг к другу и действуют одновременно как сервер и как клиент. Задачей бота является: найти другой заражённый компьютер. Логика поиска заражённого компьютера такова: бот проверяет случайные IP-адреса до тех пор, пока не свяжется с другим заражённым устройством. Найденный новый бот так же отправляет информацию о своей версии программного обеспече-

ния и список известных ему ботов. Если одна из версий ПО ниже, чем другая, то последует передача файла для обновления на более новую версию ПО. Так и получается, что каждый бот пополняет свой список заражённых машин и обновляет ПО до более свежей версии.

Одноранговые бот-сети устойчивы к динамическому оттоку узлов своей сети, то есть боты могут быстро присоединяться к сети и выходить из неё. К тому же, связь между узлами не будет нарушена в случае потери или выхода из строя нескольких ботов. В противовес централизованным сетям, ботнеты "Peer-to-Peer" представляются более надёжными и сложными для полного обнаружения. Получение управление происходит посредством установки бота. Эта установка невидимая для пользователя, обычно происходит, используя:

1. Вирусы.
2. Эксплоит-киты.
3. Фишинг.
4. Непосредственный доступ к компьютеру (редко).
5. Брутфорсинг пароля к администраторскому серверу (в ЛВС).

Наиболее частым и опасным за последнее время стал эксплоит-кит Angler. Angler помогает распространять такое ПО, как Cryptowall, AlphaCrypt, Necurs, и Bedep [2]. Потенциальная жертва перенаправляется на фишнговый сайт. В это время Anlger в фоновом режиме начинает обфускацию вредоносных скриптов. Также на этом сайте есть несколько зашифрованных строк, содержащих URL разных эксплойтов (*Flash*, *Silverlight*, *Internet Explorer*), включенных в атаку.

Второй слой обфускации используют и другие эксплойт-киты, чтобы затруднить детектирование. Кроме того, что Angler имеет способность распознавать антивирусное ПО, он умеет также определять, когда исследователь пытается выполнить его код в песочнице или на виртуальных машинах, а также через прокси-отладчик Fiddler, популярный среди аудиторов информационной безопасности [3]. Все эти механизмы самозащиты сильно затрудняют анализ Angler исследователями.

Обнаружить ботнет можно, используя:

мониторинг трафика (активный IRC-трафик, высокий исходящий SMTP);

детектирование скрытых каналов (SSH-туннели, HTTP-туннели и др.);

проверку соединений с серверами, замеченными, как узел ботнета;

отслеживание одинаковых DNS-запросов;

мониторинг нагрузки процессора.

Для обхода систем обнаружения вторжений полезная нагрузка Angler шифруется для передачи по сети жертвы и расшифровывается шелл-кодом на последней стадии передачи. Такая полезная нагрузка, как Bedep, сама

по себе опасности не представляет, но используется для загрузки других вредоносных программ.

Список используемых источников

1. The World's Worst Botnet Countries [Электронный ресурс]. Режим доступа: https://www.spamhaus.org/statistics/botnet-cc/

2. Анализ Angler – самого продвинутого эксплойт-пака [Электронный ресурс]. Режим доступа: https://threatpost.ru/analiz-angler-samogo-prodvinutogo-eksplojt-paka/6096/

3. Штеренберг С. И., Раськевич А. А., Чекалов А. А. Метод дизассемблирования вирусов, использующих руткит-технологию, для анализа статистики его внедрения в технологию адаптивной защиты // Перспективы науки. 2015. № 6 (69). С. 114–119.

УДК 004.056.53

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ JAVA ПРОГРАММ ПОСРЕДСТВОМ ВЛОЖЕНИЯ ПРОГРАММНОГО ВОДЯНОГО ЗНАКА

А. В. Красов, П. И. Шариков

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

Важное преимущество Java заключается в ее кроссплатформенности, за счет использования байт-кода. Однако, использование байт-кода позволяет производить декомпиляцию Java программ, для получения доступа к их исходному коду. Это упрощает появление пиратских копий программам Java, нарушает их авторское право. Это недостаток Java по сравнению с другими языки программирования, которые компилируют в собственный объектный код.

Создание цифровых водяных знаков программного обеспечения – относительно новый подход к проблеме защиты авторских прав, которая включает вложение информации о владении программой в саму программу. Создание водяных знаков было экстенсивно исследовано и значительные успехи были сделаны в разработке устойчивых и безопасных методов. В данной статье авторы исследуют новый метод создания цифровых водяных знаков для программного обеспечения.

Метод основан на сигнальной теории обнаружения, которая используется при создании мультимедийных цифровых водяных знаков.

java, цифровой водяной знак, водяной знак, байт-код, скрытое вложение.

Нелегальное копирование программного обеспечения – главное препятствие для более широкого использования языка программирования Java.

Возможность доказать, что вы владелец Java программы, и стали жертвой нарушения авторского права, уменьшила бы опасения использования java.

Создание цифровых водяных знаков для программного обеспечения влечет за собой изменение программы, посредством вложения в нее информацию о авторском праве [1]. В данной статье авторы описывают создание цифровых водяных знаков в программном обеспечении, с помощью сигнальной теории обнаружения.

Водяной знак должен быть устойчивым против преднамеренной попытки удалить его [2]. Эффективность цифрового водяного знака может быть описана в трех пунктах:

– Устойчивость. Возможность цифрового водяного знака быть устойчивым к атакам направленных на его преобразование с целью нарушения. Преобразование, оптимизация, перекомпиляция, декомпиляция, обфускация кода. Не должно быть возможности отделить цифровой водяной знак от class-файла java.

– Объем. Допустимый объем вложения в программное обеспечение.

– Видимость. Пользователь программного обеспечения не должен знать, что в программном обеспечении вложен цифровой водяной знак. Также, вложение помимо скрытности не должно влиять на работоспособность программы, ее отображение, скорость исполнения.

Создание цифровых водяных знаков для программного обеспечения отличается от создания цифровых водяных знаков в мультимедиа тем, что водяной знак должен быт встроен в исполняемый файл, а не в пассивные данные, такие как изображение или аудиофайл [3]. Существенная трудность защиты авторских в цифровых данных – это невозможность предотвращения копирования цифровых данных. Исходный код программного обеспечения нельзя защитить от копирования, но можно вложить цифровой водяной знак, который будет являться гарантией того, что исходный код программного обеспечения и авторские права на него принадлежат вам.

Методы, применяемые для создания цифровых водяных знаков для программного обеспечения можно разделить на два типа, статические и динамические.

Статические цифровые водяные знаки. Данные знаки помещены в код или данные программного обеспечения. Они скрывают цифровой водяной знак в избыточной области программы. Этот тип похож на вложение водяных знаков в избыточных областях мультимедиа. Производится вложение цифрового водяного знака в инструкции кода исполняемого файла. Статические цифровые водяные знаки не устойчивы к таким атакам, как оптимизация или обфускация кода.

Динамические цифровые водяные знаки. Динамические цифровые водяные знаки в структурах создаваемых рабочей программой [4]. Они скрывают водяной знак в избыточных вычислениях программы. Динамические

водяные знаки сгенерированы программой во время ее выполнения, обычно на определенной входной последовательности.

Сигнальная теория обнаружения для создания цифровых водяных знаков в программном обеспечении. Если создание цифровых водяных знаков для программного обеспечения может быть смоделировано как сигнальная проблема обнаружения, тогда знание, полученное от этого исследования, может быть применено к программному обеспечению для создания цифровых водяных знаков [5].

Мультимедийный контент цифрового водяного знака может быть представлен, как сигналы в пространстве и времени. Производится моделирование слабого сигнала на основе оригинального сигнала и сводится в единый файл мультимедиа. Обнаружить такое вложение достаточно проблематично даже после сигнальных преобразований. Также популярен метод широкополосного водяного знака на основе непостоянных инструкций.

Широкополосное создание цифровых водяных знаков требует, чтобы некоторый вектор r был извлекаемым. Предлагаемый подход должен извлечь этот вектор из свойств рабочей программы. Один из простых способов сделать данную операцию заключается в том, чтобы измерить глубину графа вызовов в различных точках во время выполнения программы на каком-то определенном вводе.

Как один из примеров изменения работы программы во время ее выполнения показано в листинге.

```
func1(int a, int b) {
 if(depth == 0) {
      depth++;
      func1(a,b);
 }
  else {
      /* оригинальный метод */
  }
/* декларация переменной */
private static depth = 0;
```

Листинг. Выполнение функции после ее фиктивного блока

Таким образом, возможно, определить количество вызовов данного фиктивного метода, чтобы скорректировать цифровой водяной знак в программе. В конце выполнения программы проверяем количество вызовов каждого метода, в особенности методов, которые учитываются при создании цифрового водяного знака. Далее необходимо составить граф вызовов и преобразовать его для получения цифрового водяного знака.

Также, динамичность данного метода заключается в том, что авторы могут для проверки цифрового водяного знака задать несколько «глубин графов» на случаи некоторого редактирования исходного кода программы (следовательно, и количества вызовов специальных методов) злоумышленниками, с целью изменить оригинал и выдать за свою разработку.

Вывод. Создание и вложение цифровых водяных знаков – важная технология, позволяющая защитить свои авторские права на исходный код программы. Данная статья обеспечила введение для создания цифровых водяных знаков в программном обеспечении динамическими методами на основе сигнальной теории обнаружения.

Список используемых источников

1. Шариков П. И. Методика нахождение величины наиболее выгодного контейнера в форматах исполняемых файлов // Наукоемкие технологии в космических исследованиях Земли. 2015. Т. 7. № 5. С. 58–62.

2. Коржик В. И., Небаева К. А., Герлинг Е. Ю., Догиль П. С., Федянин И.А. Цифровая стеганография и цифровые водяные знаки / Под общей редакцией профессора В. И. Коржика. СПб. : СПбГУТ. 2016. 226 с.

3. Шариков П. И., Красов А. В., Штеренберг С. И. Методика создания и вложения цифрового водяного знака в исполняемые java файлы на основе замен опкодов // T-Comm: Телекоммуникации и транспорт. 2017. Т. 11. № 3. С. 66–70.

4. Хомяков И. Н., Красов А. В. Возможность скрытого вложения информации в байт-код java // Информационные технологии моделирования и управления. 2014. № 2 (86). С. 185–191.

5. Красов А. В., Шариков П. И. Методика защиты байт-кода java-программы от декомпиляции и хищения исходного кода злоумышленником // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2017. № 1. С. 47–50.

УДК 004.056

АНАЛИЗ АКТИВНЫХ СЕТЕВЫХ АТАК: ARP-SPOOFING и DNS-SPOOFING

А. В. Красов, И. Р. Ягудин

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

В статье рассматриваются наиболее распространённые виды активных сетевых атак, при реализации которых применяется перехват трафика между узлами и подмена сетевого адреса. Также, предложены различные методы защиты от определённых типов сетевых атак.

активная сетевая атака, злоумышленник, подмен сетевого трафика, перенаправления трафика, локальная сеть.

В настоящее время в мире существует огромное количество сетевых атак. В данной статье рассмотрены две сетевые атаки разновидностей атак MITM (англ. *Man in the middle* – человек посередине); ARP (англ. *Address Resolution Protocol* – протокол разрешения адреса) spoofing, DNS (англ. *Domain Name System* – система доменных имен) spoofing и рассматриваются возможности реализации их с использованием программного обеспечения. Обычно, для таких атак часто требуется использовать специализированное программное обеспечение. Как правило, все удалённые атаки, которые известны в нашем мире являются активными. Активные сетевые атаки оказывают непосредственное влияние на работу системы, то есть требуют от злоумышленника какие-то активные действия для того что бы попытаться нарушить принятую в системе политику безопасности. Они являются детектируемыми.

ARP-spoofing. На канальном уровне используются MAC- (от англ. *Media Access Control* – управление доступом к среде) адреса, на сетевом уровне TCP/IP(от англ. Transmission Control Protocol- протокол управления передачей)/(Internet Protocol – «межсетевой протокол») используются IP-адреса, так как для вычислительной техники IP-адрес – это набор байт, поэтому машине в локальной сети передают данные через MAC-адреса, который находится на канальном уровне, чтобы сопоставлять IP-адреса к MAC-адресам есть специальный протокол ARP (*Address Resolution Protocol* – протокол разрешения адреса) протокол позволяет сопоставить IP-адреса к адресам канального уровня. Протокол проектировался в 1992 г. и не предполагал механизмы защиты. Рассмотрим работу протокола. В нашей сети имеются 2 компьютера со следующими характеристиками: компьютер А с IP-адресом напр. (10.55.55.2) и компьютер Б с IP-адресом напр. (10.55.55.3). Они соединены между собой сетью Ethernet. Компьютер А, отправляет пакет компьютеру Б у которого есть существующий IP-адрес, однако сеть Ethernet не работает с IP-адресам, а MAC-адрес ему неизвестен. Для этого он использует протокол ARP, он посылает широковещательный запрос всем компьютерам в локальной сети с таким сообщением «Компьютер с таким напр. (10.55.55.3) IP-адресам сообщите свой MAC-адрес компьютеру, у которого такой MAC-адрес напр. (64:63:80:C9:64: F7)». Этот запрос доставляется всем устройствам в сети. Компьютер Б в ответ присылает компьютеру А свой MAC-адрес, в свою очередь они могут теперь пересылать данные [1]. Для того что бы не делать запрос каждый раз, MAC-адрес заносится в ARP таблицу. Рассмотрим Атаку «ARP-spoofing». Анализ безопасности протокола ARP показывает, что если перехватить на атакующем

хосте данного сегмента, широковещательный ARP запрос, то можно подменить ARP-ответ, тем самым объявить себя искомым хостом, и трафик будет идти через нас. Рассмотрим такую ситуацию, что злоумышленник, находясь в одной локальной сети с пользователем и ожидая его ARP запрос, то есть трафик, который злоумышленник хочет контролировать. Когда злоумышленник видит ARP запрос он старается ответить на этот запрос ложным ARP ответом, то есть подменить MAC-адрес хоста, который запрашивал пользователь, после этого узел, который будет атакован занесет в свою ARP-таблицу ложный Mac- адрес и будет слать пакеты злоумышленнику. Такую атаку производят, как и на пользователя так и на маршрутизатор [2].

На рис. показана схема контроля всего трафик атакуемого, атаки идут сразу на два узла на маршрутизатор и на атакуемый хост путем посылки ложных ARP ответов на ARP запросы которых как правило даже и не было. Рассмотрим пример реализации атаки в операционной системе «Kali linux». Для реализации атаки используются специализированные программы. В основном написанные злоумышленниками. Для начала нужно проверить работает операционная система в режиме маршрутизатора. Для того что бы это проверить используется следующая команда: «Sysctl net. ipv4.ip_forward». Если в ответ будет равен «0» это говорит о том, что режим выключен. Для включения используем эту команду «Sysctl – w net. ipv4.ip_forward=1». Для проведения атаки ARP-spoof есть специальный инструменты, их много рассмотрим некоторые из них. Рассмотрим программу «Arpspoof» в консоли вводим «arpspoof *–i* eth0 *–t* [ip жертвы] *–r* [ip как правило маршрутизатора]», где *–i* – указывает интерфейс, *–t* – указывает IP-адрес хоста, *–r* – указывает arpspoof «отравлять» arp-кэш обеих хостов. После этой команды посылаются ARP-пакеты на маршрутизатор в которых подменяются MAC адреса. В итоге мы получаем трафик чужого узла. Для просмотра пакетов можно использовать программу «wireshark». Неудобства утилиты «arpspoofing» в том, что программа умеет одновременно производить атаку только для двух хостов, для того чтобы производить атаку на несколько хостов надо открывать новый терминал и это неудобно. Рассмотрим другую программу под названием «Ettercap» [3]. Очень мощное средство для проведения атак типа Man-in-the-Middle. Есть два интерфейса: консольный и графический. Поддержка плагинов, фильтров. Поддержка разных типов атак. Реализация в консоли, прописываем «Ettercap *–I* eth0 *–T –q –M* ARP /192.168.1.1// /192.168.1.36//», где *–i* использовать этот сетевой интерфейс, *–T* использовать только текстовый интерфейс, *–q* не показывать содержимое

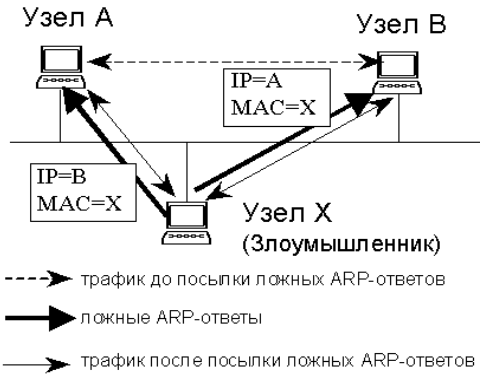


Рисунок. Атака на два узла

пакетов. *–M* выполнить атаку mitm. Другой вариант атаки «Ettercap *–I* eth0 *–T –q –M* ARP /192.168.1.1// ///» атака будет производиться по всей подсети, злоумышленник будет перехватывать трафик во всей подсети в которой он находится. В программе имеются очень полезные плагины. Рассмотрим плагин под названием «autoadd – автоматическое добавление новых жертв по мере их подключения к ARP». По умолчания утилита поддерживает 33 плагина, но это не предел так же можно написать свой плагин. Пример использования плагина. «Ettercap *–I* eth0 *–T –q –P* autoadd –M ARP /192.168.1.1// ///», где *–P* – запустить этот плагин. После того как мы запускаем атаку Ettercap сканирует все узлы, которые доступны и начинает их подменять, и если после некоторого времени появляется новый узел, то с этим плагином он будет добавлен в список к остальным узлам для подмены [4]. В программе также присутствуют так называемые «Фильтры». Фильтры нужны что бы; отсеивать только тот трафик, который нужен и в реальном времени вмешиваться в трафик (напр. Изменение картинок в веб страницы, понижение версии протокола такого как SSH (англ. *Secure Shell* – «безопасная оболочка»).

Защита от атаки ARP-spoofing. Рассмотрим два способа защиты от такого рода атак; введение статистической ARP таблицы и программно-аппаратный. Первый способ является одним из надежных решений по защите от ARP-spoofing. Заключается в введение статической ARP-таблицы. Задача очень трудная так как надо знать все узлы, IP-адреса и сопоставлять IP-адреса к MAC-адресам. Очень кропотливая работа, которая требует много времени, усилий и затрат. Так же надо отключиться динамическую поддержку ARP таблиц на ключевых узлах. Если говорить о программном способе, то это программа «arpwatch» единственная в своем роде которая позволяет наблюдать за такими атаками, обычно ставится на ключевые узлы напр. сервер. Существует и программно-аппаратный комплекс «Система обнаружения вторжений(СОВ) (англ. *Intrusion detection system*, IDS)» и «Система предотвращения вторжений (англ. *Intrusion Prevention System*, IPS)». Обычно ставится на критичные сегменты сети который выявляет атаки на сеть в том числе ARP-spoofing атаки. Различия IDS от IPS. IDS занимается только обнаружением атак, а IPS это более интеллектуальная система, она обнаруживает атаки и защищает от них. Атака детектируется, достаточно посмотреть в ARP таблицу и увидеть несоответствия [5].

DNS-spoofing. DNS-алгоритм удаленного поиска IP-адреса по имени в сети Internet. Хост посылает на IP-адрес ближайшего DNS-сервера (он, как правило, устанавливается при настройке сетевой ОС) DNS-запрос, в котором указывает имя сервера, IP-адрес которого необходимо найти. DNS-сервер, получив такое сообщение, ищет в своей базе «имен» указанное имя. Если указанное в запросе имя найдено, а, следовательно, найден и соответ-

ствующий ему IP-адрес, то DNS-сервер отправляет на хост DNS-ответ, в котором указывает искомый IP-адрес. Если же DNS-сервер не обнаружил такого имени в своей базе имен, то он пересылает DNS-запрос на один из ответственных за домены верхнего уровня DNS-серверов, адреса которых содержатся в файле настроек DNS-сервера, и описанная в этом пункте процедура повторяется, пока имя не будет найдено (или будет не найдено) [6]. Существует 3 варианта удалённой атаки на DNS. Перехват DNS-запроса, направленный шторм ложных DNS-ответов на атакуемый хост, перехват DNS-запроса или создание направленного шторма ложных DNS-ответов на DNS-сервер. Рассмотрим перехват DNS запросов. Сначала злоумышленник ожидает DNS-запрос после получения запроса задача злоумышленника ответить на этот запрос где указать вместо реального IP-адреса хост ложного DNS-сервера (может быть узел атакующего, другой узел сети, несуществующий узел (чем может повлечь за собой ту самую «DOS (от англ. *Denial of Service* – отказ в обслуживании) – атаку»)). Таким образом для атакующего хоста ложный DNS-сервер выглядит как настоящий сервер. Необходимые условия для проведения данной атаки; возможность перехвата DNS-запроса, знать с какого порта был послан запрос, transaction ID (идентификатор в заголовке DNS ответов). Рассмотрим пример атаки DNS-spoofing [7]. Пользователь хочет попасть на сайт банка, в котором он обслуживается. Для этого в поисковой системе браузера он вводит наименования банка. После этого браузер пользователя посылает запрос на DNS-сервер: «на каком IP-адресе находится банк». В ответ на запрос DNS-сервер определяет на каком IP-адресе находится банк. В результате этого пользователь заходит на сайт и производит необходимые действия с банком: перевод средств, оплата счетов и т. д. Представим ситуацию что пользователь находитесь в кафе, в котором существует открытая точка WI-FI-сети. В одном кафе с пользователем сидит злоумышленник, и он организовал на него ARP-spoofing атаку и сделал ему подмену DNS. Он заходите 6на банк, которым пользуется, браузер отправляет запрос DNS-серверу «какой IP-адрес у банка» в ответ приходит IP-адрес, где злоумышленник уже развернул точную копию банка. Таким образом пользователь считает, что он находится на сайте банка, а в действительности сайт банка подменен и злоумышленник имеет возможность завладеть персональными данными пользователя и использовать по своему назначению. Рассмотрим реализацию в Kali linux: пример реализации с помощью утилита «dnsspoof» которая подменяет IP-адрес узла на свой. Для реализации атаки надо сначала произвести атаку ARP-spoofing. Также должен быть запущен сервер, например, «Apache HTTP-сервер». При попытке перейти на любой сайт, пользователь будем перенаправлены на «Apache HTTP-сервер». Для удобства реализации атаки есть файл где мы можем указать IP-адрес и доменное имя какое нужно подменить, для того что бы перенаправлять только определённые сайты.

Для начала атаки необходимо в консоли написать «dnsspoof» и атака запустится. Так же DNS-spoof можно реализовать в Ettercap с помощью плагина «dns_spoof». Рассмотрим второй вариант удаленной атаки «Шторм ложных DNS-ответов». Постоянная передача злоумышленником ложных DNS-ответов на различные UDP-запросы атакуемого хоста и с различными ID от имени (с IP-адреса) и будет происходить подмена настоящего IP-адреса на ложный, которым будет являться IP-адрес ложного сервера – хоста атакующего. Как говорилось ранее есть определенные требования к такому виду атаки, нужно направлять ответы на тот же порт с которого был отправлен запрос и знать transaction ID. Рассмотрим третий вариант «перехват DNS-запроса или создание направленного шторма ложных DNS-ответов на DNS-сервер» [8]. В этом варианте объедены первый и второй случай, атака может реализоваться не только когда мы находимся в клиентской сети, а, например, между двумя DNS-серверами. Когда пользователь обращается к DNS-серверу, а он не знает где находится IP-адрес сайта, то он обращается к другому DNS-серверу. Тут злоумышленник может перехватить DNS-запрос и ответить, подменив IP-адрес или также организовать шторм ложных DNS-ответов. DNS-сервер отправляет запрос другому DNS-серверу с 53 порта. Злоумышленнику заранее известен порт отправителя, ему только остается перебрать transaction ID [9].

Защита от атаки DNS-spoofing. Если злоумышленник находится в локальной сети жертвы, то защититься от такой атаки очень тяжело. Так как нужно знать реальный IP-адрес сайтов.

Заключение. Таким образом в статье проведён анализ возможностей реализации сетевых атак. Рассмотрены примеры активных сетевых атак, а также методы защиты от них. В заключении стоит отметить что сетевые атаки реализуются достаточно просто, а защита от них не всегда представляется возможным. Результаты проведенного анализа могут быть полезны как для рядовых пользователей, так и для специалистов информационной безопасности.

Список используемых источников

1. Кунегина С. В. Обеспечение информационной безопасности в сетях IP [Электронный ресурс]. URL: http://kunegin.com/ref3/ip-sec/remote1.htm (дата обращения: 22.09.2017).

2. Медведовский И. Д., Семьянов П. В., Леонов Д. Г. Атака на Internet [Электронный ресурс]. Изд. ДМК, 1999. 425 с. fb2.

3. Алейников А. А., Билятдинов К. З., Красов А. В., Кривчун Е. А., Крысанов А. В. Технические аспекты управления с использованием сети интернет: монография. СПб. : Центр «Астерион», 2016. 305 с. ISBN 978-5-00045-408-4.

4. Красов А. В., Левин М. В., Штеренберг С. И., Исаченков П. А. Модель управления потоками трафика в программно-определяемой сети с изменяющейся нагрузкой // Наукоемкие технологии в космических исследованиях Земли. 2016. Т. 8. № 4. С. 70–74.

5. Красов А. В., Сахаров Д. В., Ушаков И. А., Лосин Е. П. Обеспечения безопасности передачи MULTICAST-трафика в IP-сетях // Защита информации. Инсайд. 2017. № 3 (75). С. 34–42.

6. Красов А. В., Левин М. В. Возможности управления трафиком в рамках концепции SDN // Актуальные проблемы инфотелекоммуникаций в науке и образовании. IV Международная научно-техническая и научно-методическая конференция: в 2-х т. СПб. : СПбГУТ, 2015. С. 350–354.

7. Красов А. В., Левин М. В., Штеренберг С. И., Исаченков П. А. 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.

8. Красов А. В., Левин М. В., Цветков А. Ю. Управления сетями передачи данных с изменяющейся нагрузкой // Всероссийская научная конференция по проблемам управления в технических системах. 2015. № 1. С. 141–146.

9. Алейников А. А., Билятдинов К. З., Красов А. В., Левин М. В. Контроль измерение и интеллектуальное управление трафиком: монография. СПб. : Центр «Астерион», 2016. 92 с. ISBN 978-5-00045-385-8.

УДК 004.715

ИСПОЛЬЗОВАНИЕ КОДА DSCP ДЛЯ ВЫДЕЛЕНИЯ ВЫСОКОПРИОРИТЕТНОГО ТРАФИКА

А. В. Курмазов, Н. Е. Турков, Д. О. Федосеев

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

Приоритезация трафика – это функция определенных моделей маршрутизаторов доступа, которая анализирует проходящий трафик и определяет в нем пакеты IP-телефонии, после чего дает именно таким пакетам максимальный приоритет для обеспечения гарантированной ширины полосы пропускания сети. Данный механизм позволяет повысить качество услуг реального времени, особенно в условиях «узкого» канала.

Использование кода DSCP является наиболее удобным и практичным способом приоритезации, что подтверждается в данной статье.

приоритет трафика, маршрутизаторы, код DSCP, качество обслуживания.

В современном мире в стационарных сетях услуги связи предоставляются на основе IP технологии. В различных структурах и ведомствах, где необходимо непрерывно предоставлять доступ к услугам связи должностным лицам, также используют IP технологии, за счет их возможностей. К таким услугам в первую очередь относят услуги реального времени: телефонная связь, видео и видеоконференцсвязь, факсимильная связь, услуги

передачи данных (электронная почта, файлообменники и мн.др.). Но, введу наличия мало развитой транспортной сети или аренды ее, появляются проблемы с ограниченностью пропускной способности, что не позволяет некоторым видам услуг работать с необходимым качеством (услуги реального времени).

В реальном режиме работы узлов связи, возникает ситуация превышения объема информации, формируемом при передаче над пропускной способностью доступной транспортной сети, при этом из-за возникающих перегрузок требования к качеству предоставления услуг перестают выполняться для всех услуг, и если для услуг передачи данных это не внесет особых проблем, то на услугах реального времени скажется существенным образом. Существуют разные варианты решения вышеуказанной проблемы, но наиболее приоритетным среди них выглядит использование приоритезации трафика с помощью кода DSCP [1].

Приоритезация трафика (QoS – *Quality of Service*) – это функция определенных моделей маршрутизаторов доступа, которая анализирует проходящий трафик и определяет в нем пакеты *IP*-телефонии, после чего дает именно таким пакетам максимальный приоритет для обеспечения гарантированной ширины полосы пропускания сети. Данный механизм позволяет повысить качество услуг реального времени, особенно в условиях «узкого» канала. Недостатком TCP/IP является отсутствие возможности гарантировать определенное качество сервиса (*Quality of Service* – QoS). Под QoS понимается возможность гарантировать определенные сервисы и ограничить полосу пропускания как для определенных сервисов, так и для определенных пользователей. Для крупных сетей были разработаны такие решения, как архитектура дифференцированного обслуживания – Differentiated Services (*Diffserv*), которые используют информацию в заголовках пакетов.

Единственная возможность — влиять на сами потоки данных, замедляя их до того, как в сети наступит перегрузка. Поэтому задачей маршрутизатора становится слежение за всеми сессиями проходящего трафика, определение того, какой трафик является низкоприоритетным и «подтормаживание» его за счет выборочного удаления пакетов, что приводит к замедлению передачи отправителем. NetDefendOS обеспечивает QoS, позволяя администратору указывать приоритеты для сервисов и обеспечивать гарантии полосы пропускания. Этот подход называется шейпингом трафика (*traffic shaping*) и идеально подходит для управления полосой пропускания в локальной сети, а также для управления трафиком в «узких» местах, которые могут образоваться в крупных сетях. При выполнении шейпинга выполняется сравнение значений определенных полей IP-заголовка с параметрами, указанными в конфигурации, и постановка IP-пакетов в очередь в соответствии с этими значениями. Шейпинг реализован с помощью следующих механизмов:

Приоритезация трафика в соответствии с конфигурационными параметрами, указанными администратором. Если количество трафика с более высоким приоритетом увеличивается, и канал перегружен, то трафик с более низким приоритетом может быть временно ограничен, чтобы обеспечить прохождение трафика с более высоким приоритетом.

Определенному количеству трафика присваивается максимальный приоритет. Остальному трафику, который превышает это количество, назначается такой же приоритет, как и любому другому трафику.

Обычно шейпинг трафика не ставит в очередь большое количество данных с последующей отсортировкой приоритетного трафика для его отправки перед неприоритетным. Вместо этого подсчитывается количество приоритетного трафика, а неприоритетный трафик ограничивается динамически таким образом, чтобы не препятствовать прохождению приоритетного трафика.

Ограничение скорости передачи данных может быть выполнено двумя способами (рис. 1): 1) Отбрасываются все пакеты, превышающие лимит скорости передачи (шейпер); 2) Задержка превысивших заданное ограничение скорости передачи пакетов в очереди и отправка их позже, как только появляется такая возможность, т. е. выравнивание скорости передачи (шедулер).

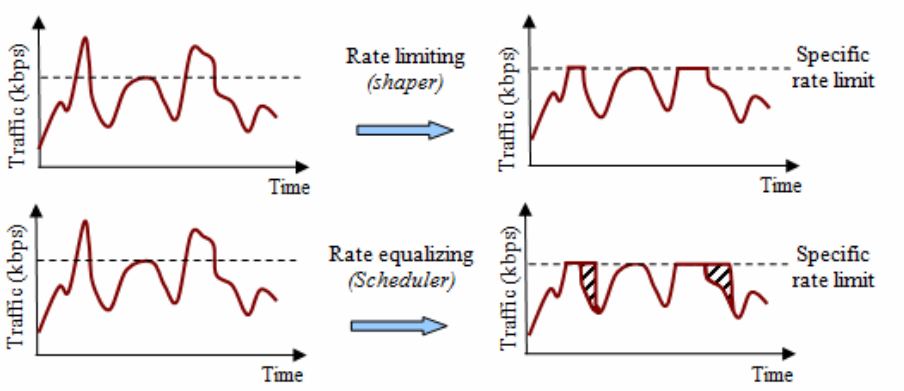


Рис. 1. Ограничение способов передачи методами Shaper и Scheduler

Как видно на иллюстрации, шейпер режет всё, что не влезло, а шедулер просто притормаживает. Соответственно, именно шедулер является более гибким механизмом. После чего каждому виду трафика присваивается свой приоритет. Первый класс обслуживается в первую очередь, последний – в последнюю.

Самый простой вариант такого решения, который зачастую и используется – просто пустить приоритетом VoIP-трафик, а весь остальной по остаточному, к примеру:

1: DNS, ICMP, ACK – в первую очередь идёт служебный трафик.

2: SIP – VoIP очень любит минимальные задержки.

3: SSH – удалённый доступ важен для работы.

4: RDP и HTTP/HTTPS – веб, видео и т. п.

5: всё, что не опознано выше.

Всем пакетам, которые проходят через каналы шейпинга трафика, присваивается определенный Приоритет (*Precedence*). С помощью приоритетов указывается как общая пропускная способность канала, так и гарантированная полоса пропускания для каждого приоритета.

Использование DSCP-битов является механизмом для установки приоритетов, приоритет пакетов определяется значением DSCP-битов в пакете [2]. DSCP является элементом архитектуры Diffserv, а биты Type of Service (ToS) являются частью заголовка IP-пакета. Существует маркировка на канальном и сетевом уровнях.

Маркировка на канальном уровне: 1) Class of Service (COS) – поле в 3 бита, позволяющее маркировать ваш трафик 8-ю различными способами; 2) Frame Relay Discard Eligible (DE) bit – поле в один бит. В случае затора трафик, с установленным битом в поле DE, первый в списке на отсечение; 3) ATM Cell Loss Priority (CLP) bit – та же концепция, что и выше; 4) MPLS EXP (*experimental*) / TC *(traffic class*) bits.

Маркировка на сетевом уровне: 1) IP Precedence (IPP) – значение, использующее первые 3 бита поля Type of Service (ToS) в заголовке пакета, позволяющее установить одно из значений от 0 до 7, где 0 наименее важный трафик, а 7 наиболее важный. Значения 6 и 7 зарезервированы и предназначены для протоколов маршрутизации и сигнализации (таких на BFD). Данные в IPP могут быть загружены из поля CoS.

2) Differential Service Code Point (DSCP) использует все 8 бит поля ToS, которое было переименовано в DS – Differential Services (Рис.2). DSCP имеет обратную совместимость с IPP благодаря первым 3 битам [3]. Достигается она следующим образом: устройства, не подразумевающие о DSCP продолжают доверять IPP битам, а более современные девайсы в состоянии понять, что в внутри класса с precedence 2 могут существовать вложенные классы с разной степенью важности.

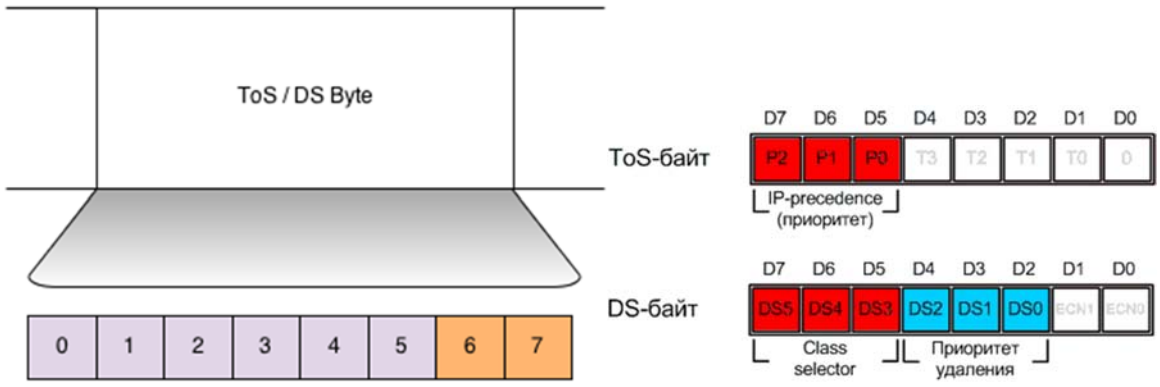


Рис. 2 Значение полей ToS / DS Byte

Когда используют терминологию ToS, то в контексте приоретизации имеют в виду 3 старшие бита P2..P0, кодирующие уровень приоритета от 0 (минимальный приоритет) до 7 (максимальный приоритет). Для IP-телефонии применяется уровень приоритета 5 (*critical*, ToS-байт равен 0×A0 или 10100000b), а для обычного трафика уровень 0 (*routine*, ToS-байт равен 0×00 или 00000000b). У Cisco есть для каждого уровня приоритета специальное имя (*precedence critical*, *precedence flash* и т. д., см. таблицу).

Когда используют терминологию DSCP, имеются в виду 6 старших бит DS5..DS0, где DS5..DS3 кодируют уровень класса обслуживания от 0 (минимальный приоритет) до 7 (максимальный приоритет) и приоритет удаления (от 0, когда приоритет удаления максимальный, до 7, когда приоритет удаления минимальный – кодирование приоритета удаления «обратное»). В итоге получается число от 0 до 63, кодирующее приоритет (чем больше число, тем трафик важнее). Такое многоуровневое кодирование приоритета часто оказывается избыточным, и поэтому используются только биты DS5..DS3. При IP-телефонии применяется класс сервиса 5 (DS-байт равен 0xA0 или 10100000b), а для обычного трафика класс сервиса 0 (DS-байт равен 0x00 или 00000000b). Сравните с ToS – изменилась только терминология, а значение байта передается то же самое.

Биты с 0 по 5 используются для DSCP, а последние два для Explicit Congestion Notification (рис. 3).

Уровень	Имя
0	routine
1	priority
2	immediate
3	flash
4	flash-override
5	critical
6	internet
7	network

IPP	DSCP Type	DSCP Binary
0	CS0/DF	000 000
1	CS1	001 000
	AF11	001 010
	AF12	001 100
	AF13	001 110
2	CS2	010 000
	AF21	010 010
	AF22	010 100
	AF23	010 110
3	CS3	011 000
	AF31	011 010
	AF32	011 100
	AF33	011 110
4	CS4	100 000
	AF41	100 010
	AF42	100 100
	AF43	100 110
5	CS5	101 000
	EF	101 110

Рис. 3 Таблицы приоритезации IPP

Научно-техническое предложения по реализации механизмов приоритизации трафика в инфокоммуникационной сети позволяют устранить ряд нерешенных научно-прикладных задач. В рамках работы был создан опытный стенд инфокоммуникационной сети для контроля, оценки и тестирования качества предоставления услуг в инфокоммуникационной сети объединения с учетом используемых механизмов приоритизации трафика.

Список используемых источников

1. Cisco QoS – классификация и маркировка [Электронный ресурс]. Режим доступа: http://twistedminds.ru/2013/02/cisco-qos-classifying-and-marking/

2. Битнер В. И., Попов Г. Н. Нормирование качества телекоммуникационных услуг: учебное пособие. М. : Горячая линия-Телеком, 2004. 312 с.

3. Ершов В. А., Кузнецов Н. А. Мультисервисные телекоммуникационные сети. М. : МГТУ им. Н. Э. Баумана, 2003. 432 с.

УДК 004.056.53

МЕТОД ПОДТВЕРЖДЕНИЯ ПОДЛИННОСТИ БАНКОВСКИХ ПЛАТЕЖНЫХ КАРТ И БАНКОВСКИХ ТЕРМИНАЛОВ С ИСПОЛЬЗОВАНИЕМ КВАНТОВОЙ КРИПТОГРАФИИ

Д. В. Кушнир, М. В. Павлюкович

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

Банковские платежные карты представляют альтернативу наличному денежному обращению. Увеличивается количество как банковских карт, так и банковских терминалов, в связи с чем возникает необходимость надежной защиты подобных систем, способных сочетать возможность аутентификации как карты, так и банковского терминала. В работе приводится пример работы квантовой метки, различные преимущества и недостатки подобного внедрения.

квантовая криптография, безопасность банковских карт, квантовая метка.

В последние десятилетия, и особенно с 2008 г. наблюдается тенденция на увеличение объема использования электронных платежных карт, эмитированных кредитными организациями. В июле 2017 г. их количество достигло почти 260 000 тыс. единиц [1]. Данная статистика обусловлена повышением интереса к использованию безналичного расчета.

Несмотря на то, что в товарно-денежном обращении в России до сих пор преобладает использование наличных денежных средств [2], безналичный расчет всегда является перспективной альтернативой. Для физических лиц безналичный расчет в большинстве случаев предполагает использование электронных платежных карт. С учетом развития технологий выделяют следующие преимущества платежных карт [3]:

1. Устойчивость к фальшифомонетничеству – большинство атак направлены не на подделку или кражу карты как таковой, а на копирование информации или способа доступа.

2. Долговечность – передовые технологии позволяют изготовить карты достаточно износостойкими, нежели бумажные купюры. Необходимость замены карты каждые несколько лет обусловлена не качеством корпуса.

3. Универсальность – при безналичном расчете отпадает необходимость учета, например, географического признака денежной единицы. Это происходит автоматически.

4. Верифицируемость – плательщика возможно отследить.

Электронные платежные карты существуют двух типов [4] – кредитные и дебетовые, среди которых выделяют технологии: с магнитной полосой, с чипом (в т. ч. для бесконтактной оплаты) и комбинированные. В России отдается предпочтение картам с комбинированной технологией, включающей магнитную полосу и чип. На сегодняшний день более защищенной является карта с чипом за счет сложности перехвата сообщений аутентификации карты. Целостность магнитной полосы надежно защищается дополнительным кодом аутентификации, но прочитанные данные с карты терминал передает через банк-эквайер в банк-эмитент, статические данные для банка-эмитента не меняются на протяжении всего срока службы карты, за счет этого недостатка, магнитные полосы наиболее подвержены скимингу, т. е. копированию данных карты. Чип на карте представляет из себя микропроцессор, благодаря этому, для каждой транзакции формируется ключ для шифрования статических данных, причем банк-эквайер не расшифровывает статические данные, а считывает лишь поле от обслуживаемого терминала и пересылает пакет дальше до банка-эмитента. Карты с чипом являются популярной мишенью для фрода, популярным видом мошенничества в сфере информационных технологий, допускающим неправомерные действия с информационными ресурсами в сетях связи. Распространен данный способ в Интернет-сети, когда пользователь собственноручно вводит данные карты на сайте, принадлежащем злоумышленнику, который впоследствии, например, совершает несанкционированные платежи. Фальшивые терминалы и неразрешенные дополнения легальных терминалов, направленные на незаконное овладевание конфиденциальной информацией пользователя, также способствуют продвижению фрода.

Для улучшения безопасности платежной карты предлагается использовать квантовые метки [5], безопасность которых основана на принципах квантовой криптографии. Подразумевается, что квантовая метка крепится к переносному информационному объекту, например, к банковской платежной карте. Под квантовой меткой понимается, например, совокупность фотонов с определенными состояниями поляризации, для правильного считывания которой требуется знать способ их измерения. Данные, записанные в виде квантовой метки, связаны с номером банковской платежной карты и хранятся в банке-эмитенте. Банк-экваер обращается к банку-эмитенту [6] для уточнения способа измерения, запрашивая его по номеру карты. Если подобный номер карты имеется, то банк высылает в ответ совокупность способов измерения элементов квантовой метки, при этом банк-экваер информацию не считывает, сведения для настройки считывания поступает напрямую на терминал. Если номер карты числится без квантовой метки, метка подготавливается и высылается для нанесения на карту. В следующий раз считыватель и банк выполняют проверку данных квантовой метки. Если все верно – карта легитимна. Злоумышленник не сможет скопировать квантовую метку с банковской платежной карты без повреждения аутентификатора, делая процедуру копирования карты бессмысленной. Квантовую метку нельзя перенести без участия банка на другую карту, поскольку происходит привязка к номеру платежной карты.

Использование квантовой метки на карте с чипом позволяет внести дополнительный аутентификатор, при наличии которого украденный пин-код не приблизит злоумышленника к содержимому платежной карты. При онлайн-транзакции возможно прямое обращение к банку-эмитенту для возможности взаимодействия с квантовой меткой, банк-экваер в данном случае служит промежуточным пунктом обслуживания и не затрагивает передаваемый пакет, обращаясь исключительно к заголовкам, отмеченным обслуживаемым терминалом.

При использовании квантовой метки также появляется возможность проверки подлинности терминала [7]. Рассмотрим два вида атаки:

1. Злоумышленник ставит терминал официально, но хочет использовать его для перехвата данных. Пользователь использует такой терминал, вводит пин-код, совершает какие-либо операции. В данном случае выгода злоумышленника сомнительна. Во-первых, при официальном использовании доступ к устройству HSM, являющимся модулем шифрования внутри терминала, имеет крайне ограниченный и доверенный круг лиц, а именно HSM отвечает за зашифрованную связь между терминалом и банком. Несанкционированный доступ ведет к уничтожению всех хранимых ключей. Во-вторых, при воспроизведении метки на карте, терминал не сохраняет какую конкретно метку он нанес, т.е. информация подобного рода при-

нимается, воспроизводится и удаляется. Любой несанкционированный доступ к приемнику подобной информации ведет к его уничтожению. К тому же банк вправе инициировать дополнительную проверку карты и держателя, в случае возникновения подозрительной активности.

2. Злоумышленник ставит терминал неофициально. Имея пин-код пользователя и номер карты, без связи с банком-эмитентом невозможно получить полную копию карты. После считывания квантовой метки она разрушается, новую нанести невозможно без связи с банком-эмитентом. К тому же пользователь может обратить внимание на существенные технические заминки и пресечь незаконную деятельность. Терминалы возможно оснастить дополнительным идентификатором наличия/сохранности меток, в таком случае, даже если злоумышленник выведет пользователю сообщение о воспроизведении метки банком, обман вскроется при следующей транзакции, например, лицензированный терминал не обнаружит метки. В этот период времени списать денежные средства либо совершить иные махинации будет невозможно – копии карты не получено, метка не скопирована, пин-код в таком случае нагрузки не несет.

Для подобного средства аутентификации банковских карт, можно выделить следующие преимущества метода:

1. Дополнительная защита карт с магнитной полосой, за счет невозможности копирования метки без ее уничтожения и невозможность фальшивого воспроизведения.

2. Предотвращения несанкционированного копирования информации с карты.

3. Более защищенное проведение онлайн-транзакций.

4. Вариант противодействия фроду в сфере использования и обслуживания банковских терминалов.

Наряду с некоторыми преимуществами применение квантовых меток оставляет нерешённым ряд проблем с безопасностью и требует дополнительных усилий при внедрении:

1. Технологические проблемы в создании квантовых меток на текущим уровне развития соответствующих технологий.

2. Невозможность функционирования с офлайн-транзакциями.

3. Недостаточная проработанность способа оповещения банка о несанкционированном использовании квантовых меток, о неисправностях терминала при считывании метки и невозможности ее воспроизведения.

4. Необходимость дополнительного аутентификатора для удобного контроля за присутствием квантовой метки на банковской платежной карте.

С учетом повышения интереса к использованию банковских платежных карт и развития информационных технологий, является актуальным поиск новых способов противодействия злоумышленнику. Дополнительным

методом защиты может служить использование квантовой криптографической метки, сочетающей в себе подтверждение подлинности как банковских платежных карт, так и банковских терминалов. Несмотря на определённые трудности применения данного метода защиты, в перспективе он может быть задействован в различных инновационных системах обеспечения информационной безопасности [8].

Список используемых источников

1. Центральный банк Российской Федерации: Статистика: Количество платежных карт, эмитированных кредитными организациями, по типам карт [Электронный ресурс] // Центральный банк Российской Федерации. Режим доступа: http://www.cbr.ru/statistics/p_sys/print.aspx?file=sheet013.htm (дата обращения 22.09.2017).

2. Центральный банк Российской Федерации: Банкноты и монеты: Показатели наличного денежного обращения [Электронный ресурс] // Центральный банк Российской Федерации. Режим доступа: https://www.cbr.ru/Bank-notes_coins/?PrtId=nal (дата обращения 22.09.2017).

3. Лабусов М. В. Тенденции развития безналичных расчетов в Российской Федерации // Молодой ученый. 2015. № 24. С. 489–494. Режим доступа: https://moluch.ru/archive/104/24482/ (дата обращения 22.09.2017).

4. Банковские платежные карты [Электронный ресурс] // Сбербанк. Режим доступа: https://www.sberbank.ru/ru/person/bank_cards (дата обращения 22.09.2017).

5. The ACM Digital Library is published by the Association for Computing Machinery [Электронный ресурс] // СПС Stephen Wiesner: A special issue on cryptography. URL: http://archive.li/J4a0q#selection-275.19-275.50 (дата обращения 22.09.2017).

6. Центральный банк Российской Федерации: Национальная платежная система: Реестр кредитных организаций, признанных Банком России значимыми на рынке платежных услуг [Электронный ресурс] // Центральный банк Российской Федерации. Режим доступа: https://www.cbr.ru/Bank-notes_coins/?PrtId=nal (дата обращения 23.09.2017).

7. Путешествие банковской транзакции [Электронный ресурс] // Хабрахабр. Режим доступа: https://habrahabr.ru/post/229393/ (дата обращения 22.09.2017).

8. Андрианов В. И., Красов А. В., Липатников В. А. Инновационное управление рисками информационной безопасности: учебное пособие. СПб. : Федеральное агентство связи, Федеральное гос. образовательное бюджетное учреждение высш. проф. образования «Санкт-Петербургский гос. ун-т телекоммуникаций им. проф. М. А. Бонч-Бруевича», 2012, 396 с.

УДК 004.7

ПРИМЕНЕНИЕ MESH-СЕТЕЙ ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПЕРЕДАЧИ ДАННЫХ

О. С. Лаута, Д. В. Соловьев

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

Рассмотрены вопросы устройства самоорганизующихся mesh-сетей, а также топология их построения. Приведены основные преимущества использования таких сетей, их возможности по организации беспроводных сервисов для мобильных абонентов, а также выделены проблемы проектирования такого рода сетей.

Mesh-сети, самоорганизующиеся сети, обеспечение безопасности в сетях.

На сегодняшний день наиболее остро встаёт задача обеспечения безопасной передачи данных по сетям. Для решения данной задачи используются различный антивирусные программы, анализаторы сетевого трафика, интеллектуальные системы обнаружения вторжений и многое другое, однако злоумышленники находят всё новые и новые способы обхода защиты и получения доступа к перепискам, файлам или оборудованию пользователей. Одно из направлений обеспечения безопасности заключается в использовании Mesh-сетей.

Первые упоминания о Mesh для решения задач передачи информации следует искать в военных приложениях. На базе технологии Mesh созданы системы для организации мобильной связи с единичными объектами в зоне военных действий. Подобные системы обеспечивают высокоскоростную передачу цифровой информации, видео- и речевую связь, а также определяют местоположение объектов. В настоящий момент не существует точных критериев, определяющих термин Mesh-сеть в применении к системам широкополосного беспроводного доступа. Наиболее общее определение звучит как: «Mesh – сетевая топология, в которой устройства объединяются многочисленными (часто избыточными) соединениями, вводимыми по стратегическим соображениям» [1]. В первую очередь понятие Mesh определяет принцип построения сети, отличительной особенностью которой является самоорганизующаяся архитектура, реализующая следующие возможности:

– создание зон сплошного информационного покрытия большой площади;

– масштабируемость сети (увеличение площади зоны покрытия и плотности информационного обеспечения) в режиме самоорганизации;

– использование беспроводных транспортных каналов для связи точек доступа в режиме «каждый с каждым»;

– устойчивость сети к потере отдельных элементов.

Топология Mesh основана на децентрализованной схеме организации сети, в отличие от типовых сетей 802.11a/b/g, которые создаются по централизованному принципу. Точки доступа, работающие в Mesh-сетях, не только предоставляют услуги абонентского доступа, но и выполняют функции маршрутизаторов/ретрансляторов для других точек доступа той же сети. Благодаря этому появляется возможность создания самоустанавливающегося и самовосстанавливающегося сегмента широкополосной сети. Mesh-сети строятся как совокупность кластеров. Территория покрытия разделяется на кластерные зоны, число которых теоретически не ограничено. В одном кластере размещается от 8 до 16 точек доступа. Одна из таких точек является узловой (*gateway*) и подключается к магистральному информационному каналу с помощью кабеля (оптического либо электрического) или по радиоканалу (с использованием систем широкополосного доступа). Узловые точки доступа, как и остальные точки доступа (*nodes*) в кластере, соединяются между собой (с ближайшими соседями) по транспортному радиоканалу. В зависимости от конкретного решения точки доступа могут выполнять функции ретранслятора (транспортный канал) либо функции ретранслятора и абонентской точки доступа. Обобщенная топология Mesh-и показана на рис. 1.

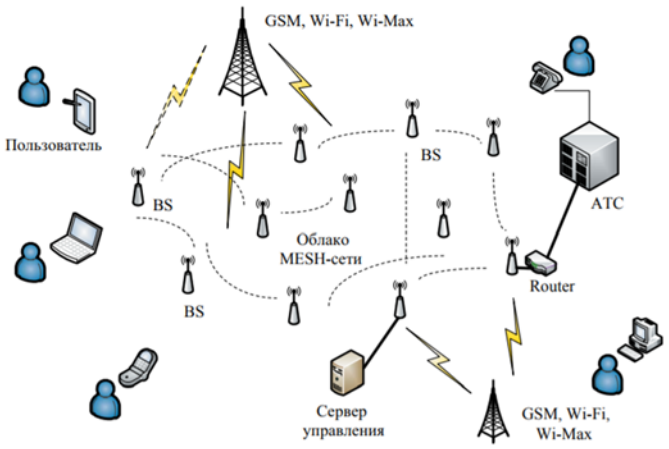


Рис. 1. Обобщенная топология Mesh-сети

Особенностью Mesh является использование специальных протоколов, позволяющих каждой точке доступа создавать таблицы абонентов сети с контролем состояния транспортного канала и поддержкой динамической маршрутизации трафика по оптимальному маршруту между соседними точками. При отказе какой-либо из них происходит автоматическое перенаправление трафика по другому маршруту, что гарантирует не просто

доставку трафика адресату, а доставку за минимальное время. Процедура расширения сети в пределах кластера ограничивается установкой новых точек доступа, интеграция которых в существующую сеть происходит автоматически. Недостаток подобных сетей заключается в том, что они используют промежуточные пункты для передачи данных; это может вызвать задержку при пересылке информации и, как следствие, снизить качество трафика реального времени (например, речи или видео). В связи с этим существуют ограничения на количество точек доступа в одном кластере. На сегодняшний день выпускается Mesh-оборудование как внешнего, так и внутреннего размещения.

Mesh-топология позволяет реализовать уникальные по своим возможностям сети муниципального назначения, ориентированные на службы оперативного реагирования (милиция, «Скорая помощь», МЧС). На рис. 2 показана принципиальная схема организации такой зоны (одним из требований является наличие производителей мобильных роутеров).

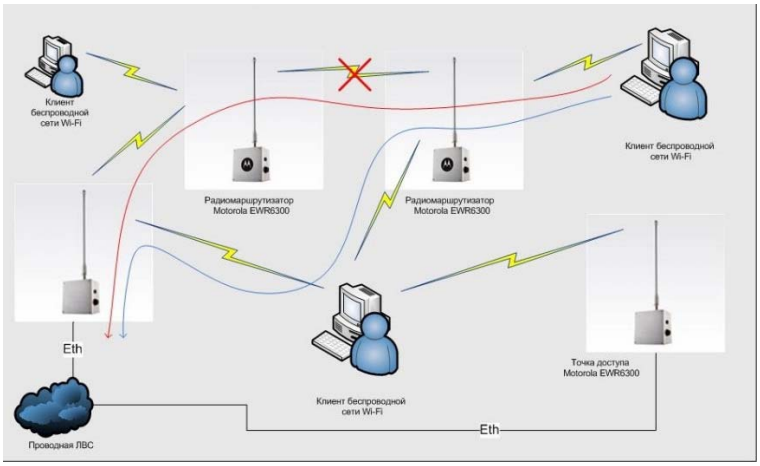


Рис. 2. Принципиальная схема организации муниципальной сети беспроводного доступа стандарта Wi-Fi

Основу сети составляют узловые и абонентские точки доступа, размещаемые на улице (как правило, вдоль дорог) и организующие зоны информационного покрытия, в которых обеспечивается подключение абонентов со стандартными Wi-Fi-адаптерами. Дополнительно точки доступа могут использоваться для организации управления движением (светофоры) и сбора видеоинформации, с подключением видеокамер по проводному или беспроводному интерфейсу. Подключение пользователей, расположенных внутри помещений, к внешней сети производится с помощью внутриофисных точек доступа, которые характеризуются пониженной выходной мощностью и «комнатным» исполнением корпуса. Наибольший интерес представляют мобильные точки доступа, предназначенные для эксплуатации

в автомобилях [2]. Использование этих устройств не только увеличивает радиус действия между точками доступа до 800–1200 метров, но и позволяет организовать:

– информационное обеспечение пользователей внутри автомобиля при проводном или беспроводном подключении конечных устройств (ноутбук, PDA и т. д.);

– информационное покрытие в радиусе 300 м вокруг автомобиля для абонентов со стандартными Wi-Fi-адаптерами 802.11b/g;

– контроль положения автомобиля при использовании встроенного в точку доступа GPS-приемника.

Применение мобильных точек доступа позволяет организовать оперативное расширение зоны покрытия или увеличение информационной емкости сети за счет концентрации оборудованных автомобилей в «горячих точках». Механизмы самоорганизации Mesh-сети позволяют за минимальное время (определяемое временем прибытия автомобилей, оборудованных Mesh-точками доступа) организовывать зону Wi-Fi с передачей оперативной аудио- и видеоинформации на центральный пульт. Анализ создания и развития Mesh-сетей показывает, что существует устойчивая тенденция объединения абонентских и муниципальных сетей [3]. Зачастую сети, построенные по муниципальному заказу, дополняются впоследствии точками доступа и эксплуатируются операторами в объединенном «муниципально-абонентском» режиме.

Вопросы безопасности Mesh-сети являются весьма актуальными. Широко применяемый в настоящее время стандарт шифрования (*wired equivalent privacy* (WEP)) является несовершенным, поэтому принятие стандарта 802.11i (WPA2) сделает доступной более безопасную схему аутентификации и кодирования трафика. Стандарт IEEE 802.11i предусматривает использование в продуктах Wi-Fi таких средств, как поддержка алгоритмов шифрования трафика, например, TKIP (*temporal key integrity protocol*), WRAP (*wireless robust authenticated protocol*) и CCMP (*counter with cipher block chaining message authentication code protocol*) [4]. Эти стандарты позволяют достаточно надежно защищать каналы сети от несанкционированного доступа.

Усложнение Mesh-систем по мере увеличения их масштаба и необходимость объединения с альтернативными сетями (GSM, 3G, Wi-Max, LTE и т. д.) потребуют создания более сложных систем управления, основанных на централизованных унифицированных решениях. Наибольшей эффективности такого рода сетей следует ожидать при реализации Mesh-сетей в масштабах города (MAN) [5]. Особенности организации и использования подобных сетей определяются социальной и коммерческой целесообразностью, при этом сети могут либо строиться только как корпоративные или абонентские, либо решать обе задачи одновременно.

Живучесть такой сети в условиях чрезвычайных ситуаций достаточно велика за счет динамической переконфигурации и перемаршрутизации трафика, а также вследствие наличия большого количества обходных и резервных путей для трафика внутри сети. Как правило, каждый узел такой сети имеет связность, равную двум и более, что позволяет повысить отказоустойчивость структуры сети в целом и оперативно решать поставленные задачи. Важным аспектом беспроводных Mesh-сетей, обусловливающим высокий потенциал этой технологии, является возможность быстро и недорого предоставлять мобильным пользователям широкополосные услуги. Стоимость развертывания Mesh-сети может быть значительно меньше стоимости традиционных проводных сетей, поскольку для этого не требуется наличия дорогостоящей инфраструктуры и прокладки кабелей. Кроме того, Mesh-сеть эффективна при эксплуатации, поскольку, как отмечено выше, обладает способностью к самовосстановлению и самоадаптации.

Список используемых источников

1. Осипов И. Е. Mesh-сети: технологии, приложения, оборудование [Электронный ресурс] // Технологии и средства связи: электрон. научн. журн. 2006. № 4. С. 38–45. URL: http://www.dateline.ru/resources/Публикации/mesh-osipov.pdf (дата обращения 29.01.2018).

2. Портнов Э. Л. Принципы построения первичных сетей и оптические кабельные линии связи. М. : Горячая линия – Телеком, 2009. 544 с.

3. Вишневский В. М., Портной С. Л., Шахнович И. В. Энциклопедия WiMAX. Путь к 4G. М. : Техносфера, 2009. 471 с.

4. Шахнович И. Современные технологии беспроводной связи. М. : Техносфера, 2006. 288 с.

5. Соколов Н. А. Задачи планирования сетей электросвязи. СПб. : Техника связи, 2012. 432 с.

УДК 004.056

ПРОБЛЕМЫ ЗАЩИТЫ ДАННЫХ В ВИРТУАЛЬНОЙ ИНФРАСТРУКТУРЕ

М. В. Левин, Е. С. Фостач

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

Проблема обеспечения безопасности данных, размещенных в облачных средах, является уязвимым местом эксплуатации модели виртуализации. В данной статье рас-

смотриваются особенности безопасности облачной архитектуры, а также проводится анализ перспективы развития модели предоставления облачных услуг. Результаты проведенного анализа позволяют сформировать требования к обеспечению информационной безопасности, а также определить ключевые функции, которые должны быть поддержаны как поставщиком, так и потребителем услуг. Такой подход способствует обеспечению высокой скорости развертывания, оперативности и эффективности, обеспечивая по требованию пользователя доступ к общим источникам вычислительных ресурсов в автономном, динамично масштабируемом и выверенном режиме.

облачные технологии, SaaS, PaaS, IaaS, виртуализация, информационная безопасность, облака.

Введение

Облачные вычисления являются следующим шагом развития Интернет-технологий, где вычислительные ресурсы предоставляются пользователю в качестве услуги «as-a-service». У модели предоставления облачных услуг имеется ряд проблем, которые влияют на ее эксплуатацию. Для поставщиков облачных услуг обеспечение безопасности требует значительных финансовых затрат и ресурсов (т.к. обеспечение безопасности является задачей потребления ресурсов) [1]. Тем не менее, ответственность за обеспечение безопасности должна возлагаться как на поставщика, так и на потребителя облачных услуг в зависимости от используемой сервисной модели.

Архитектура облачных технологий

Согласно стандарту NIST, модель облачных вычислений описывает три модели предоставления услуг: инфраструктура как услуга (IaaS), платформа как услуга (PaaS), программное обеспечение как услуга (SaaS) [2]. Архитектура облачных вычислений представляет собой упорядоченный набор уровней объектов виртуализации, где функциональность и безопасность более высокого уровня зависит от обеспечения и контроля безопасности на нижних уровнях. Для поддержания трех базовых свойств информационной безопасности – конфиденциальности, целостности и доступности данных пользователей, были обозначены ключевые проблемы, которые необходимо решить в первую очередь:

1. Исследование механизмов аутентификации пользователей и использования защищенного канала связи на пути между клиентом и сервером.
2. Исследование способов хранения информации в зашифрованном виде, ее обработки и поиска в облачном хранилище.

Решение данных проблем позволит повысить уровень конфиденциальности, целостности и доступности данных в облачных средах.

Определение способов конфиденциальной передачи данных

За основу была взята схема функциональной архитектуры облачной среды, на базе которой построено исследование. Схема демонстрирует способ развертывания баз данных и приложений на ресурсах облачной инфраструктуры вместе с сетевой схемой взаимодействия, показывает уровни коммутации (L2) и маршрутизации (L3) данных между объектами облачной инфраструктуры.

В соответствии с решаемой проблемой, ключевыми аспектами информационной безопасности, которые должны лежать в основе каждого надежного облачного сервиса, являются – определение способов конфиденциальной передачи данных, организация доступа авторизованных пользователей к данным.

Решение первой задачи, определение способов конфиденциальной передачи данных, требует использования криптографических механизмов, позволяющих обеспечить надежное шифрование данных. С целью снижения вероятности перехвата в открытом виде передаваемого сообщения, шифрование данных должно происходить до того момента, как информация покинет браузер пользователя (т. е. до момента отправки сообщения на сервер).

Использование протокола TLS v1.2 позволяет создать канал конфиденциальной передачи данных. Механизмы работы данного протокола не обеспечивают контроль времени жизни каждой пользовательской сессии и повторную аутентификацию клиента для возобновления сессии в случае разрыва установленного соединения. Протокол TLS v1.2 не позволяет аутентифицировать самого пользователя, в связи с этим, рассмотрим механизм аутентификации пользователей в рамках протокола OAuth2.0.

Организация доступа авторизованных пользователей к данным

В связи с глобальным развитием облачных сервисов и многообразием служб, позволяющих создавать и распространять медиа-контент или получать мгновенный доступ к электронным услугам перед разработчиками сервисов возникает задача обеспечения безопасности. Необходимо решать задачи защиты данных от несанкционированного доступа пользователей, работающих в большом количестве приложений. Ситуация осложняется тем, что работа пользователя не должна затрудняться внутренними механизмами безопасности и перемещение между сервисами должно происходить максимально быстро и безопасно для услуг, предоставляемых пользователю [3, 4, 5].

Чтобы решить задачу, связанную с упрощением авторизации пользователя при работе с большим количеством приложений и онлайн сервисов, был разработан протокол OAuth. При использовании OAuth-авторизации

к основным преимуществам принято относить отсутствие передачи логина и пароля в приложение, с которым работает пользователь [6]. Таким образом, приложение может выполнить только то, что явно разрешил пользователь. Так же, отпадает необходимость решения вопроса обеспечения защищенного хранения пароля и логина приложением.

Актуальная версия стандарта OAuth 2.0, опубликована в 2012 г. в документе IETF RFC 6749. OAuth 2.0 позволяет сторонним приложениям получать доступ от своего имени или ограниченный доступ к HTTP-службе от имени владельца ресурса, организовав процесс согласования взаимодействия между владельцем ресурса и HTTP-службой. Результатом авторизации является Access Token – ключ, предъявление которого является пропуском к защищенным ресурсам. Стандарт не определяет формат ключа, который получает приложение, поэтому ключ сам по себе не может быть использован для аутентификации пользователя [7, 8].

Таким образом, снижение риска несанкционированного доступа к ресурсам, и, как следствие, обеспечение доступности информации, можно добиться за счет внедрения механизма аутентификации.

Суммируя описанные ранее подходы, представим концептуальную схему (рис.), которая отражает ключевые элементы облачной архитектуры (клиентскую часть приложения, сервер аутентификации, сервер приложения (который включает в себя механизмы обработки информации), а также хранилище данных). Дополнительно, на схеме отмечено, на каких сегментах сети применимы рассмотренные ранее протоколы OAuth 2.0, TLSv1.2 для обеспечения надежного соединения.

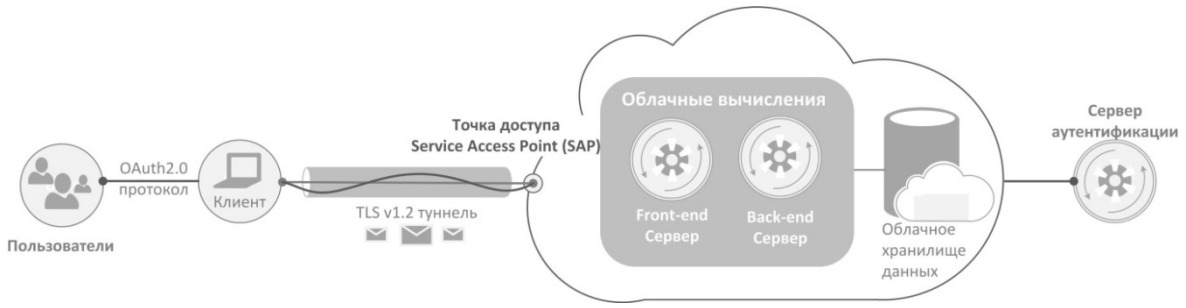


Рисунок. Концептуальная схема построения защищенной облачной среды

Заключение

В результате исследования показано, что для создания надежного TLS соединения важно иметь возможность аутентификации именно клиентской части приложения, а не самого пользователя. Так же стоит отметить, что в основе протокола TSL v1.2 отсутствуют механизмы контроля времени жизни пользовательской сессии и механизмы повторной аутентификации для возобновления сессии в случае разрыва соединения. Вследствие чего

необходимо внедрение средств аутентификации пользователей за счет протокола OAuth2.0.

Список используемых источников

1. Wayne Jansen, Timothy Grance, Guidelines on Security and Privacy in Public Cloud Computing, NIST, Draft Special Publication 800-144, January 2011.

2. T. Dierks, E. Rescorla. The Transport Layer Security (TLS) Protocol, Version 1.2 (RFC5246).

3. 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. 2015. № 1. С. 141–146.

4. Красов А. В. Левин М. В. Возможности управления трафиком в рамках концепции SDN // Актуальные проблемы инфотелекоммуникаций в науке и образовании. IV Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 2 т., 2015. С. 350–354.

5. Алейников А. А., Билятдинов К. З., Красов А. В., Левин М. В. Контроль, измерение и интеллектуальное управление трафиком : монография. СПб. : Центр «Астерион», 2016. 92 с. ISBN 978-5-00045-385-8.

6. Красов А. В., Левин М. В., Штеренберг С. И., Исаченков П. А. Модель управления потоками трафика в программно-определяемой сети с изменяющейся нагрузкой // Наукоемкие технологии в космических исследованиях Земли. 2016. Т. 8. № 4. С. 70–74.

7. Security issues in OAuth 2.0 SSO implementations. Li, W. & Mitchell, C. J. 2014 Information Security // 17th International Conference, ISC 2014, Hong Kong, China, October 12–14, 2014. Proceedings. Chow, S., Camenisch, J., Hui, L. & Yiu, S-M. (eds.). Springer-Verlag, p. 529–541, 13 p.

8. Алейников А. А., Билятдинов К. З., Красов А. В., Кривчун Е. А., Крысанов А. В. Технические аспекты управления с использованием сети интернет : монография. СПб. : Центр «Астерион», 2016. 305 с. ISBN 978-5-00045-408-4.

Статья представлена научным руководителем, кандидатом технических наук, доцентом А. В. Красовым.

УДК 004.057.4, 004.056.5

БЕЗОПАСНАЯ ТРАНСПОРТИРОВКА СООБЩЕНИЙ С ИСПОЛЬЗОВАНИЕМ ПРОТОКОЛА SECURE SCTP

А. В. Лейкин

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

Протокол Secure SCTP обеспечивает функции безопасности на транспортном уровне без необходимости использования других протоколов безопасности, например,

TLS или IPSec. В данной статье мы продолжим его рассмотрение и остановимся более детально на процедурах, необходимых для интегрирования криптографических функций в базовый протокол SCTP. В статье приводится MSC-сценарий процесса установления, сопровождения и разрушения безопасного сеанса связи с поясняющими комментариями.

SCTP, S-SCTP, Secure SCTP, информационная безопасность.

Для защиты данных, передаваемых с использованием протокола SCTP [1], возможно использование нескольких решений, в зависимости от требуемого уровня реализации в модели OSI [2, 3], а именно: SCTP поверх IPSec [4], TLS поверх SCTP [5] и решение Secure SCTP (далее S-SCTP) [6], которое сейчас находится в стадии разработки. Проведенное сравнение этих решений [7] показало, что предлагаемая разработчиками интеграция криптографических функций непосредственно в протокол SCTP позволяет полностью избежать недостатков не интегрированных решений при этом обеспечивая полную совместимость с базовым протоколом SCTP.

На текущий момент нотификация протокола S-SCTP имеет статус Интернет-проекта (англ. Internet Draft), являясь по сути черновиком, вынесенным на всеобщее рассмотрение и в который можно внести изменения. Более подробно вопросы стандартизации протоколов освещены в [8].

Ранее [9] мы рассмотрели основной принцип работы протокола S-SCTP, его структурную схему, возможности, поддерживаемые уровни безопасности, а также новые команды, которые необходимо добавить в базовый протокол SCTP для поддержки им криптографических функций.

Напомним, что S-SCTP позволяет передавать как зашифрованные, так и не зашифрованные данные в рамках одного безопасного сеанса[1]. Приложения, использующие данный протокол, могут установить один из четырех уровней безопасности, который может быть изменен в любой момент времени в течение срока службы сеанса связи. Для поддержки криптографических функций в базовый протокол вводятся новые команды и параметры, которые могут быть объединены с другими командами в единый пакет. Названия и назначение новых команд приведены в [9]. Их формат, а также формат, названия и назначение новых параметров в п. 5.1 [6].

Новые процедуры протокола S-SCTP

Так как протокол S-SCTP является протоколом, ориентированным на соединение, то его работу можно условно разбить на несколько фаз: «создание безопасного сеанса связи», «передача данных» и «разрушение безопасного сеанса связи». Рассмотрим сценарий сигнального обмена с использованием протокола S-SCTP между двумя конечными точками (см. рис.),

[1] Безопасный сеанс (англ. *Secure session*) – это сеанс, который обеспечивает функции безопасности для установленной SCTP ассоциации.

а также процедуры, которые необходимо реализовать для безопасной передачи данных.

1. В фазе создания безопасного сеанса (далее – сеанса) выполняются следующие процедуры:

Установление сеанса связи. Сеанс может быть установлен и завершен приложением в любой момент времени в течение срока службы ассоциации SCTP [10], но если сеанс связи уже существует, то создание нового невозможно. Процедура начинается, когда одна из взаимоувязанных в ассоциацию конечных точек устанавливает значение уровня безопасности больше «0». Конечная точка, инициализирующая сеанс, называется клиентом, а встречная сервером. Для запуска процедуры конечная точка-клиент передает команду «Secure Session Open request, SSOpReq» с необходимым набором параметров, а сервер в качестве подтверждения ее приема использует команду «Secure Session Open Acknowledge, SSOpReq_Ack». Во время установления сеанса рекомендуется аутентифицировать конечную точку с помощью сертификата, который может быть передан встречной стороне командой «Secure Session Certificate, SSCert».

Выбор набора шифров и метода сжатия. Каждая конечная точка содержит упорядоченный список поддерживаемого набора шифров[2]. Упорядочение в списке указывает на предпочтение, с которым должен быть использован метод шифрования.

Генерация секретного мастер-ключа. Сервер и клиент вычисляют секретный мастер-ключ[3] раздельно, а для его генерации используется алгоритм 3DES_CBC. Во время алгоритма обмена ключами сервером и клиентом используются команды «Secure Session Server Key, SSSerKey» и «Secure Session Client Key, SSCliKey» соответственно.

Генерация случайного числа. Используется при вычислении мастер-ключа и хеш-функции, требования к процедуре приведены в RFC 4086 [11].

Алгоритм HMAC. S-SCTP использует такой же алгоритм расчета криптографической хеш-функции как IPSec и TLS. Алгоритм HMAC определен в RFC 2104 [12].

Завершается фаза установления сеанса двухсторонним обменом командой «Secure Session Open Complete, SSOpCom». После приема этой команды конечная точка верифицирует данные проверки, которые содержатся в команде и в случае неуспешной проверки сеанс будет закрыт.

[2] Набор шифров (англ. *Cipher suite*) – это набор криптографических алгоритмов, которые используются для обмена ключами, шифрования/дешифрования данных и аутентификации пакетов.

[3] Секретный мастер-ключ (англ. *Master secret key*) – S-SCTP использует два вида секретных ключей: для аутентификации пакетов S-SCTP и для шифрования/дешифрования данных.

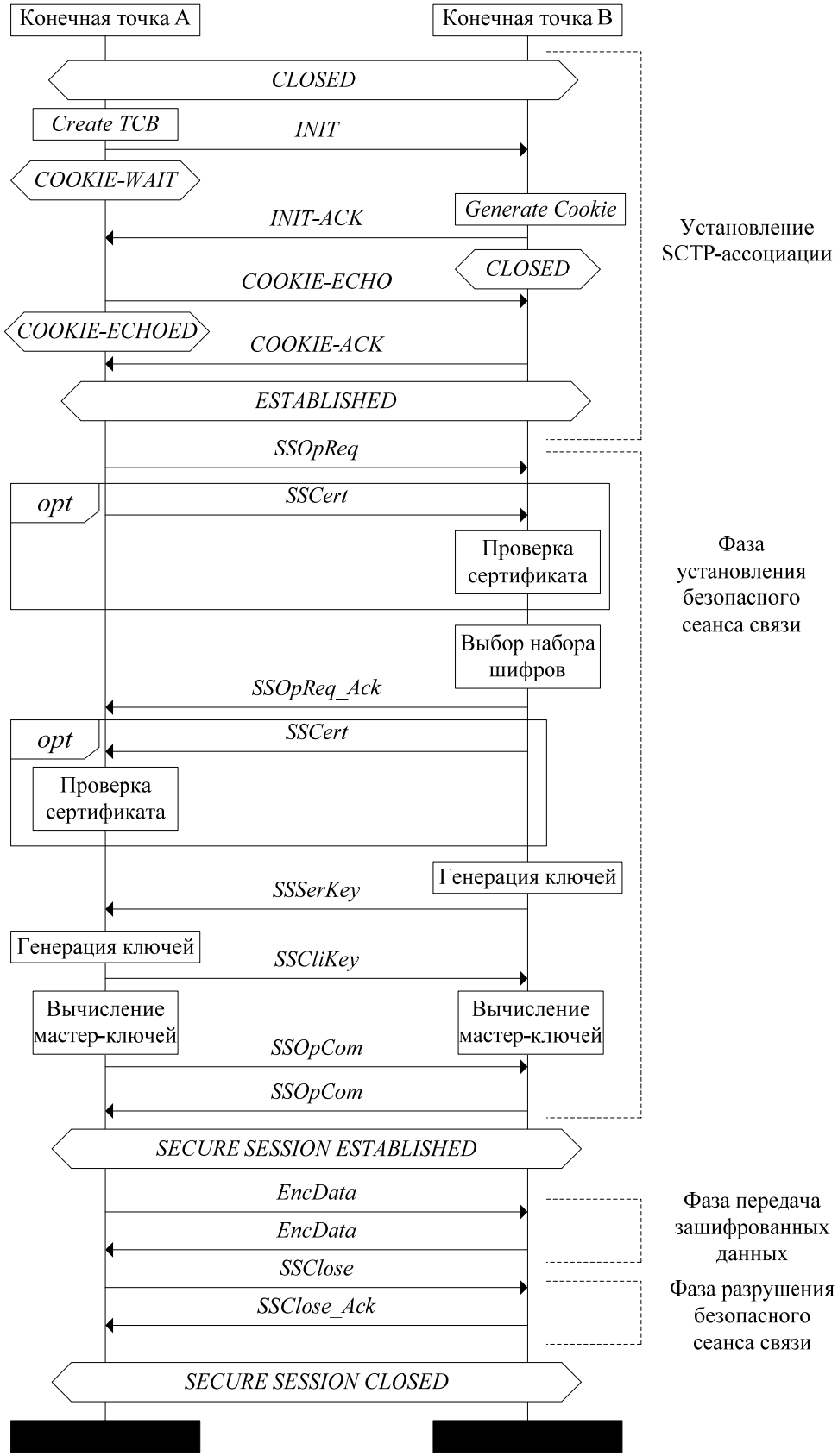


Рисунок. Сценарий сигнального обмена с использованием протокола Secure SCTP

2. Фаза передачи данных.

Обновление секретного мастер-ключа. Процедура очень важна для обеспечения безопасности, всего существует два типа секретных ключей: мастер-ключ для шифрования данных и секретный ключ HMAC, который используется для аутентификации пакетов. Для повышения безопасности при продолжительной безопасной сессии секретные мастер-ключи необходимо обновлять. Процедура может быть запрошена любой из сторон передачей команды «SSOpReq».

Передача данных. Осуществляется в следующей последовательности:

a) S-SCTP разделяет блоки данных на две группы: зашифрованные (требующие шифрования) и незашифрованные. Если уровень безопасности равен «3», то все данные определяются в первую группу.

b) Объединение команд «DATA» в зашифрованную группу. S-SCTP вычисляет размер команды «Padding»[4] и при необходимости добавляет ее в конец подлежащей шифрованию группы. При этом размер подлежащих шифрованию данных не должен превышать текущий размер MTU[5], в противном случае S-SCTP должен создать две группы шифрования. После шифрования данные помещаются в поле команды «EncData», которая может содержать одну или несколько команд «DATA».

c) SCTP создает пакет данных в зависимости от уровня безопасности и добавляет команду «AUTH» в конец сформированного пакета.

d) S-SCTP отправляет пакет.

Начало выполнения процедуры зависит от установленного уровня безопасности, который проверяется перед передачей пакета по сети. Если уровень безопасности равен «0», то процедура начинается с шага «d», «1» с шага «c», «2» – если пользователю требуется шифрование данных, то процедура начинается с шага «a», в обратном случае – с шага «c» и, наконец, при уровне «3» процедура начинается с шага «a».

3. Фаза разрушения сеанса

Завершение безопасного сеанса связи. Процедура запускается отправкой конечной точкой команды «Secure Session Close, SSClose» – эта команда включает в себя последние зашифрованные данные. После ее отправки шифрование и аутентификация всех команд или пакетов конечной точкой прекращается, но передача незашифрованных данных будет продолжаться. Для подтверждения приема используется команда «Secure Session Close Acknowledge, SSClose_Ack».

[4] Алгоритмы симметричного шифрования используют блок-ориентированное шифрование пользовательских данных. Например, DES использует 64-битные блоки, а AES 128-битные. Перед процедурой шифрования пользовательские данные должны быть отформатированы в соответствии с требуемым размером блока, поэтому если последний блок не полный, то добавляется «Padding».

[5] MTU – Maximum transmission unit – это максимальный размер полезного блока данных одного пакета, который может быть передан протоколом без фрагментации.

В случае обнаружения ошибки в момент создания или обновления безопасного сеанса связи, обработки сертификата, расшифровки команды «EncData», аутентификации или распаковки сжатых данных S-SCTP ассоциация немедленно останавливает процесс. При этом сама SCTP ассоциация продолжает выполняться, но без поддержки функций безопасности. Для извещения встречной стороны используется команда «Ошибка, ERROR» [1, 10], в которой передается параметр «Причина ошибки, Error Causes» с соответствующим кодом ошибки (см. п. 6. [6]).

Список используемых источников

1. Stewart R. RFC4960 Stream Control Transmission Protocol. September 2007. URL: https://tools.ietf.org/html/rfc4960 (дата обращения 04.03.2018).

2. Лейкин А. Протоколы транспортного уровня UDP, TCP, SCTP: достоинства и недостатки // Проводные сети. Первая миля. 2013. № 5. С. 62–69.

3. Лейкин А. В., Гольдштейн А. Б. Протоколы группы SIGTRAN. Часть 1 : учебное пособие ; СПбГУТ. СПб., 2017. 82 с.

4. Bellovin S., Ioannidis J., Keromytis A., Stewart R. RFC 3554 On the Use of Stream Control Transmission Protocol (SCTP) with IPsec. July 2003. URL: https://tools.ietf.org/html/rfc3554 (дата обращения 04.03.2018).

5. Jungmaier A., Rescorla E., Tuexen M. RFC3436 Transport Layer Security over Stream Control Transmission Protocol. 2002. https://tools.ietf.org/html/rfc3436 (дата обращения 04.03.2017).

6. Hohendorf C., Unurkhaan E., Dreibholz T. Secure SCTP draft-hohendorf-secure-sctp-25.txt. 2018. URL: https://tools.ietf.org/html/draft-hohendorf-secure-sctp-25 (дата обращения 25.03.2018).

7. Лейкин А. В. Сравнение решений безопасности для SCTP // Актуальные проблемы инфотелекоммуникаций в науке и образовании. V Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 3 т. 2016. Т. 1. 451–456 с.

8. Лейкин А. В. Вопросы стандартизации протоколов группы SIGTRAN // Вестник связи. 2017. № 7. С. 4–13.

9. Лейкин А. В. Введение в протокол SECURE SCTP // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VI Международная научно-техническая и научно-методическая конференция; сб. науч. ст. в 4 т. 2017. Т. 2. 481–486 с.

10. Лейкин А. В., Гольдштейн А. Б. Протоколы группы SIGTRAN. Часть 2 : учебное пособие ; СПбГУТ. СПб., 2018.

11. D. Eastlake 3rd, J. Schiller, S. Crocker. RFC 4086. Randomness Requirements for Security. June 2005. URL: https://tools.ietf.org/html/rfc4086 (дата обращения 10.03.2018).

12. H. Krawczyk, M. Bellare, R. Canetti. RFC 2104 HMAC: Keyed-Hashing for Message Authentication. February 1997. URL: https://tools.ietf.org/html/rfc2104 (дата обращения 10.03.2018).

Статья представлена заведующим кафедрой, доктором технических наук, профессором Б. С. Гольдштейном.

УДК 621.391

РАЗВИТИЕ ТРЕБОВАНИЙ К СИСТЕМАМ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

О. М. Лепешкин, Ю. К. Худайназаров

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

Изменение требований к системам обеспечения информационной безопасности происходит эволюционно с различными темпами на определенных этапах развития методологии управления организационно-техническими системами и уровня техники связи и автоматизации управления. Возможны переходные этапы, когда требования к системе обеспечения информационной безопасности, например, информационно-телекоммуникационной системы специального назначения, теряют актуальность, вследствие изменений влияющих факторов, которые не всегда очевидны.

обеспечение информационной безопасности, моделирование, требования к системе.

Основными факторами, которые определяют актуальность требований к системе обеспечения информационной безопасности (СОИБ) организационно-технической системы (ОТС) являются влияющие на нее внутренние и внешние факторы, достигнутый уровень техники в предметной области информационной безопасности (ИБ), а также используемые методология управления организационно-техническими системами и методология моделирования устойчивости ОТС (рис. 1).

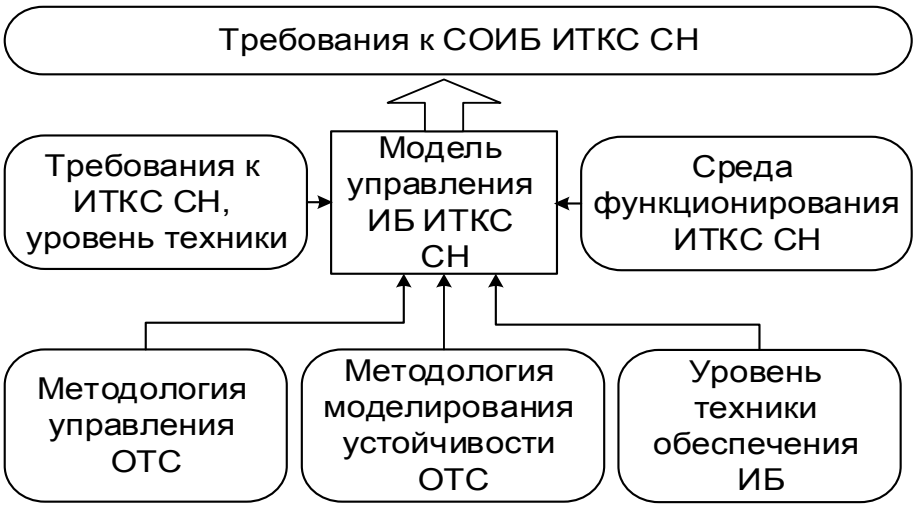


Рис. 1. Взаимосвязь основных факторов, определяющих требования к СОИБ ИТКС

Современный уровень техники информационно-телекоммуникационной системы специального назначения (ИТКС СН) характеризуется следующими основными особенностями.

Облачные технологии реализуются в продвинутой сетевой архитектуре «клиент-сервер» с расширенной вычислительной интерпретацией, направленной на предоставление не только информационных, но и алгоритмических услуг в широких диапазонах применения.

Технология программно-конфигуриемых сетей, Software Defined Networks (SDN) предполагает структуру сети с централизованным управлением, в которой отсутствует уровень управления (*Control Plane*) в каждом сетевом устройстве, что, удешевляет и это устройство.

Концепция виртуализации сетевых функций, Network Functions Virtualization (NFV) предполагает замещение разнообразных сетевых устройств стандартизированными высокопроизводительными серверами, коммутаторами и системами хранения данных с реализацией сетевых функций (служб) с помощью программного обеспечения.

Технология программно-определяемого радио (SDR) позволяет с помощью программного обеспечения управлять основными функциональными параметрами радиоустройства. Наблюдается конвергенция SDR с RFID.

Система когнитивного радио (CRS) способна получать сведения об условиях и результатах своего функционирования и на основе этих данных корректировать контролируемые параметры работы. Наблюдается конвергенция CRS с геоинформационными технологиями.

Развитие технологии «умных вещей» («Интернет вещей»), таких, как NBiOT и NDFi. Технологии NBiOT-сетей – технологии связи между устройствами телеметрии с низкими объемами обмена данными на базе сетей сотовой связи. NDFi – российский стандарт «Интернета вещей».

Ведутся исследования в области создания наносетей – технологии самоорганизующейся сети, в которой в качестве узлов сети используются наномашины, а информация и сигнализация могут быть переданы в том числе и путем перемещения вещества.

Широко внедряются экспертные системы обеспечивающего характера, которые позволят анализировать в реальном масштабе времени обстановку, в значительной мере поддающуюся формализации системы управления: системы для поиска неисправностей в сложных системах и агрегатах, планирования тылового обеспечения военных операций, автоматической дешифровки визуальных изображений, моделирования боевой обстановки при проведении командно-штабных игр.

Уязвимости и угрозы ИБ ИТКС СН

Централизованное управление в SDN уменьшает отказоустойчивость (живучесть) сети. Контроллер как ключевой компонент в управлении всей инфраструктурой является наиболее уязвимым элементом, традиционные атаки на который может повлечь критичные для всей инфраструктуры последствия.

Виртуализация и переход к облачным средам радикально сужают возможности традиционных средств безопасности [1] и приводят к появлению принципиально новых угроз. Основными проблемами облачной инфраструктуры являются: защита периметра и разграничение сети, динамичность виртуальных машин, уязвимости и атаки внутри виртуальной среды, защита бездействующих виртуальных машин.

На основе достижений нанотехнологий и сетевых технологий возник новый вид разведки: измерительно-сигнатурная разведка (MASINT – *Measurement And Signature INTelligence*), которая заключается в комплексности и применения различных физических принципов наблюдения за объектом (измерение геометрических размеров и соотношений, физических характеристик, регистрация сигнатур характерных полей и сигналов объекта, выявление химических и биологических агентов, состава конструкционных материалов) с целью выявления назначения, тактики применения, возможностей, основных характеристик и уязвимостей объекта.

Наличие в современных ИТКС управления по протоколу OpenFlow технологически позволяет использовать SDN-сеть как сенсор. Таким образом, новые технологии позволяют создать наложенную распределенную глобальную сеть для сбора данных на основе существующих региональных и локальных сетей. Любое мобильное устройство связи в таком случае при установке специального программного обеспечения (программной закладки) может служить датчиком системы измерительно-сигнатурной разведки [2]. Примерами таких сетей являются:

MAINWAY – система анализа телефонных метаданных по звонкам;

MARINA – система анализа записей из Интернет (основной инструмент АНБ для хранения и анализа метаданных);

SHELLTRUMPET&EVILOLIVE – система сбора Интернет-метаданных;

PRISM – система негласного сбора информации, передаваемой по сетям электросвязи (Интернет-контента) и другие.

Методология моделирования устойчивости ИТКС СН

Для адекватного отражения сложного многопараметрического объекта такого, как ИТКС, одного инструмента моделирования недостаточно. Современные научные тенденции заключаются в построении иерархических

гибридных моделей для сложных объектов. В данном случае целесообразно использовать следующие уровни моделирования: модель информационного взаимодействия агентов в распределенной системе; модель противоборства распределенных мультиагентных систем (например, на основе *WarGaming*); модель управления устойчивостью ИТКС СН.

Уровень техники обеспечения ИБ ИТКС СН

Потенциально технологии виртуализации позволяют использовать традиционные технологии обеспечения безопасности на новом уровне более эффективно. Известные стратегии обеспечения безопасности виртуальных сред подразумевают развитие двух независимых направлений:

1. Создание и усовершенствование защиты хостов и виртуальных машин.

2. Защита данных, расположенных в виртуальной среде.

Распределенная система управления виртуальными системами и средствами защиты может создаваться на основе следующих технологий:

когнитивные технологии контроля киберпространства и раннего предупреждения компьютерного нападения (iSOPKA); технологии автоматизированного моделирования обстановки и прогнозирование поведения оппонентов (*WarGaming*); технологии адаптивной архитектуры безопасности (*Adaptive Security Architecture*); ителлектуальные технологии обеспечения информационной безопасности на основе больших данных и потоковой обработки данных (*BigData*+ETL); технологии доверенной сетки устройств (безопасные мобильные технологии (*Device Mesh*); доверенные «облачные» и виртуальные среды.

Подходы к управлению ИБ ИТКС СН

Необходимость повышения качества управления в ИТКС привело к использованию технологий, реализующих функции искусственного интеллекта, которые распространяются в системы разведки и радиоэлектронной борьбы и в системы обеспечения информационной безопасности (рис. 2).

Анализ представленных тенденций свидетельствует о превращении ИТКС в организационно-техническую суперсистему, требования по обеспечению безопасности которой должны быть адекватны уровню техники, актуальным уязвимостям и угрозам, а также учитывать особенности процессов в суперсистемах. Под суперсистемой понимается множество элементов, функционально аналогичных друг другу, самоуправляемы (или управляемы извне) в пределах иерархически высшего объемлющего управления на основе информации, хранящейся в их памяти. Это может быть внешний по отношению к безинтеллектуальной суперсистеме интеллект (например, SDN),

может быть интеллект, присутствующий в суперсистеме, а также и интеллект, порождённый самой суперсистемой некоторым образом (наложенные сети на основе NFV).

Время / Факторы	I этап	II этап	III этап	IV этап
Подходы к управлению ИБ ИТКС СН	Фрагментарный (объектовый уровень)	Комплексный (локальный уровень)	Системный (региональный уровень)	Суперсистемный (глобальный уровень)
Методология моделирования устойчивости ИТКС СН	Модели распространения сигналов, Модели криптосистем	Модели противодействия техническим разведкам	Модели противоборства программных агентов, модели компьютерных стегосистем	Иерархические модели противоборства мультиагентных распределенных систем
Уровень техники обеспечения ИБ ИТКС СН	Средства стеганографии, шифрования и имитозащиты	Комплексы защиты информации, Технологии анализа кода программ	Криптографические модули, Квантовые технологии защиты информации, Системы безопасности (IDS, SIEM).	Распределенная система управления виртуальными системами и средствами защиты, адаптивная архитектура безопасности
Угрозы ИБ ИТКС СН	Средства разведки, радиоподавления и дезинформации	Комплексы разведки и РЭБ, вредоносное ПО, компьютерные атаки	Сенсорные сети, сетевые средства РЭБ, программные закладки, ботсети	MASINT, глобальные сенсорные сети, атаки на виртуальные машины и гипервизоры
Уровень техники ИТКС СН	Средства связи, средства вычислительной техники, навигации	Комплексы средств связи и обработки информации (АСУ), геоинформационные технологии	Сетевые, конвергентные технологии, Data Mining, облачные технологии	Технологии виртуализации (SDN, NFV), Mesh-сети, когнитивные сети и системы

Рис. 2. Результаты сопоставления основных этапов развития уровня техники, угроз и обеспечения информационной безопасности ИТКС СН

Соответственно управление и обеспечение безопасности ИТКС СН должно осуществляться с учетом особенностей суперсистемы. В суперсистемах возможно структурное и (или) бесструктурное управление. При структурном способе управления информация передаётся адресно по вполне определённым элементам структуры, сложившейся (или целесообразно сформированной) ещё до начала процесса управления. При бесструктурном способе управления таких, заранее сложившихся, структур нет. Происходит безадресное циркулярное распространение информации в среде, способной к порождению структур из себя при установлении информационно-алгоритмических взаимосвязей между слагающими среду элементами [3].

Таким образом, для исследования проблем обеспечения информационной безопасности ИТКС, обоснования требований, разработки новых методов и технологий управления информационной безопасностью ИТКС СН необходимы исследования процессов в суперсистемах.

Список используемых источников

1. Бударин Э. А., Васюков Д. Ю., Дементьев В. Е., Колбасова Г. С., Краснов В. А., Лепешкин О. М., Лаута О. С., Митрофанов М. В., Худайназаров Ю. К. Обеспечение защиты информации в локальных вычислительных сетях: Военная академия связи им. Маршала Советского Союза С. М. Буденного. СПб., 2013.

2. Репников А. Ю., Стародубцев Ю. И., Худайназаров Ю. К. Контроль защищенности системы связи от радиоэлектронной разведки // Актуальные проблемы защиты и безопасности: Труды XIX Всероссийской научно-практической конференции РАРАН (4–7 апреля 2016 г.). Т. 1. С. 247–254.

3. Достаточно общая теория управления (вторая редакция 2003–2004 гг.). М. : НОУ «Академия управления», 2011. 416 с.

УДК 621.372.543.2

МИКРОПОЛОСКОВЫЙ ПОЛОСНО-ПРОПУСКАЮЩИЙ ФИЛЬТР СО ЗНАЧИТЕЛЬНО СНИЖЕННЫМИ РАЗЕМЕРАМИ

Д. А. Летавин, Д. А. Трифанов

Уральский федеральный университет им. первого Президента России Б. Н. Ельцина

В данной работе был смоделирован и изготовлен микрополосковый фильтр, с идентичными по конструкции треугольными резонаторами. Питание расположено на противоположной стороне подложки от резонаторов. Центральная частота 1790 МГц, а полоса пропускания 10,5 %. Фильтр имеет размеры 16×15×1,5 мм.

микрополосковая линия, резонатор, полосно-пропускающий фильтр.

Введение

Фильтр представляет собой устройство, предназначенное для полезного извлечения сигнала в заданном диапазоне частот. Как известно, полосовые фильтры являются наиболее важными элементами коммуникационных и радиолокационных систем различного измерительного и специального радиооборудования. При создании и изучении новых конструкций частотно-избирательных устройств ы традиционно стараются обеспечить низкий уровень вносимых потерь в полосе пропускания, высокие селективные свойства, миниатюрный дизайн и технологичность. Поиск новых конструкций и методов проектирования, позволяющих обеспечить достижение требуемых параметров, является важным направлением на сегодняшний день.

Цель этой работы – создать фильтр с компактным размерами и селективными свойствами на уровне стандартных конструкций. Для достижения этой цели необходимо разработать трехмерную модель микрополоскового полосового фильтра для проведения электродинамического численного анализа.

Сегодня написано много разных статей по теме микрополосковых фильтров на основе резонаторов [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12]. Однако стоит отметить, что не все предлагаемые конструкции фильтров обеспечивают компактными размерами или технологичностью. В этой статье основное внимание уделяется описанию компактной конструкции фильтра с узкой полосой пропускания.

Проектирование

В этой статье описывается микрополосковый полосовой фильтр на двух идентичных резонаторах. Такие фильтры предназначены для передачи сигнала в пределах диапазона рабочих частот. Фильтр реализуется на подложке из традиционного материала FR-4, с диэлектрической проницаемостью $\varepsilon = 4{,}4$, $\mathrm{tg}\delta = 0{,}02$ и высотой $h = 1{,}5$ мм. Рассмотрим конструкцию с осевой симметрией, реализованную на двух идентичных треугольных резонаторах (рис. 1) и представленную как криволинейный участок линии микрополосковой передачи с общей длиной λw (где λw – длина волны в линии). Питающие микрополосковые линии расположены на противоположной стороне подложки от резонатора.

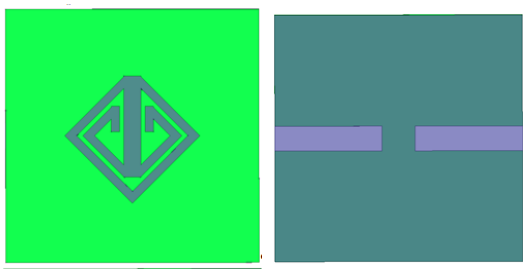


Рис. 1. Топология фильтра

Для того чтобы установить рабочую частоту, необходимо определить требуемый размер резонатора, равный длине волны линии. После этого необходимо найти оптимальное положение микрополосковых линий передачи и их взаимодействие с резонатором, разъеденные диэлектриком. И таким образом мы получаем минимальное коэффициент передачи на центральной частоте и в ее окрестности. Стоит также отметить, что ширина линий микрополосковых каналов выбирается на основе волнового импеданса, который в нашем случае равен 50 Ом.

После настройки фильтра получили ширину полосы пропускания 10,5 % его размеры составляли 15×16 мм. Полоса пропускания измерялась на уровне –3 дБ от уровня минимальных потерь, который составлял –2,1 дБ на центральной частоте 1,79 ГГц полосы передачи. АЧХ (амплитудная частотная характеристика), рассчитанная с помощью электродинамического численного анализа 3D-моделей, представлена на рис. 2, 3.

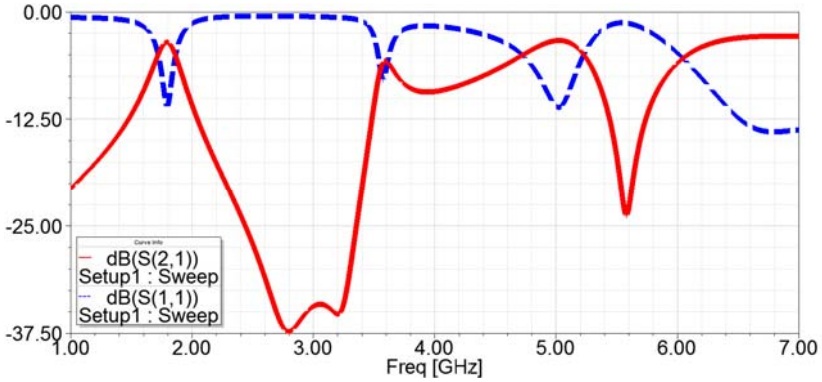


Рис. 2. АЧХ фильтра

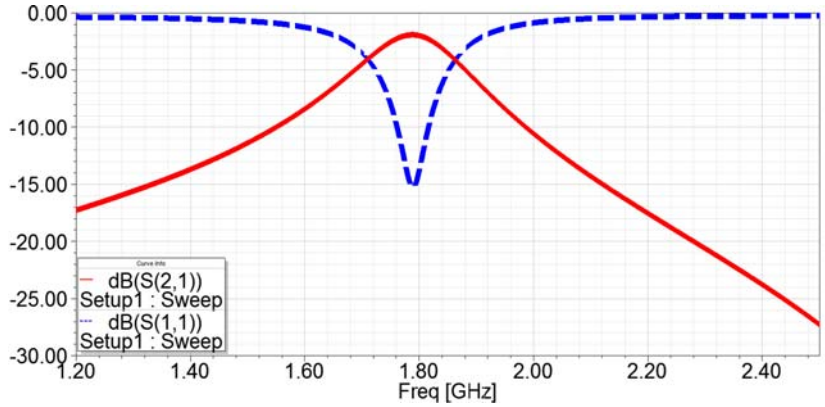


Рис. 3 Фрагмент АЧХ фильтра

На основе результатов численного моделирования видно, что минимальная потери коэффициента передачи в полосе пропускания составляет –1,93 дБ. Рабочий диапазон частот начинается с 1690 МГц и заканчивается на 1879 МГц, что составляет 10,5 % от центральной частоты в относительных величинах. Настройка входного порта (S11) установлена на –18 дБ на центральной частоте 1790 МГц.

Различные типы фильтров с одинаковой центральной частотой и полосой пропускания были разработаны с использованием встроенного инструмента AWR DE iFilter для сравнения их с предлагаемой топологией. Результаты показаны в таблице.

ТАБЛИЦА. Сравнение параметров фильтров

Тип фильтра	Площадь, мм^2	Полоса пропускания (–3 дБ), МГц	Коэффициент передачи, дБ
Hairprin	1208	234	–3,7
Edge coupled	1410	207	–3,4
Shunt stub	1723	201	–3,5
proposed	240	178	–2,3

По результатам моделирования был изготовлен макет (рис. 4), а затем были измерены частотная характеристика с использованием векторного анализатора. Измеренная АЧХ показана на рис. 5.

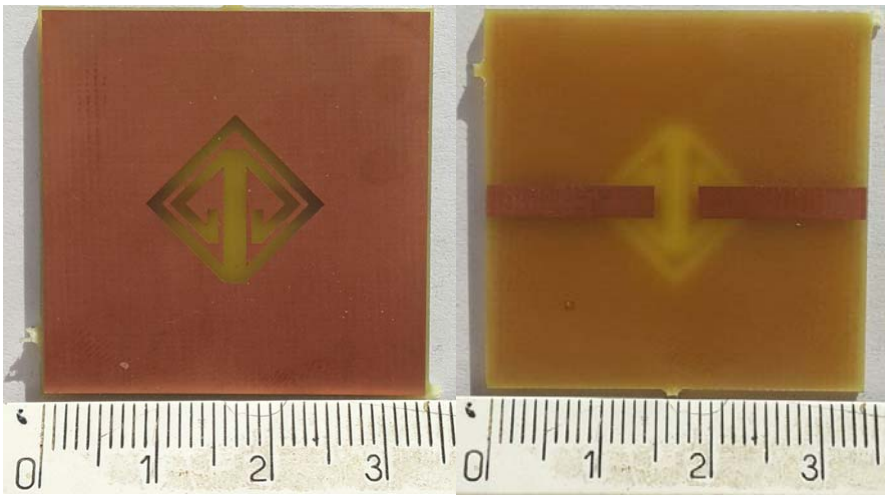


Рис. 4. Макет фильтра

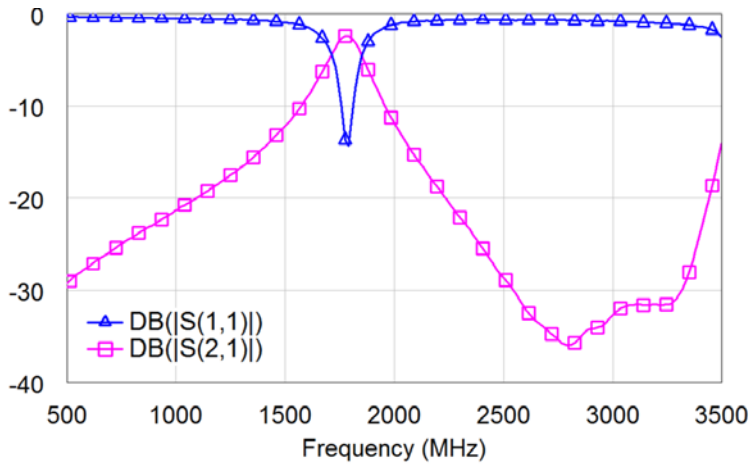


Рис. 5. Измеренная АЧХ макета

Минимальные потери коэффициента передачи в полосе пропускания составляет –2,3 дБ. Рабочий диапазон частот начинается с 1692 МГц и заканчивается на 1870 МГц, что составляет 9,9 % от центральной частоты в относительных величинах. Настройка входного порта (S11) установлена на –15 дБ на центральной частоте 1790 МГц.

Заключение

Таким образом, был разработан оригинальный дизайн микрополоскового полосового фильтра. Эта конструкция отличается миниатюрными размерами, технологичностью и простотой настройки. Для достижения желаемой центральной частоты и минимального коэффициента передачи

на полосе пропускания необходимо найти оптимальную длину резонатора и коэффициент включения входной и выходной микрополосковой линии передачи. С помощью электродинамического анализа 3D-моделей мы разработали и исследовали фильтр с размерами 16×15×1,5 мм с рабочей полосой частот 178 МГц.

Список используемых источников

1. Yang T., Tamura M., Itoh T. Compact hybrid resonator with series and shunt resonances used in miniaturized filters and balun filters // IEEE Transactions on microwave Theory and Techniques. 2010. V. 58. N 2. P. 390–402.

2. Zhu J., Feng Zh. Microstrip interdigital hairprin resonator with an optimal physical length // IEEE Microwave and Wireless Components Letters. 2006. V. 16. N 12. P. 672–674.

3. Hung C.-Y., Weng M.-H., Lan S.-W., Huang C.-Y. // J. Electromagnetic Waves and Applications. 2012. V. 26. P. 12–23.

4. Vegesna S. and Saed M. Compact two-layer microstrip bandpass filter using broadside-coupled resonators // Progress In Electromagnetics Research B, vol. 37, 81–102, 2012.

5. Jia-Qi Liu; Jun-Ye Jin; Li J.L.-W. A Miniature Bandpass filter with split ring resonator and asymmetrical coupled lines // International Conference on Communications, Circuits and Systems. 2013. V. 2. p. 425–427.

6. Rathore V.; Awasthi S.; Biswas A. Design of compact dual-band bandpass filter using frequency transformation and its implementation with Split Ring Resonator Dual-band bandpass filter using SRR // 44th European Microwave Conference. 2014. p. 949–952.

7. Panda A. K.; Sahu K. S.; Mishra R. K. A compact triangular SRR loaded CPW line and its use in highly selective wideband bandpass filter for WiMAX communication system // 5th International Conference on Computers and Devices for Communication. 2012. p. 1–4.

8. Horestani A.K.; Duran-Sindreu M.; Naqui J.; Fumeaux C.; Martin F. Coplanar Waveguides Loaded with S-Shaped Split-Ring Resonators: Modeling and Application to Compact Microwave Filters // IEEE Antennas and Wireless Propagation Letters. 2014. V. 13. p. 1349–1352.

9. Belyaev B. A., Serzhantov A. M., Bal'va Ya. F., Leksikov An. A., Galeev R. G. A new design of a miniature filter on microstrip resonators with an interdigital structure of conductors // Pis'ma v Zhurnal Tekhnicheskoi Fiziki. 2014. V. 41. I. 5. p. 504–507.

10. Hong J. S.; Lancaster M. J. Development of new microstrip pseudo-interdigital bandpass filters // IEEE Microwave and Guided Wave Letters. 1995. V. 5. N. 8. p. 261–263.

11. Chen Y. M., Chang S. F. A compact stepped-impedance pseudo-interdigital bandpass filter with controllable transmission zero and wide stopband range // Microwave Conference. 2009. p. 783–786.

12. Wu S.-R., Hsu K.-W., Tu W.-H. Compact wide-stopband microstrip bandpass filter based on stub-loaded stepped-impedance resonators // IET Microwaves, Antennas & Propagation. 2012. V. 6 N. 13. p. 1422–1428.

Статья представлена кандидатом технических наук института радиоэлектроники и информационных технологий УрФУ И. Н. Корниловым.

УДК 621.372.543.2

МИНИАТЮРНЫЙ ПОЛОСНО-ПРОПУСКАЮЩИЙ ФИЛЬТР В МИКРОПОЛОСКОВОМ ИСПОЛНЕНИИ

Д. А. Летавин, Д. А. Трифанов

Уральский федеральный университет им. первого Президента России Б. Н. Ельцина

В данной работе в программе электродинамического моделирования Ansys HFSS 3D был спроектирован микрополосковый полосно-пропускающий фильтр, работающий на частоте 5,2 ГГц, с полосой 1240 МГц. Данный фильтр реализован на подложке с диэлектрической проводимостью ε = 4,4 и толщиной h = 1,5 мм. Данная топология является технически просто реализуемой.

микрополосковая линия, резонатор, полосно-пропускающий фильтр.

Введение

Как известно, радиосвязь и телекоммуникация являются очень важными сферами радиотехники. Частотно-селективные устройства незаменимы и активно используются в современных радиотехнических системах. В зависимости, от местоположения полосы пропускания, используемые делятся на фильтры нижних частот, полосно-пропускающие, заградительные и высоких частот. Полосовой фильтр является наиболее востребованным среди перечисленных фильтров. Он пропускает сигнал в заданной полосе пропускания и подавляет его на других частотах. При разработке новых фильтров инженеры стараются обеспечить минимальные потери в полосе пропускания, миниатюрность размеров и технологичность. Принимая во внимание совокупность вышеупомянутых требований, мы используем микрополосковые линии передачи, созданные с использованием планарной технологии. Широко известные фильтры (шпилечный, связанных линиях, шлейфах и т. д.) имеют слишком большие размеры и поэтому не могут использоваться для работы в небольших радиотехнических системах. Эта статья предназначена для разработки полосового фильтра с технически реализуемыми и компактными размерами. Чтобы ускорить процесс и улучшить точность проектирования, мы будем использовать программу электродинамического моделирования Ansys HFSS 3D. В настоящее время существует множество технических решений для создания различных микрополосковых полосовых фильтров [1, 2, 3, 4, 5, 6, 7, 8, 9, 10].

Проектирование

В этой статье рассматривается миниатюрный микрополосковой полосовой фильтр, состоящий из двух идентичных резонаторов, представленных линиями в виде меандра, короткозамкнутыми с обоих концов. Вход и выход фильтра расположены с другой стороны подложки, от резонаторов. В зависимости от местоположения этих линий можно получить различный коэффициент передачи. Предлагаемый ППФ расположен на подложке FR-4 с диэлектрической проводимостью ε = 4,4, коэффициентом диэлектрических потерь tgδ = 0,02, толщиной h = 1,5 мм и металлическим слоем t = 35 мкм. Детальная процедура проектирования такого фильтра состоит из следующих этапов:

– разработка модели микрополоскового резонатора;

– отобразить полученную схему резонатора относительно оси;

– спроектировать микрополосковые линии, отвечающие за вход и выход фильтра на другой стороне подложки. Они должны располагаться на одинаковом расстоянии от центра фильтра.

Конструкция резонатора показана на рис. 1. Оба конца линии заземлены на полностью металлизированном слое.

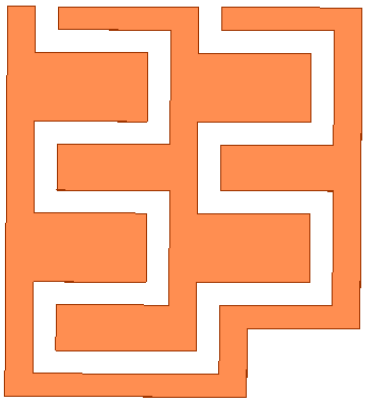


Рис. 1 Конструкция резонатора

Рассмотрим осесимметричную структуру фильтра на двух идентичных резонаторах (рис. 2). Следует отметить, что фильтр имеет диэлектрическую подложку с одной стороной, представляющей полностью заземленное основание, из которого вытравлены резонаторы, а с другой стороны – линии питания. Такое конструктивное решение позволило нам сделать устройство малого размера, потому что линии питания находятся под резонаторами и не приводят к увеличению габаритов фильтра.

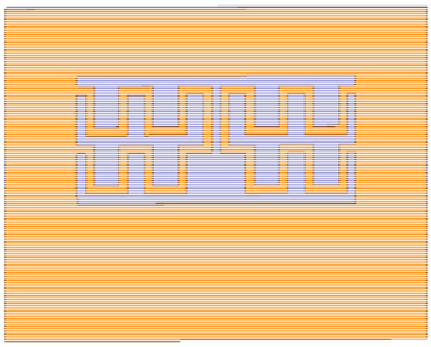


Рис. 2 Топология фильтра

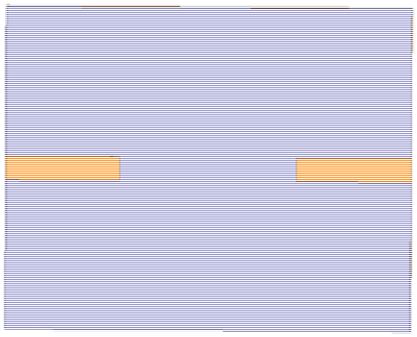


Рис. 3 Линии питания фильтра

После чего подпирается оптимальное расположение линии передачи так, чтобы получить самое низкое значение коэффициентов передачи (см. рис. 3).

Амплитудно-частотная характеристика, полученная в программе, приведена на рис. 4. Следует также отметить, что рабочая полоса будет оценена по уровню –3 дБ от минимального уровня потерь. Площадь разработанного фильтра составляет 50 мм × 40 мм.

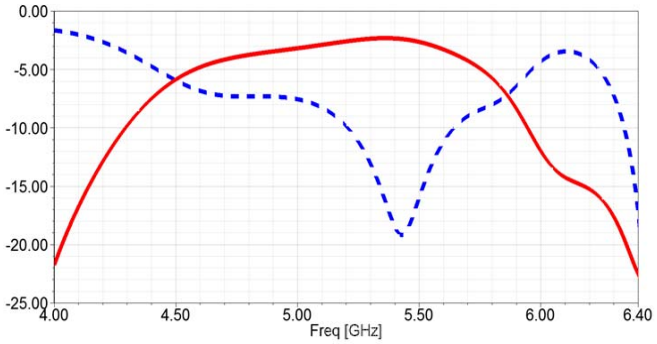


Рис. 4 Амплитудно-частотная характеристкиа фильтра

На основе результатов моделирования можно сказать, что фильтр работает на центральной частоте 5160 МГц. Полоса пропускания начинается с 4540 МГц и заканчивается на 5780 МГц. Относительная полоса пропускания равна 24 %. Минимальное значение коэффициента распространения в полосе пропускания составляет –2,3 дБ. Высокое затухание в полосе пропускания можно объяснить большими потерями в материале подложки (tgδ = 0,02). Коэффициент S11, отвечающий за согласование, составляет –15 дБ на центральной частоте.

Заключение

В этой статье описывается процесс моделирования микрополоскового полосового фильтра, состоящего из двух идентичных резонаторов и двух линий питаний, расположенных на стороне, противоположной резонаторам. Весь процесс проектирования был выполнен с использованием программы электродинамического моделирования Ansys HFSS 3D. Эта программа помогает значительно повысить точность полученных результатов и ускорить процесс проектирования новых частотно-селективных устройств. Изменив положение линий подачи, мы выяснили, что фильтр работает на второй гармонике (5 160 МГц) и имеет полосу пропускания 1240 МГц. Минимальные потери в полосе пропускания составляют –2,3 дБ. Площадь фильтра составляет 2000 мм^2.

Список используемых источников

1. Yang T., Tamura M., Itoh T. Compact hybrid resonator with series and shunt resonances used in miniaturized filters and balun filters // IEEE Transactions on microwave Theory and Techniques. 2010. V. 58. N 2. P. 390–402.

2. Zhu J., Feng Zh. Microstrip interdigital hairprin resonator with an optimal physical length // IEEE Microwave and Wireless Components Letters. 2006. V. 16. N 12. P. 672–674.

3. Hung C.-Y., Weng M.-H., Lan S.-W., Huang C.-Y. // J. Electromagnetic Waves and Applications. 2012. V. 26. P. 12–23.

4. Vegesna S. and Saed M. Compact two-layer microstrip bandpass filter using broadside-coupled resonators // Progress In Electromagnetics Research B, vol. 37, 81–102, 2012.

5. Jia-Qi Liu; Jun-Ye Jin; Li J.L.-W. A Miniature Bandpass filter with split ring resonator and asymmetrical coupled lines // International Conference on Communications, Circuits and Systems. 2013. V. 2. p. 425–427.

6. Rathore V.; Awasthi S.; Biswas A. Design of compact dual-band bandpass filter using frequency transformation and its implementation with Split Ring Resonator Dual-band bandpass filter using SRR // 44th European Microwave Conference. 2014. p. 949–952.

7. Panda A. K.; Sahu K. S.; Mishra R. K. A compact triangular SRR loaded CPW line and its use in highly selective wideband bandpass filter for WiMAX communication system // 5th International Conference on Computers and Devices for Communication. 2012. p. 1–4.

8. Horestani A. K.; Duran-Sindreu M.; Naqui J.; Fumeaux C.; Martin F. Coplanar Waveguides Loaded with S-Shaped Split-Ring Resonators: Modeling and Application to Compact Microwave Filters // IEEE Antennas and Wireless Propagation Letters. 2014. V. 13. p. 1349–1352.

9. Belyaev B. A., Serzhantov A. M., Bal'va Ya. F., Leksikov An. A., Galeev R. G. A new design of a miniature filter on microstrip resonators with an interdigital structure of conductors // Pis'ma v Zhurnal Tekhnicheskoi Fiziki. 2014. V. 41. I. 5. p. 504–507.

10. Hong J. S.; Lancaster M. J. Development of new microstrip pseudo-interdigital bandpass filters // IEEE Microwave and Guided Wave Letters. 1995. V. 5. N. 8. p. 261–263.

Статья представлена кандидатом технических наук института радиоэлектроники и информационных технологий УрФУ И. Н. Корниловым.

УДК 004.7

ПРОАКТИВНОЕ ОБНАРУЖЕНИЕ ВТОРЖЕНИЙ В ОРГАНИЗАЦИИ ЗАЩИТЫ АВТОМАТИЗИРОВАННЫХ СИСТЕМ МЕНЕДЖМЕНТА ИНТЕГРИРОВАННОЙ СТРУКТУРЫ

В. А. Липатников, Б. Ю. Малышев, А. А. Шевченко

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

Перспективным направлением является внедрение автоматизированных систем менеджмента организации интегрированной структуры. Имеет место противоречие между возможностями при перспективных средствах информационного вторжения, включая с кем и каким образом будет осуществляться коммуникация, с одной стороны. С другой стороны, требуется сохранение целостности существующих систем менедж-

мента при планировании и внесении в нее изменений в условиях информационного противоборства. Необходимо разработать способ, при котором документированная информация АСМ ОИС будет находиться под управлением для обеспечения того, чтобы она: a) доступна и пригодна для применения, где и когда она необходима; b) адекватно защищена (от потери конфиденциальности, ненадлежащего использования или потери целостности).

автоматизированная система менеджмента организации интегрированной структуры (АСМ ОИС), информационно-вычислительная сеть (ИВС); компьютерные атаки (КА); защита информации (ЗИ); оценка рисков; контейнерная виртуализация; проактивное управление; масштабирование; показатель защищенности.

В связи с быстрым развитием компьютерных технологий, и переходом к информационному обществу проблема обеспечения информационной безопасности (ИБ) и построения автоматизированных систем менеджмента организации интегрированной структуры (АСМ ОИС) стала одной из наиболее актуальных проблем [1]. На рис. 1 (см. ниже) изображен алгоритм построения и функционирования, рассматриваемой ИВС. Данный алгоритм включает в себя 2 параллельных процесса. Первый процесс представляет собой тестирование ИВС и выявление уязвимостей, разработанный на основе патента Российской Федерации [2]. Второй процесс представляет собой анализ цифрового потока (ЦП) с выявлением аномалий и последующим анализом динамики действий нарушителя, аналогом данного процесса является метод, представленный в источнике [3]. На основании динамики действий нарушителя строится модель угроз и принимаются меры по защите. Данный метод помогает защитить реальную информационную систему (ИС) от компьютерных атак (КА), за счет принятия рациональных мер по защите реальных и возможных уязвимостей в данной сети.

В ходе выявления в журнале регистрации аномальных событий действия нарушителя блокируются с оповещением администратора. На рис. 2 изображен граф событий действий нарушителя.

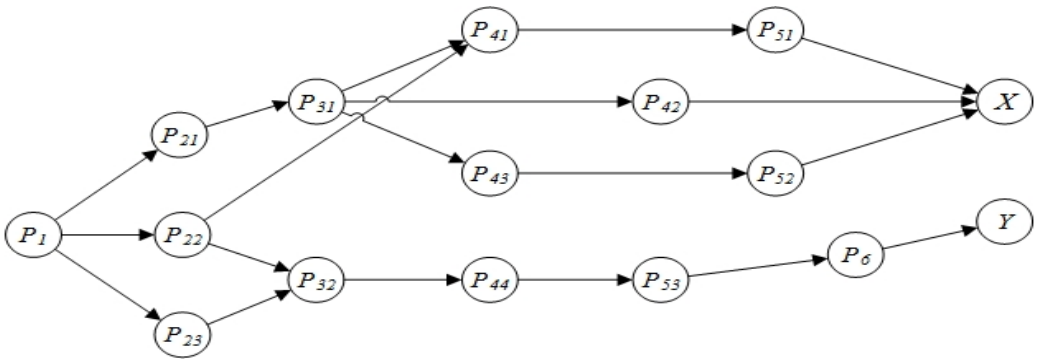


Рис. 2. Граф событий действий нарушителя

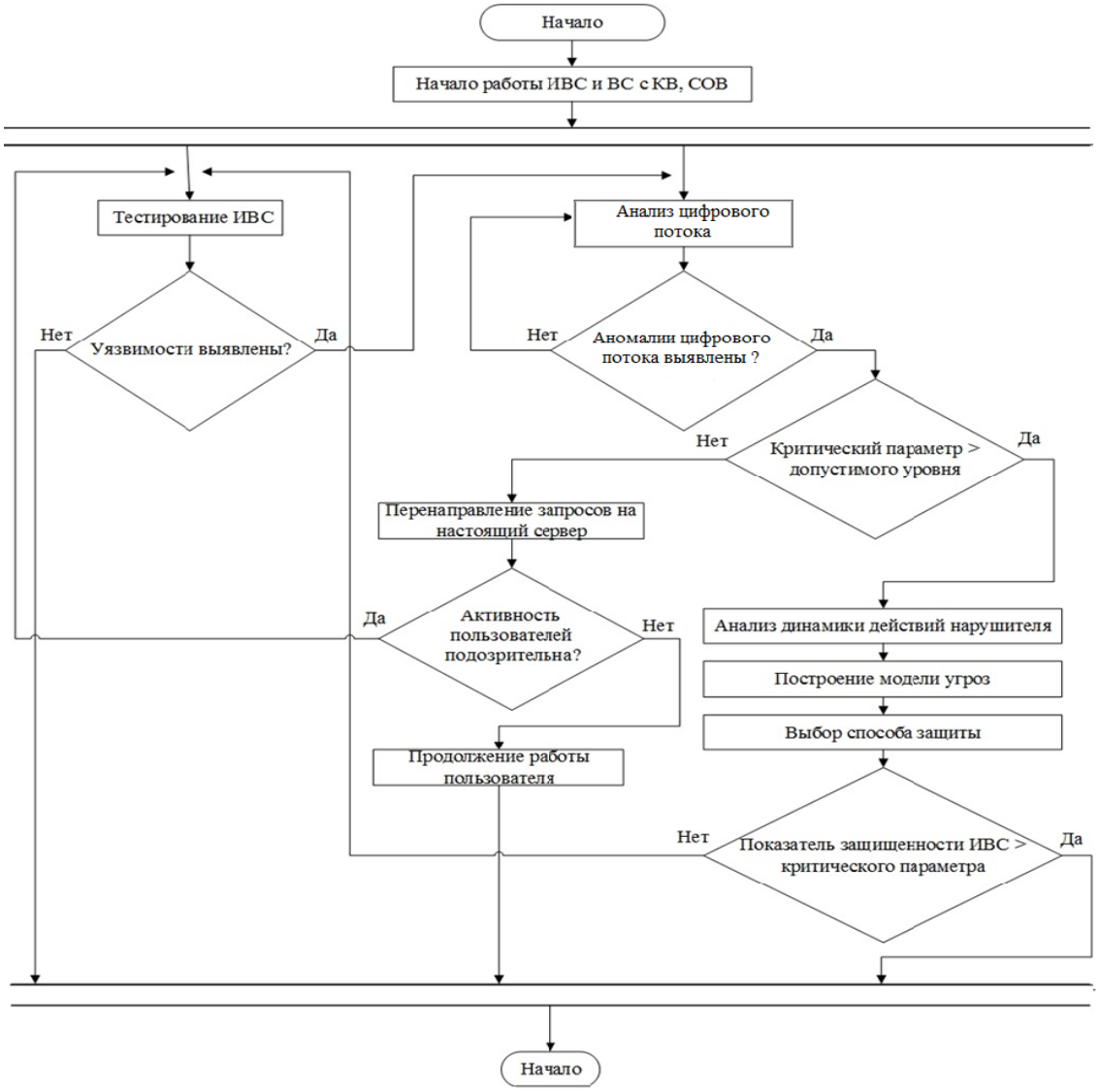


Рис. 1. Обобщенный алгоритм функционирования ИВС

В качестве одной из возможных моделей можно использовать представление действия нарушителя как систему с переменной структурой, поведение которой на случайных интервалах времени характеризуется различными структурами и описывается вероятностными законами.

Состояние «P_1» соответствует началу действий нарушителя. Состояние «P_{21}» соответствует событию, в котором происходит измерение характеристик ИВС путем внедрения снифера. Состояние «P_{22}» соответствует стадии, в которой проводится тестирование состояния ИВС путем анализа запросов. Состояние «P_{23}» соответствует событию анализа «эхо-запросов». Состояние «P_{31}» соответствует событию анализа исходящего цифрового потока. Состояние «P_{32}» соответствует событию выявление хостов. Состояние «P_{41}» соответствует событию выявления паролей. Состояние «P_{42}» соответствует со-

бытию дешифрования информации. Состояние «P_{43}» соответствует событию несанкционированного использования IP адреса в сети. Состояние «P_{44}» соответствует событию сканирования портов. Состояние «P_{51}» соответствует событию подмены пользователя в сети. Состояние «P_{52}» соответствует событию изменения целостности, доступности и конфиденциальности информации. Состояние «P_{53}» соответствует событию анализа характеристик приложений. Состояние «P_6» соответствует режиму осуществления DDoS атак. Состояние «X» соответствует реализации угрозы хищения информации. Состояние «$У$» соответствует реализации отказа в обслуживании. Определим коэффициенты реализуемости событий (элементов графа), воспользовавшись методикой [4]:

$$P = \frac{(У_1 + У_2)}{20},$$

где $У_1$ – коэффициент исходной защищенности; $У_2$ – коэффициент реализации угрозы.

Время перехода из одного события в другое, зависит от коэффициента реализуемости события:

$$T_i = T_{maxj} - P_i \times T_{исхij},$$

где T_{maxj} –максимальное времяреализации j-го события (T_{maxj} = 24 часа); P_i – коэффициент реализуемости i-го события; $T_{исхij}$ – исходное время перехода из i-го события в j-е событие ($T_{исхij}$от 0 до 24 часа).

Для определения наиболее вероятного пути реализации угроз необходимо рассчитать вероятности наступления каждого из событий в графе. Поэтому воспользуемся формулой:

$$P = P_{(i)} + P_{(i+1)} - (P_{(i)} \times P_{(i+1)}),$$

где $P_{(i)}$, $P_{(i+1)}$ – вероятность наступления двух последующих событий.

Рассмотрим действие способа адаптивного управления защитой ИВС на основе анализа динамики действий нарушителя на примере защиты от угрозы хищения информации по пути реализации P_{x1}. Оно представлено в таблице.

При использовании адаптивного способа защиты ИВС нарушитель потратит на 7 % больше времени на реализацию угрозы хищения информации, чем при использовании традиционного способа управления защитой ИВС, что и является положительным эффектом предлагаемого способа защиты ИВС на основе анализа динамики действий нарушителя.

ТАБЛИЦА. Сравнение адаптивного и традиционного управления защитой ИВС

Событие	Коэффициент реализуемости события		Время перехода одного события в другое, ч.	
	Адаптивный способ управления защитой ИВС	Традиционный способ управления защитой ИВС	Адаптивный способ управления защитой ИВС	Традиционный способ управления защитой ИВС
P_1	0,8	0,8	14,4	14,4
P_{21}	0,8	0,9	12,5	12,5
P_{31}	0,8	0,9	11	12,8
P_{41}	0,8	0,8	15,2	13,8
P_{51}	0,9	0,9	10,4	11,6
X	0,4	0,9	19,9	13,6
Время реализации угрозы			83,4	78,7

На рис. 3 представлена зависимость вероятности реализации угрозы и вероятности защищенности ИВС от времени для реализации способа адаптивного управления защитой ИВС на основе анализа динамики действий нарушителя.

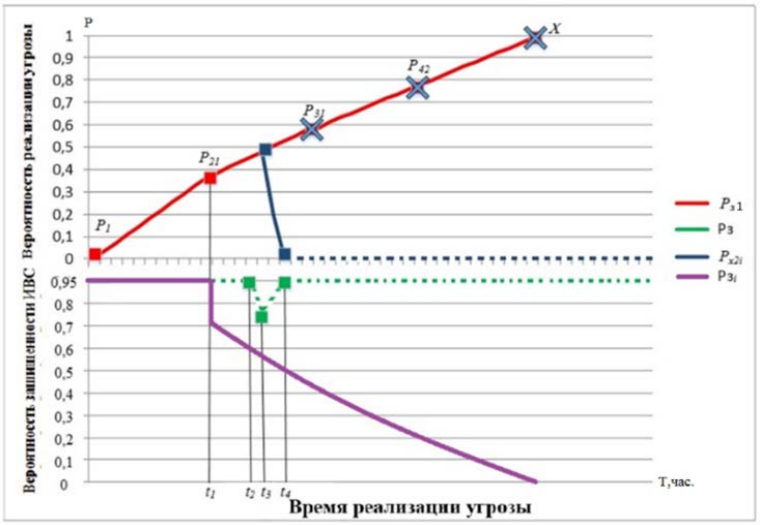


Рис. 3. Зависимости вероятности реализации угрозы и вероятности защищенности ИВС от времени при реализации способа адаптивного управления защитой с анализом динамики действий нарушителя

На рис. 3 P_{x1} – последовательность действий нарушителя для реализации угрозы X; $P_з$ – уровень ИБ ИВС, t_1, t_2, t_3, t_4 – время, $P_{зi}$ – график зависимости защищенности ИВС от вероятности реализации угрозы, P_{x2i}–зависимость действий нарушителя от принятых мер защиты.

В промежуток времени t_1 происходит внедрение снифера. В момент времени t_2 происходит обнаружение данного воздействия, при этом уровень защищенности падает. В дальнейшем происходит построение модели угроз. Затем принимаются меры по нейтрализации угрозы, которая была обнаружена с принятием актуальных мер защиты объектов ИВС, которые будут атакованы нарушителем в ближайшее время, согласно графу действий нарушителя. После принятия в момент t_4 мер защиты, реализация следующего воздействия нарушителя P_{31} уже невозможна, в силу снижения вероятности реализации угрозы к нулю, защищенность вернется на уровень в 95%.

Заключение. Разработан способ адаптивного управления защитой ИВС АСМ ОИС, отличающийся от известных, основанных на использовании специальных мер защиты, тем, что предложено применять результаты анализа динамики действий нарушителя. Предусмотрен алгоритм контроля ситуационных параметров во взаимной противоборствующей обстановке при стохастической неопределенности. Этот подход возможно реализовать на программной эмуляции компонентов ИС введения нарушителя в заблуждение:

1) сегмента сети – где производится эмулирование работы ВС с КВ (дубликат сети с рабочими серверами);

2) дубликата хоста рабочих серверов (хост-приманка);

3) дубликат сервисов и приложений – программы, которые копируют работу сервисов и приложений.

Список используемых источников

1. Липатников В. А., Шевченко А. А. Способ контроля уязвимостей при масштабировании автоматизированной системы менеджмента предприятия интегрированной структуры // Информационные системы и технологии. 2016. №2(94). С. 128–140.

2. Карганов В. В., Костарев С. В., Липатников В. А., Лобашев А. И., Шевченко А. А. Способ защиты информационно-вычислительной сети от несанкционированных воздействий. Патент 2635256 Российская Федерация; заявитель и патентообладатель Военная академия связи имени Маршала Советского Союза С. М. Буденного; заявл. 04.05.2016; опубл. 09.11.2017.

3. Липатников В. А., Шевченко А. А., Яцкин А. Д. Метод управления безопасностью информационно-вычислительных сетей на основе выделенного сервера с контейнерной виртуализацией // Информационные системы и технологии. 2017. № 4 (102). С 116-126

4. Плетнев П. В., Белов В. М. Методика оценки рисков информационной безопасности на предприятиях малого и среднего бизнеса // Доклады Томского государственного университета систем управления и радиоэлектроники. 2012. Т. 1. № 2. С. 83–86.

УДК 004;621.398;681

МОДЕЛЬ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ РАСПРЕДЕЛЕННОЙ ИНФОРМАЦИОННОЙ СЕТИ НА ОСНОВЕ КОНТРОЛЯ ЗА УЯЗВИМОСТЯМИ

В. А. Липатников, А. А. Шевченко

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

В статье изложена модель системы защиты информации распределенной информационной сеть на основе контроля за уязвимостями. Модель учитывает параметры процесса атак и защиты, а также внутренние и внешние факторы, влияющие на состояние сети. Предложена общая структура модели, которая в отличие от известных представляет собой совокупность модулей, выполняющих постоянное сканирование на факт появления новых уязвимостей и одновременное функционирование виртуальной сети, которая позволит более точно выявлять и достоверно оценивать уязвимость за счёт своевременной регистрации и анализа реальных попыток компьютерных атак. Комплекс данных модулей выполняет основную функцию повышения информационной безопасности на основе выявления и анализа уязвимостей.

распределенная информационная сеть, информационная безопасность, компьютерная атака, показатель защищённости, выявление и оценка уязвимостей, оценка рисков, вероятностный граф.

Под распределенной информационной сетью (РИС) понимают программно-аппаратную сеть, предназначенную для автоматизации целенаправленной деятельности конечных пользователей и обеспечивающую, в соответствии с заложенной в нее логикой, возможность получения, модификации и хранения информации. В современной РИС появляется большое количество уязвимостей из-за масштабирования структуры. Предполагается, что активный злоумышленник может определять за короткое время уязвимости после их появления.

Модель должна позволить определить закономерности процессов выявления «узких мест», отказов программного и аппаратного оборудования. Необходимо предусмотреть внедрение принципов управления рисками в данную модель для обеспечения уверенности в повышении уровня ИБ РИС.

Постановка задачи

Разработать модель системы защиты информации (СЗИ) РИС с учетом выявления и оценки уязвимостей, объема выделенных ресурсов, видов потенциальных компьютерных атак (КА), цены потери при реализации уязвимости, возможностей управляющих воздействий на СЗИ.

Решение

Для решения поставленной задачи предлагается следующая общая структура модели СЗИ РИС, представленной на рис. 1.

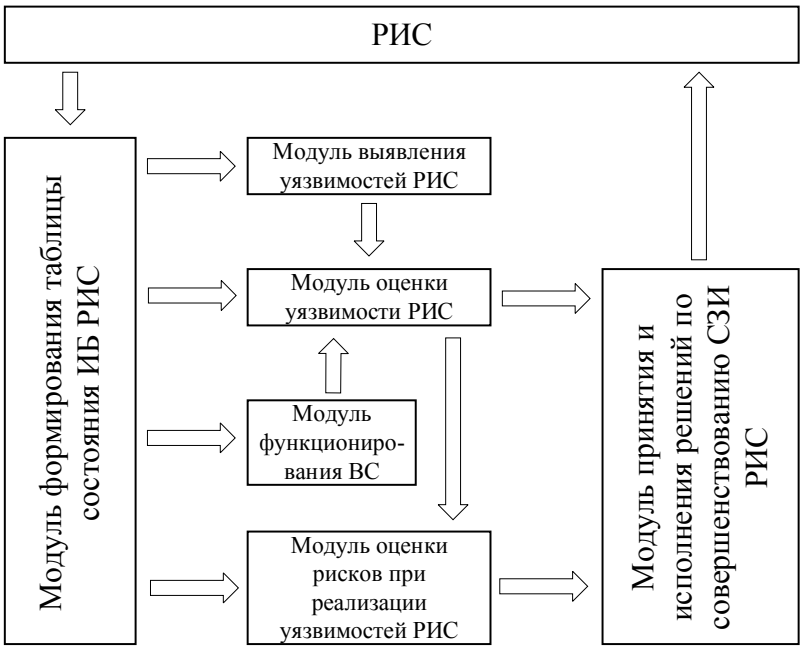


Рис. 1. Общая структура модели СЗИ РИС

Модель СЗИ РИС представляет собой совокупность модулей. Алгоритм работы модели СЗИ РИС представлен на рис. 2. Модуль формирования таблицы состояния ИБ РИС составлен аналогично процессу идентификации объектов в [1]. Модуль функционирования виртуальной сети (ВС) разработан на основе [2, 3], который позволит более достоверно выявлять и оценивать уязвимость за счёт своевременной регистрации и анализа реальных попыток проникновения злоумышленника в РИС. Модуль выявления уязвимостей РИС составлен аналогично патенту Российской Федерации [4]. Модуль оценки уязвимости РИС и модуль оценки рисков при реализации уязвимостей разработаны на основе программного обеспечения [5]. Модуль принятия и исполнения решений по совершенствованию СЗИ РИС.

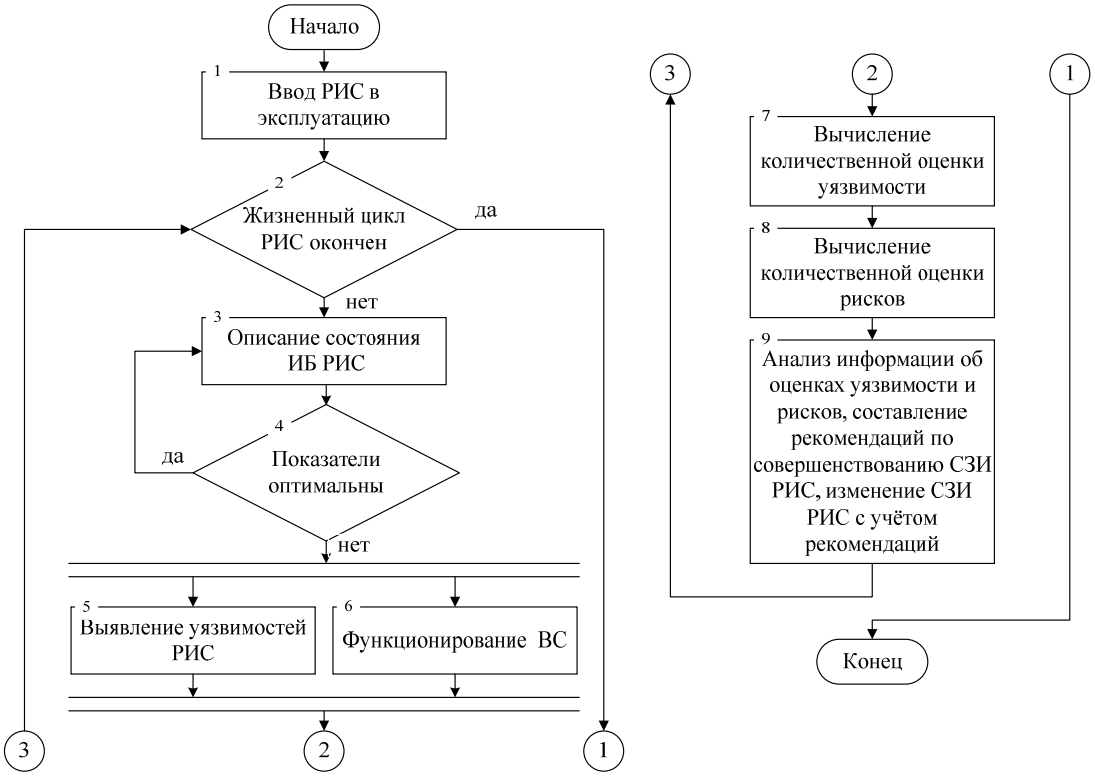


Рис. 2. Алгоритм работы модели СЗИ РИС

Практическая значимость

Для удобства анализа модели СЗИ РИС составляется вероятностный граф перехода РИС из одного состояния в другое вовремя работы СЗИ по алгоритму, представленному на рис. 2. В результате получается вероятностный граф, показанный на рис. 3. Вероятностный граф используется для получения производящей функции, соответствующей переходу РИС из начального состояния в конечное.

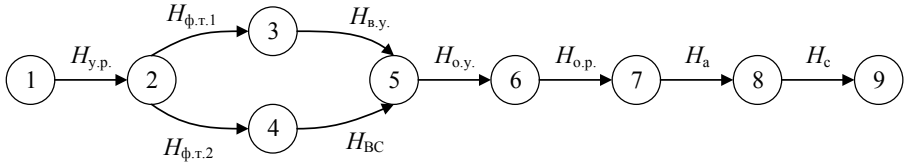


Рис. 3. Вероятностный граф перехода РИС из одного состояния в другое вовремя работы СЗИ

На рис. 3 «1» – состояние функционирования РИС после успешного ввода в эксплуатацию; «2» – состояние РИС, в котором происходит формирование таблицы состояния ИБ РИС; «3» – состояние, в котором происходит выявление уязвимостей; «4» – состояние функционирования ВС; «5» – состояние, в котором происходит количественная оценка уязвимости РИС; «6» – состояние, в котором происходит количественное оценивание рисков

с учётом оценки уязвимости РИС; «7» – состояние, в котором проводится анализ всей информации, полученной после оценки уязвимости РИС и рисков; «8» – состояние, в котором происходит совершенствования СЗИ по составленным рекомендациям, «состояние 9» –состояние функционирования РИС после изменения СЗИ.

Производящая функция для этого графа имеет вид:

$$H_{ИБ} = H_{у.р.} \cdot (H_{ф.т.1} \cdot H_{в.у.} \cdot H_{ф.т..2} \cdot H_{ВС} + H_{ф.т.1} \cdot H_{в.у.} + H_{ф.т..2} \cdot H_{ВС}) \cdot H_{о.у.} \cdot H_{о.р.} \cdot H_{а} \cdot H_{с},$$

где $H_{у} = p_{у} \cdot x^{T_{у}}$, где $p_{у}$ – вероятность перехода из одного состояния в другое, а $T_{у}$ – время, необходимое для перехода из одного состояния в другое.

Показатель защищённости РИС согласно графу состояний, определяется в виде:

$$P_{ИБ} = H_{ИБ}(x = 1) =$$
$$= p_{у.р.} \cdot (p_{ф.т.1} \cdot p_{в.у.} \cdot p_{ф.т..2} \cdot p_{ВС} + p_{ф.т.1} \cdot p_{в.у.} + p_{ф.т..2} \cdot p_{ВС}) \cdot p_{о.у.} \cdot p_{о.р.} \cdot p_{а} \cdot p_{с}.$$

Вероятность перехода из одного состояния в другое зависит от пропускной способности канала связи (скорости передачи данных (ПД)) и, являясь случайной величиной, распределяется по нормальному закону.

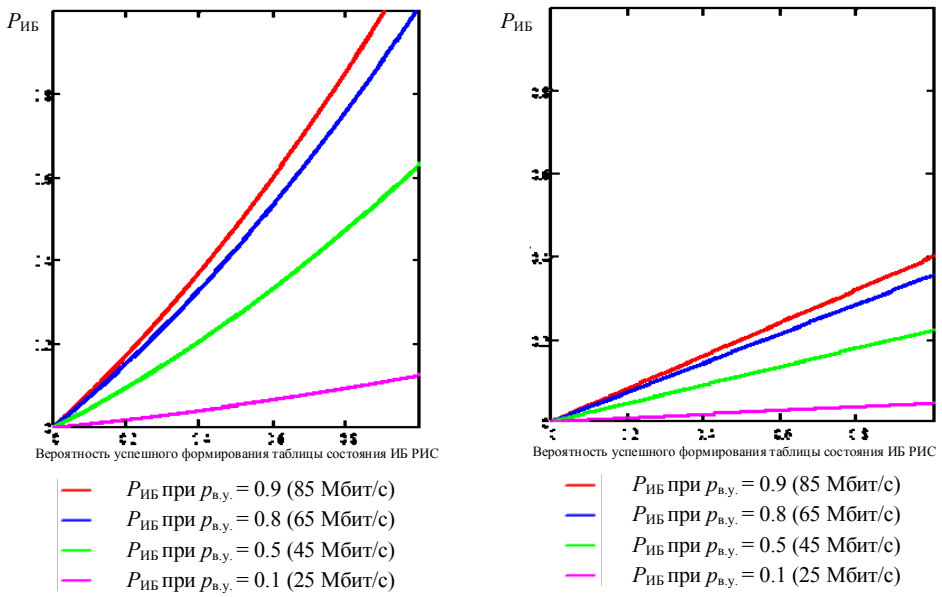
ТАБЛИЦА. Исходные данные моделирования зависимости показателя защищённости РИС от влияния различной пропускной способности канала связи и неполного функционирования РИС в конкретный момент времени

Фактор	Скорость ПД в РИС и $p_{у}$	Вероятность того, что выявление уязвимостей РИС прошло успешно, $p_{в.у.}$	Вероятность успешной регистрации реальных КА, $p_{ВС}$
Различная пропускная способность канала связи	70–80 Мбит/с, $p_{у}$ = 0,85	0,9 (при 85 Мбит/с) 0,8 (при 65 Мбит/с) 0,5 (при 45 Мбит/с) 0,1 (при 25 Мбит/с)	1
Неполное функционирование РИС в конкретный момент времени			0

Графики зависимости показателя защищённости РИС полученные в результате использования разработанной модели СЗИ РИС представлены на рис. 3.

Из рис. 3*а* видно, что со снижением скорости ПД между узлами РИС показатель защищённости падает. Поэтому следует вывод, что, исходя из того какие именно каналы связи, сетевое оборудование, технологии, стандарты ПД и физический интерфейс используются для создания РИС, нужно рассчитывать время на формирование таблицы состояния ИБ РИС.

Сравнивая графики рисунков 3*а* и 3*б*, можно сделать вывод, что при использовании либо модуля выявления уязвимостей РИС, либо модуля функционирования ВС, необходима безотказная работа модуля описания состояния ИБ РИС. Следовательно, необходимо обеспечивать работу всех модулей модели СЗИ РИС за счёт постоянного контроля над функционированием модулей.



а) б)

Рис. 3. Графики зависимости показателя защищённости РИС (вероятности защиты РИС) вследствие: а) различной пропускной способности канала связи; б) неполного функционирования сети в конкретный момент времени

Заключение

Модель СЗИ РИС на основе контроля за уязвимостями обеспечивает защиту РИС в зависимости от различных факторов, влияющих на ИБ РИС, что позволяет повысить ИБ РИС.

Разработанная модель позволяет наглядно показать зависимость показателя защищённости РИС от факторов, влияющих на ИБ РИС. Приведённые выше частные модели показывают, что при скорости ПД меньше 65 Мбит/с и при работе одного из двух модулей, обеспечивающих выявление уязвимостей РИС или функционирование ВС, показатель защищённости РИС будет находиться ниже 0,95. Это подтверждает, что низкая скорость ПД и неполное функционирование сети являются одними из важных факторов, влияющих на ИБ РИС.

Выводы, сделанные на основе полученных зависимостей, совпадают с реальными фактами влияния вышеуказанных факторов на быстродействие

и корректность работы сети или системы в целом, что доказывает адекватность и эффективность разработанной модели.

Список используемых источников

1. Кузнецов И. А., Липатников В. А., Шевченко А. А. Способ многофакторного управления безопасностью информационно-телекоммуникационной сети системы менеджмента качества предприятий интегрированных структур // Вопросы радиоэлектроники. 2016. № 6. С. 23–28.

2. 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. № 4 (89). С. 67–76.

3. Костарев С. В., Липатников В. А., Шевченко А. А., Яцкин А. Д. Программа управления виртуальной сетью. Свидетельство о государственной регистрации программы для ЭВМ №2017662876; заявитель и правообладатель Военная академия связи имени Маршала Советского Союза С. М. Буденного. – №2017615768; заявл. 19.06.2017; опубл. 17.11.2017.

4. Карганов В. В., Костарев С. В., Липатников В. А., Лобашев А. И., Шевченко А. А. Способ защиты информационно-вычислительной сети от несанкционированных воздействий. Пат. 2635256 Российская Федерация; заявитель и патентообладатель Военная академия связи имени Маршала Советского Союза С.М. Буденного. – № 2016117662; заявл. 04.05.2016; опубл. 09.11.2017.

5. Костарев С. В., Карганов В. В., Липатников В. А., Шевченко А. А. Многоуровневая количественная оценка уязвимости информационно-вычислительной сети. Свидетельство о государственной регистрации программы для ЭВМ №216611634; заявитель и правообладатель Военная академия связи имени Маршала Советского Союза С. М. Буденного. – №2015662272; заявл. 15.12.2015; опубл. 08.02.2016.

УДК 621.395.741

АНАЛИТИЧЕСКОЕ ОПИСАНИЕ МЕТОДА ОБНАРУЖЕНИЯ ЗАМКНУТЫХ ПЕТЕЛЬ В СЕТЯХ ТАКТОВОЙ СЕТЕВОЙ СИНХРОНИЗАЦИИ

М. В. Лобастова, А. Ю. Матюхин

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

Рассматриваются основные проблемы в сетях ТСС. Приводится аналитическое описание метода обнаружения замкнутых петель в сетях синхронизации. Обсуждаются вопросы вычислительной сложности предлагаемого алгоритма.

тактовая сетевая синхронизация, петли в сети синхронизации, матрица смежности.

Цифровые сети связи не могут работать эффективно без тактовой сетевой синхронизации [1]. Одним из требований, предъявляемых к сетям ТСС, является отсутствие петель в сети синхронизации [2].

Предложенный метод обнаружения петель основывается на анализе матрицы смежности графа сети. Наличие связей между узлами графа в матрице смежности обозначено единицами, отсутствие – нулями [3].

Можно сказать, что элементы сети, которым соответствуют нулевые строки или столбцы матрицы, не могут участвовать в петлях.

Воспользуемся одним из элементарных преобразований матрицы, а именно сложением элементов строки (столбца) матрицы.

При сложении элементов всех строк получится матрица строка размерности $1\times n$: $[a_{11}\ a_{12}\ a_{13}\ \dots\ a_{1n}]$ [4]. Так как связи в исходной матрице обозначены единицами, то каждый из элементов полученной матрицы строки будет показывать, от какого числа узлов может получать сигнал синхронизации данный узел.

При сложении элементов всех столбцов получится матрица столбец размерности $n\times 1$:

$$\begin{bmatrix} a_{11} \\ a_{21} \\ a_{31} \\ . \\ . \\ . \\ a_{n1} \end{bmatrix}.$$

Можно сказать, что каждый из элементов полученной матрицы столбца будет указывать, какое число узлов синхронизируется от данного узла.

В том случае, когда матрица смежности имеет нулевой столбец, при сложении элементов строк один из элементов полученной матрицы строки окажется нулевым. Это означает, что узел, которому соответствует данный нулевой элемент, не синхронизируется ни одним из других узлов. А значит, этот элемент можно исключить из сети, так как в петле он участвовать не может.

Если же исходная матрица имеет нулевую строку, то при сложении всех элементов столбцов, один из элементов полученной матрицы столбца окажется нулевым [5]. Это означает, что соответствующий данному элементу узел не синхронизирует ни один из элементов сети. И его также можно исключить из рассмотрения.

Исключение элемента из сети приведет к тому, что размерность матрицы уменьшится. А также уменьшится число связей в сети. В результате какие-то строки или столбцы новой полученной матрицы смежности могут

оказаться нулевыми. Значит, из сети можно будет исключить новые элементы, не участвующие в петлях.

В том случае, если в матрице строке и матрице столбце нет нулевых элементов, то можно сказать, что в сети есть петли (петля).

Рассмотрим пример. Пусть задана некоторая сеть, включающая шесть узлов (рис.).

Составим для графа этой сети матрицу смежности.

$$\begin{array}{c} \\ A \\ B \\ C \\ D \\ E \\ F \end{array} \begin{array}{c} \begin{array}{cccccc} A & B & C & D & E & F \end{array} \\ \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix} \end{array}$$

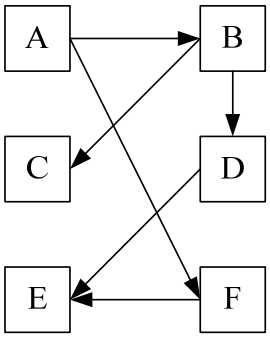


Рисунок. Граф сети синхронизации

Полученная матрица смежности содержит шесть единиц, что равно числу связей в графе. Сложив строки данной матрицы, получим матрицу строку:

$$\begin{array}{cccccc} A & B & C & D & E & F \\ \begin{bmatrix} 0 & 1 & 1 & 1 & 2 & 1 \end{bmatrix}. \end{array}$$

Сложив столбцы матрицы смежности, получим матрицу столбец:

$$\begin{array}{c} \\ A \\ B \\ C \\ D \\ E \\ F \end{array} \begin{bmatrix} 2 \\ 2 \\ 0 \\ 1 \\ 0 \\ 1 \end{bmatrix}$$

Опираясь на вышеприведенное заключение, можно сказать, что в петлях не будут участвовать узлы A, C и E.

Удалим из первоначальной матрицы смежности первый столбец и первую строку, соответствующие узлу A, и составим новую матрицу смежности:

$$\begin{array}{c} \\ B \\ C \\ D \\ E \\ F \end{array} \begin{array}{c} \begin{array}{ccccc} B & C & D & E & F \end{array} \\ \begin{bmatrix} 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix} \end{array}$$

Получим новые матрицы строку и столбец.

$$\begin{matrix} & B & C & D & E & F \end{matrix}$$
$$\begin{bmatrix} 0 & 1 & 1 & 2 & 0 \end{bmatrix}$$ – матрица строка.

$$\begin{matrix} B \\ C \\ D \\ E \\ F \end{matrix} \begin{bmatrix} 2 \\ 0 \\ 1 \\ 0 \\ 1 \end{bmatrix}$$ – матрица столбец.

Глядя на эти матрицы можно сказать, что узлы B, C, E и F не участвуют в петлях. А один узел D также не может образовывать петлю.

Данный метод обнаружения петель проще метода, основанного на возведении матрицы смежности графа сети в степень равную ее порядку.

Сложение элементов строки матрицы смежности эквивалентно умножению матрицы смежности на единичный вектор строку того же порядка. Сложение элементов столбцов матрицы смежности эквивалентно умножению на единичный вектор столбец того же порядка [5].

Для умножения матрицы размерности n на вектор необходимо произвести n^2 операций умножения и $n(n–1)$ операций сложения [4]. Так как для предложенного метода нужно рассчитать два вектора, то число математических операций увеличится вдвое, т.е. число операций умножения составит $2n^2$, а число операций умножения составит $2n(n–1)$.

При использовании метода основанного на возведении матрицы смежности графа сети в степень, равную ее порядку, число операций умножения достигнет n^4, а число операций сложения составит $n^3(n–1)$.

Важно отметить, что данный способ указывает лишь на наличие петель в сети, но не позволяет определить количество петель и их конфигурацию.

Список используемых источников

1. Давыдкин П. Н., Колтунов М. Н., Рыжков А. В. Тактовая сетевая синхронизация / Под ред. М. Н. Колтунова. М. : Эко-Трендз, 2004. 205 с.

2. Слепов Н. Н. Синхронизация цифровых сетей. Методы, терминология, аппаратура // Электроника: наука, технология, бизнес. 2002. № 2. С. 24–29.

3. Лобастова М. В. Анализ системы синхронизации сети SDH // Первая миля. 2014. № 3 (42). С. 66–71.

4. Корн Г., Корн Т. Справочник по математике для научных работников и инженеров. СПб. : Лань, 2003. 831 с.

5. Справочник по высшей математике / А. А. Гусак, Г. М. Гусак, Е. А. Бричикова. Мн. : ТетраСистемс, 2009. 640 с.

УДК 004.4:004.7

ИСПОЛЬЗОВАНИЕ OPENFLOW КАК РЕШЕНИЯ ДЛЯ ПОСТАВЩИКОВ УСЛУГ VPN

Н. О. Лоханько, И. А. Ушаков, В. С. Чехутский

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

BGP / MPLS IP VPN и VPLS широко используются в сетях IP / MPLS для подключения удаленных клиентов. Однако поставщики услуг борются с множеством проблем для предоставления этих услуг. Сложность управления, стоимость оборудования и, что не менее важно, проблемы масштабируемости возникающие по мере увеличения числа клиентов – это лишь некоторые из проблем. Программно-конфигурируемые сети возникающая парадигма, которая может решить вышеупомянутые проблемы, используя логически централизованный контроллер для управления сетевыми устройствами.

Решение на основе SDN значительно снижает сложность определения служб VPN и управления. Данный метод устраняет сложные и дорогостоящие взаимодействия устройств.

программно-конфигурируемые сети, масштабирование, VPN, SND.

Услуги VPN относятся к числу важных услуги поставщиков услуг операторского класса (SP). Эти услуги предоставляются для многих клиентов и направлены на подключение географически распределенные клиентов. Поскольку IP / MPLS доминирует в ядре сетей операторского класса, услуги VPN реализуются с использованием MPLS. L3VPN для клиентов обычно предоставляется через «BGP / MPLS IP VPN «(также называемый MPLS VPN)» VPLS является наиболее известная услуга предоставления VPN уровня 2 через MPLS сеть [1, 2]. В этой архитектуре сеть поставщика услуг разделена на две части: область ядра и граница. На границе, сеть провайдера подключается к сети пользователя через PE-устройства. В целом, ядро сети состоит из маршрутизаторов, использующих технологию MPLS для пересылки трафика между PE-устройствами и CE-устройствами клиента, подключенными к провайдеру. На рис. 1 представлено стандартное построение сети MPLS.

Основные проблемы, связанные с работой MPLS VPN:

– *Сложность управления.* Услуги MPLS VPN и VPLS создают серьезные трудности с управлением для поставщиков услуг. Распределенная архитектура управляющей плоскости вызывает сложность конфигурации сети. В результате операторы должны освоить сложный и трудоемкий про-

цесс настройки VPN для обеспечения и поддержки многих клиентов. Особенно эти проблемы усиливаются в среде с несколькими производителями оборудования.

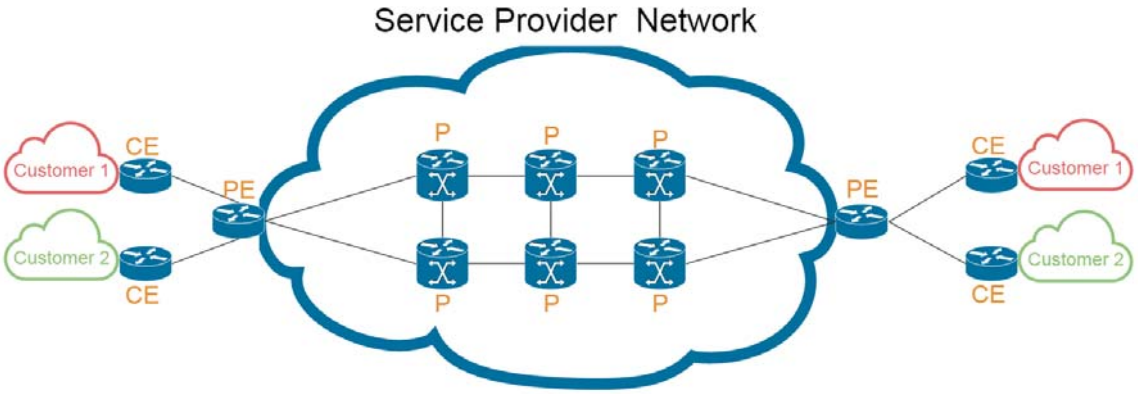


Рис. 1. Схема построения сети MPLS

– *Дороговизна оборудования.* Поскольку в текущей архитектуре плоскости управления и данных интегрированы, значительное количество функций управления должно быть реализовано в устройствах PE (например, MP-BGP, LDP, IS-IS). Кроме того, многочисленные IP-префиксы клиентов (в MPLS VPN) и MAC-адреса (в VPLS) должны поддерживаться с помощью PE-устройств [1, 2]. Как следствие, сеть требует дорогостоящих и высокопроизводительных маршрутизаторов (например, Cisco 7600 series). Использование многих из этих устройств не экономичное решение для поставщиков услуг в отношении растущего числа клиентов и их чрезмерных потребностей в PE-устройствах.

– *Масштабируемость.* В настоящее время поставщики MPLS VPN и VPLS сталкиваются с серьезными проблемами масштабируемости. Например, устройства PE обеспечивают ограниченное количество памяти для хранения MAC-адресов и IP-префиксов многочисленных клиентов. Кроме того, управляющие функции (например, MP-BGP для MPLS VPN и поддержания полного сетка псевдопроводников среди PE для VPLS) составляют высокую нагрузку на устройства, особенно, когда количество PE-устройств увеличиваются в соответствии с ростом услуг.

SDN (Программно-конфигурируемые сети) – это новая сетевая архитектура, которая обещает лучшее управление сетью путем разделения плоскостей управления и данных [3]. Согласно этой архитектуре, плоскость данных превращается в простое устройство, состоящее из таблицы потоков, которые должны быть созданы логически централизованным контроллером, который запускает сетевые приложения поверх себя. Плоскости взаи-

модействуют через стандартные протоколы, среди которых OpenFlow является наиболее широко-распространенным [4]. На рис. 2 показана структура построения SDN сети.

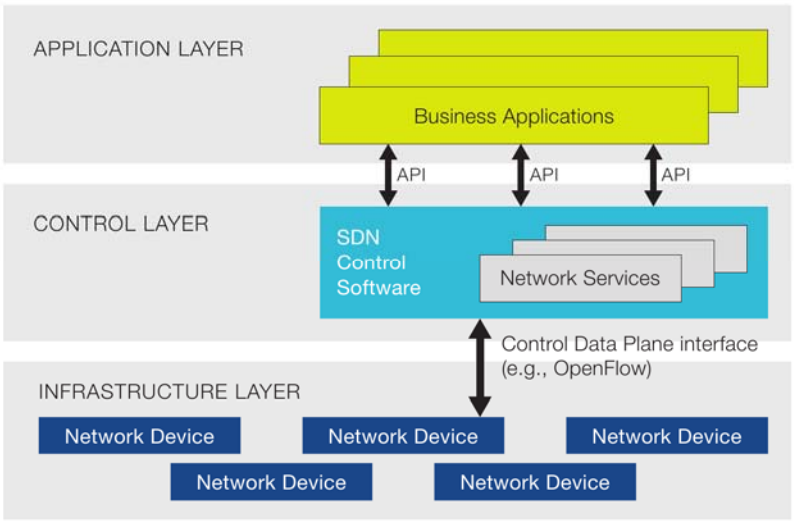


Рис. 2. Схема взаимодействия SDN-устройств

Программно-конфигурируемый подход предоставления MPLS VPN и VPLS может решить вышеупомянутые проблемы.

Во-первых, использование централизованной системы управления позволяет:

1. Уменьшить сложность контроля за устройствами.
2. Упростить конфигурирование, необходимых клиенту услуг.
3. Снизить нагрузку на устройства, за отсутствия необходимости построения путей.
4. Сократить время для ввода в эксплуатацию новых сервисов.
5. А также уменьшить время реагирования при внештатных ситуациях.

Во-вторых, за счет разделения плоскостей управления и данных, устройства передачи данных в сети поставщика услуг становятся простыми, за счет чего значительно уменьшается их стоимость, относительно традиционных устройств, что способствует уменьшению затрат на замену оборудования или при наращивании мощностей [3].

В-третьих, данное решение достаточно масштабируемо для обслуживания большого количества. При нехватке мощностей, достаточным будет является улучшение централизованного управляющего устройства. Значительно упрощается ввод в эксплуатацию новых устройств. А добавление второго контроллера делает сеть более отказоустойчивой.

На рис. 3 показана схема использования SND в гипотетической сети поставщика услуг VPN. Устройства CE этих клиентов подключены к PE-устройствам, чтобы иметь VPN-сеть, реализованную службами VPLS

или MPLS VPN. PE маршрутизаторы меняются на программно-конфигурируемые коммутаторы, управляемые логически централизованным контроллером через OpenFlow.

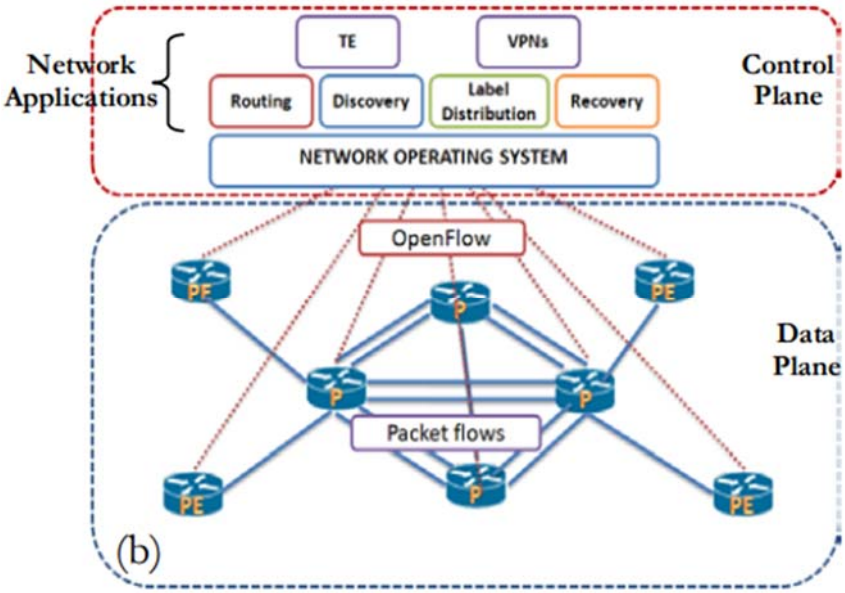


Рис. 3. Схема построения сети MPLS с помощью SDN

Таким образом, SDN – это программно-сетевое решение для поставщиков услуг MPLS VPN и VPLS. Оно упрощает сложность управления, сокращает расходы, налагаемые традиционными не-SDN-устройства, и обещает решить проблемы масштабируемости, с которыми приходится сталкиваться поставщикам услуг, без снижения производительности текущей конфигурации. А также позволяет увеличить надежность работы сети, за счет централизованного управления сетевыми параметрами на уровне сессий, пользователей и приложений.

Список используемых источников

1. Teare D., Vachon B. Rick Graziani Implementing Cisco IP Routing (ROUTE) // Foundation Learning Guide, 2015.

2. Левин М. В., Ушаков И. А., Цветков А. Ю., Исаченков П. А. Основы построения компьютерных сетей. СПб. : СПбГУТ, 2016. 56 с.

3. Швидкий А. А. Моделирование и реализация средств виртуализации сетевых функций NFV: отчет о НИР. СПб. : СПбГУТ, 2015. 50 с.

4. McKeown N., Anderson T., Balakrishnan H., Parulkar G., Peterson L., Rexford J., Shenker S. and Turner J. Openflow. Enabling innovation in campus networks // SIGCOMM Computer Communication Review, vol. 38, no. 2, pp. 69–74, 2008.

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

УДК 004.4

ИНФОРМАЦИОННАЯ СИСТЕМА ДЛЯ КАФЕДР НА БАЗЕ ИНФРАСТРУКТУРЫ DOCKER КОНТЕЙНЕРОВ

Д. П. Морозов, О. Б. Петрова

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

С каждым годом растет популярность системы виртуализации Docker. Интерес к Docker проявляют как конечные пользователи, так и разработчики программного обеспечения, что обеспечивает его динамичное развитие. В статье представлена реализация информационной системы кафедры на базе Docker контейнеров. Показано взаимодействие контейнеров в системе.

виртуализация, docker, изолированное окружение, контейнеры, образы, учебные материалы, сайт кафедры.

В настоящее время на кафедре ежегодно увеличивается объем используемых данных. А данные предыдущих лет используются для анализа и повторного использования.

Для того, чтобы хранить большой объем данных, необходима информационная система, позволяющая получить регламентированный доступ к материалам кафедры, гарантирующая безопасность данных и быстрое восстановление после сбоев.

Можно выделить следующие данные:

- документы, связанные с управлением персоналом, оборудованием;
- нормативные документы;
- учебные материалы и публикации;
- информационные материалы кафедры (общедоступный сайт).

Для реализации подобной системы может быть использовано приложение с открытым исходным кодом Docker.

Docker – это opensource-приложение (проект, инфраструктура), написанное на языке Go, позволяющее упаковывать, распространять, устанавливать и использовать opensource-приложения [1]. Каждое приложение работает в изолированной среде, называемой контейнером. Контейнеры (*containers*) – это простые и переносимые между платформами хранилища для приложения и его зависимостей [1], каждый из которых содержит изолированный экземпляр операционной системы (ОС). Под зависимостями

понимается набор библиотек, необходимых для корректного запуска инкапсулированного приложения.

Благодаря Docker разработчики могут создавать программное обеспечение на любой современной локальной системе, внутри контейнеров, точно зная, что оно будет работать одинаково в любой другой операционной среде [2].

Инженеры по эксплуатации могут сосредоточиться на обеспечении бесперебойной работы программного обеспечения и тратить меньше времени на конфигурирование окружения и на борьбу с системными зависимостями [2].

Инфраструктура кафедры ПИВТ

Для кафедры программной инженерии и вычислительной техники (ПИВТ) актуальны следующие приложения: СУБД для хранения документов кафедры, информационный сайт и программа для управления его контентом (CMS), ПО для доступа к учебным материалам кафедры.

На данном этапе в состав информационной системы кафедры входят следующие приложения: СУБД PostgreSQL для хранения документов кафедры, сайт под управлением CMS «PyMod», разработанная на языке Python 3.

Новые контейнеры для приложений создаются на основе образов. Готовые образы можно получить из Docker Hub, либо собрать новый на основе Dockerfile. Dockerfile – это обычный текстовый файл, содержащий набор сценариев (инструкций), которые могут быть использованы для создания Docker-образа. Все образы доступны только для чтения.

Для контейнеров Docker использует файловую систему UnionFS (*Union File System*), которая позволяет монтировать несколько файловых систем в общую иерархию, которая выглядит как единая файловая система.

На данном этапе разработки инфраструктуры кафедры ПИВТ используются следующие образы (см. рис. ниже):

- ubuntu последняя актуальная версия;
- nginx 1.12.2;
- postgres 9.6.2;
- python 3.6.1;
- app_pymod;
- develope.

Образы app_pymod и develope содержат в себе Python 3.6.1 и все необходимые зависимости для работы CMS «PyMod». При этом app_pymod содержит в себе полную независимую копию системы управления контентом «PyMod», а образ develope только необходимые зависимости (модули).

Разворачивание (автоматизация) данной инфраструктуры происходит с помощью инструмента Docker Compose. Compose использует файлы yaml (язык сериализации данных) для хранения конфигурации групп контейнеров (сервисов в контексте *Compose*).

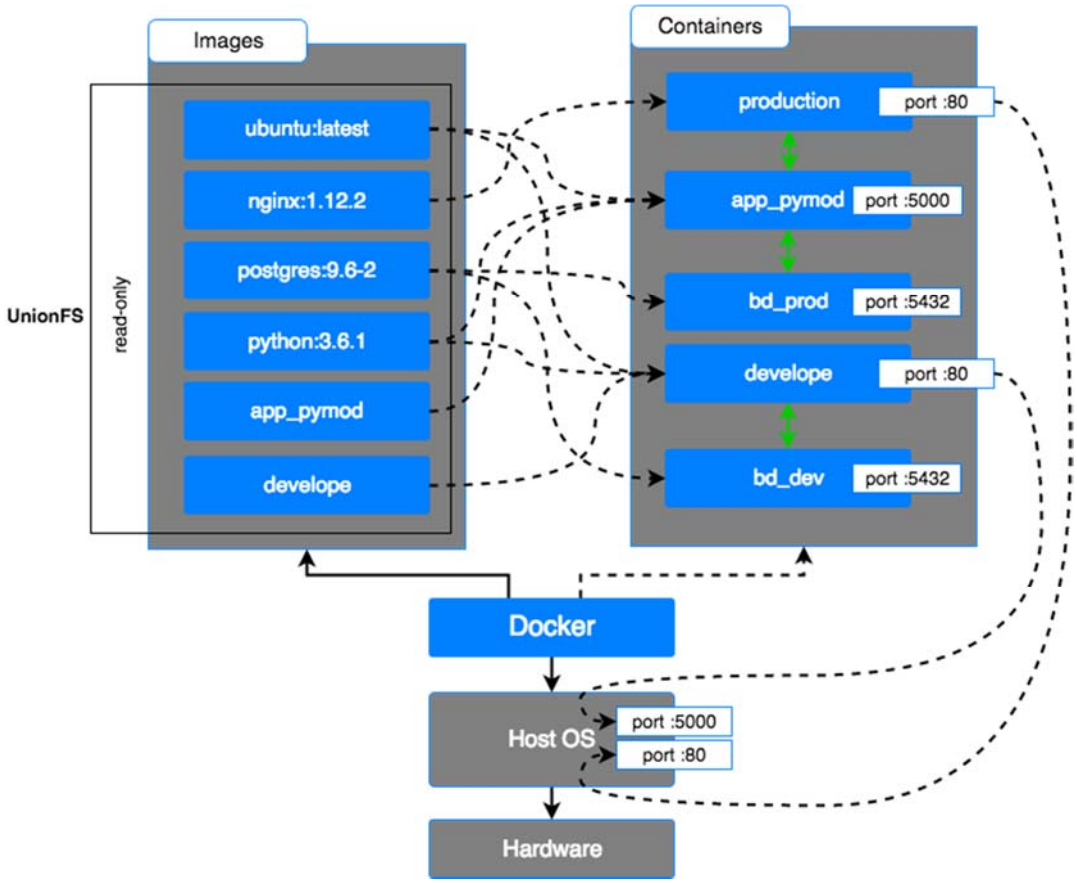


Рисунок. Инфраструктура кафедры ПИВТ

На основе образа postgres создаются контейнеры db_prod и db_dev с пробросом директорий, хранящих данные базы данных, на хостовую машину и запускают сервисы (приложения) внутри контейнеров на внутреннем порту 5432 (порт доступен только для других контейнеров и не доступен извне хостовой машины). Подключение к базе данных возможно только из другого контейнера.

На основе образов app_pymod и develope создаются контейнеры. Контейнер app_pymod содержит в себе «PyMod», а в контейнер develope пробрасываются все директории и файлы, необходимые для корректной работы CMS.

В контейнерах develope, app_pymod запускается внутренний сервис (CMS) на порту 80, 5000, соответственно, доступном только из других контейнеров. Для контейнера develope данный сервис доступен извне по порту 5000.

На основе образа nginx создается контейнер production с пробросом директорий для статических файлов в режиме read-only и запускается внутренний сервис на порту 80 доступном извне. Данный контейнер занимается отдачей статического контента. Для отдачи динамического контента nginx выступает в режиме proxy, направляя все запросы другому контейнеру app_pymod на 5000 порт. CMS, запущенная в контейнере, отдает динамический контент обратно на nginx, который отдает контент клиенту.

В случае «выхода» одного из контейнеров, его на лету можно заменить идентичным контейнером буквально за несколько секунд.

Контейнер production связывает с собой контейнеры app_pymod и bd_prod и между ними пробрасываются необходимые локальные порты и ip-адреса. А контейнер develope связывает с собой только один контейнер bd_dev.

Заключение

Подведём итоги:

– Проведено исследование локально развернутой среды Docker.

– Развернута система Docker контейнеров в виртуальной машине ЦОД.

– Разработана информационная система кафедры в составе базы данных, системы управления контентом, сайта.

Основные проблемы при разработке и эксплуатации:

– нехватка дисковой квоты;

– программный сбой внутри одного из контейнеров;

– потеря данных базы данных, находящихся в контейнере при некорректной конфигурации.

На данный момент, все контейнеры с базой данных сконфигурированы с корректным пробросом директорий хранящих файлы базы данных. Уничтожение контейнера не влечет за собой потерю всех данных базы данных.

Выход из строя одного из компонентов не влечет за собой крах всей системы, и контейнеры, не связанные с данным компонентом, будут работать в штатном режиме.

Список используемых источников

1. Невижин А. Docker. [Электронный ресурс]. URL: http://it.nevizhin.ru/2016/06/11/docker/

2. Моуэт Э. Использование Docker / пер. с англ. А. В. Снастина; науч. ред. А. А. Маркелов. М. : ДМК Пресс, 2017. 354 с.: ил. ISBN 978-5-97060-426-7.

Статья представлена заведующим кафедрой, кандидатом технических наук, профессором Л. Б. Бузюковым.

УДК 621.391

ПРОБЛЕМЫ ВНЕДРЕНИЯ СЕТЕЙ NGN

Э. А. Набиев

Азербайджанский Технологический Университет

Развитие телекоммуникации привело к формированию новой концептуальной модели построения сетей, называемых Сети следующего поколения NGN. Однако ей, как и любому новому направлению, свойственны недостатки, недооценка которых чревато серьезными последствиями для рынка телекоммуникационных услуг. Настоящая работа посвящена анализу проблем внедрения и эксплуатации сетей NGN и взаимодействий их компонентов зависимости от множества поставщиков оборудования.

телекоммуникация, сеть следующего поколения, микропроцессорная технология, компьютерная логика, мультисервис, многопротокольная коммутация по меткам, асинхронный режим передачи.

Современная технологическая революция в системах связи связывается обычно с концепцией сетей следующего поколения. Оборудование NGN (*Next Generation Network*) построено на основе современной микропроцессорной технологии, поэтому сети NGN можно отнести к системам распределенного интеллекта. Компьютерная логика используется на всех стадиях разработки оборудования NGN. Идея перехода к NGN очень привлекательна как операторам связи, так и всему телекоммуникационному миру в целом. Однако ей, как и любому новому направлению развития связи, свойственны недостатки, недооценка которых может отразиться серьезными последствиями для всех участников рынка телекоммуникационных услуг. Наряду с явными достоинствами, сети NGN, на сегодняшний день, имеют ряд недостатков, которые необходимо отметить для полного формирования представления о сетях связи следующего поколения.

К внедрению сетей NGN можно отнести следующие проблемы:

- Отсутствие чёткой нормативной базы.
- Взаимодействие оборудования разных поставщиков.
- Недостаточная надёжность.
- Проблема качества обслуживания.
- Недостаточная квалификация персонала.
- Риски инвестиций.

Отсутствие чёткой нормативной базы

Одним из важнейших факторов, тормозящих развитие NGN, является отсутствие чёткой нормативной базы, определяющей архитектуру NGN. Для выбора конкретной технологии оператору необходимо обладать решительностью и богатым собственным опытом, который не всегда подсказывает оптимальные решения. Зачастую операторам и производителям самим приходится составлять требуемые документы.

Взаимодействие оборудования разных поставщиков

При отсутствии чёткой нормативной базы часто возникает проблема взаимодействия оборудования разных поставщиков. При тестировании практически ни один из производителей не прошел все тесты без ошибок. В процессе доработки оборудования и повторных испытаний была снята примерно треть замечаний. Многие фирмы-поставщики телекоммуникационных услуг утверждают, что именно у них имеется вся линейка оборудования, для реализации NGN. Однако на данный момент NGN является не более чем концепцией, за которой нет пока строгой структуры стандартов на используемые протоколы и интерфейсы, на технологии, реализующие эти стандарты. Поэтому, пока нельзя утверждать, что оборудование какой-либо фирмы позволят реализовать весь спектр услуг NGN. Сегодня еще нет технологий, которые бы полностью удовлетворяли запросам перспективной мультисервисной сети. Однако технологические решения, способные стать ее основой, существуют и на сегодняшний день, т. е. можно построить прообраз мультисервисной сети, которая со временем сможет эволюционировать к мультисервисной сети будущего. В этих условиях термин NGN, является больше рекламным ходом фирм, для проталкивания своей продукции на телекоммуникационный рынок. Традиционных телефонных операторов, потерявших значительную долю доходов за счет междугородных телефонных услуг, перешедших в руки менее инерционных IP (*Internet protocol*, Интернет протокол) – телефонных провайдеров, одолевают предложениями, о приобретении оборудования NGN, тем самым превратиться в современного мультисервисного оператора. Однако, уже имеющийся опыт построения элементов мультисервисных сетей, показывает, что проблемы заключаются не только в отсутствии современной технологической основы для обеспечения мультисервисных услуг. Среди проблем, стоящих перед оператором, внедряющим технологии сетей следующего поколения, основным является взаимодействие различных компонентов сетей следующего поколения от различных поставщиков, который требует тщательной проработки, например, в форме создания опытной зоны NGN. Несомненно, данные недоработки в дальнейшем будут устранены, но они снижают доверие

потенциальных покупателей оборудования, тем самым отодвигая сроки окончательной доработки функциональности.

Недостаточная надёжность

Надежность обычной телефонной сети в последние 10–15 лет оценивается коэффициентом готовности, который выражается в числе «девяток» и равен «5 девяткам», т. е. 99,999 %. Архитектура NGN предполагает применение на транспортном уровне пакетной коммутации и традиционное оборудование данных для IP не обеспечивает готовности «5 девяток». Надежность компьютерных систем сегодня оценивается величиной 98,5 %. Эта величина определяется не только сетью ПД (передачи данных), но и реализацией приложений с использованием серверов. В сети NGN надёжность также определяется на двух уровнях – транспортном и уровне приложений, соответственно, коэффициент готовности системы определяется как произведение коэффициентов готовности её составляющих. Надёжность транспортной системы целиком и полностью определяется оператором. Надёжность уровня приложений может зависеть как от оператора (в случае предоставления всего спектра услуг оператором), так и от сторонних провайдеров. Надёжность серверов приложений может находиться в зависимости не только от оператора, предоставляющего транспортную сеть, но и от поставщика контента. Кроме того, необходимо учитывать специфику предоставляемых услуг [1].

Проблема качества обслуживания

На сегодняшний день нет чёткого ответа на вопрос обеспечения качества обслуживания. Очевидно, что при переходе от традиционных сетей к сетям следующего поколения качество обслуживания, по меньшей мере, не должно ухудшиться. Сегодня многие маршрутизаторы, используемые на магистральных участках Интернет, не поддерживают приоритезацию трафика, следовательно, в инфраструктуре NGN использовать их будет нельзя. Потребуется замена очень больших объёмов оборудования. Не до конца определена и технология обеспечения качества обслуживания. На ранних этапах развития мультисервисной сети предлагалось использовать ATM (*Asuchronous Transfer Mode* –асинхронный режим передачи), которая блестяще справлялась с поставленной задачей. К сожалению, решения с применением ATM оказались слишком дорогими. Несколько лет назад основным механизмом обеспечения QoS в NGN считали MPLS (*MultiProtocol Label Switching* – многопротокольная коммутация по меткам). Однако сегодня это утверждение не может быть принято безусловно. Появляются пред-

ложения использования Ethernet в качестве транспортной технологии. Таким образом, вопрос обеспечения качества обслуживания в NGN остаётся открытым [2].

Недостаточная квалификация персонала

Одной из проблем NGN является недостаточная квалификация персонала основных операторов. Опыта и знаний в данной области не хватает всем. В реальном понимании как технических, так и коммерческих законов NGN специалисты не обладают достаточной квалификацией.

Риски инвестиций

Сеть NGN для чистой голосовой телефонии неэффективна. В настоящее время многие ошибочно считают, что недорогой маршрутизатор, пригодный для десяти компьютеров, будет с легкостью обслуживать десять телефонов. Но этого не произойдет, поскольку в телефонии другие требования к производительности и качеству, ведь это услуга действует в реальном времени. По оценкам некоторых специалистов, создание качественной мощной инфраструктуры для NGN-сети потребует в 1,3 раза больше средств, чем покупка самой телефонной станции. Кроме того, необходимо учитывать финансовую инерцию – телефонные станции стоят довольно дорого, и менять их с той же частотой, с какой мы обновляем компьютерный парк, уже не получится.

В последнее время общепризнанно, что особое внимание для обеспечения эффективного внедрения и эксплуатации NGN следует уделять тестированию и мониторингу. В NGN задачи тестирования и мониторинга породили новую стратегическую проблему, так называемую глобальную совместимость, под которой понимается совместимость как технических средств, так и услуг, классов и параметров качества обслуживания [3, 4].

Список используемых источников

1. Нетес В. А. Надежность сетей связи в период перехода к NGN // Вестник связи. 2007. № 9. С. 27–29.

2. Вегешна Ш. Качество обслуживания в сетях IP. М. : Вильямс, 2003. 368 с.

3. Кучерявый А. Е., Парамонов А. И., Кучерявый Е. А. Сети связи общего пользования. Тенденции развития и методы расчета. М. : ФГУП ЦНИИС, 2008. 228 с.

4. Андреев Д. В., Тарасов Д. В., Кучерявый А. Е. Модельные сети для тестирования технических средств NGN. Рекомендация МСЭ-Т Q.3900 // Электросвязь. 2007. № 12. С. 32–35.

Статья представлена доцентом кафедры компьютерной инженерии и телекоммуникаций АТУ, кандидатом технических наук П.Д. Мурадовым.

УДК 681.518

UNIVERSAL RANK-SIZE DISTRIBUTIONS IN NETWORK TRAFFIC

V. D. Nguyen

Saint Petersburg Electrotechnical University LETI

In this paper network traffic rank-size statistics at different levels and organization are analyzed. Obtained results indicate that the rank-size traffic distributions of internal IPs in the local network and web servers can be described by beta distribution; rank-size traffic distributions of external IPs of the local network can qualitatively be approximated by the q-exponential distribution; rank-size traffic distribution of source and destination IPs of the backbone link closer to power law that is conventional form of Zipf's law.

Internet traffic, Local network, Rank distribution, Zipf's Law.

Cooperative behavior due to erratic user activity is a key determinant of network traffic complexity. Nowadays online communities are permanently and strongly linked thus taking only seconds to involve far more participants into an active conversation by exchanging links to some source of interest. Although the emergence of Zipf's law [1] in the network traffic patterns has been reported as early as late 1990s [2], due to the intensification of inter-user communications and increased role of social networks strongly affecting the network activity patterns nowadays, we next revisit this approach with new data and find good approximations that are valid for typical traffic patterns taking into account typical discreteness and finite size effects.

In our analysis we use the daily traffic traces collected at the downlinks between the local campus networks of St. Petersburg Electrotechnical University (LETI) and Ivanovo State University (IvSU) and their ISPs. The LETI dataset contained 10 complete daily traffic patterns from 17/03/2015 until 18/03/2015, from 16/04/2015 until 19/04/2015, and from 26/04/2016 until 29/04/2016. The IvSU dataset covered 15 consecutive days from 31/01/2017 until 14/02/2017. To support the extension of our findings to other network levels and organizations, we also consider historic access data of NASA web server and University of Saskatchewan web server obtained from the Internet Traffic Archive [3] and the WIDE network backbone link traces obtained from the MAWI archive [4].

First, we study the rank-size traffic distributions of the internal IPs of the local network for the entire daily traffic traces. For this purpose, all internal users who were active at least once in the analyzed days are identified. For the IvSU network, about 250 users are active at least once per day, and the LETI network

has more than 350 active users per day in 2015, and more than 550 active users per day in 2016 due to network expansion. Then, the number of packets received by each active user within 24 hours is determined. As a result, a series that characterizes the number of packets received by each active user per day was obtained. Then this series was ranked in descending order. The resulting ranked series takes the form $f(r) = f(1) \geqslant f(2) \geqslant f(3) \geqslant ... \geqslant f(N)$, where N is the number of active IPs in the network in the studied day; r = 1, 2, ... N are the corresponding ranks. The series (r) is represented on the graph as a function of the corresponding ranks r (see two left panels in Fig. 1 for LETI and IvSU local networks). According to the discreteness effects and the finite size, the functional form of the obtained rank statistics can be successfully approximated by discrete generalized Beta-distribution (DGBD) [5, 6]:

$$f(r) = c(N+1-r)^b r^{-a},$$

where c, b and a are fitting parameters.

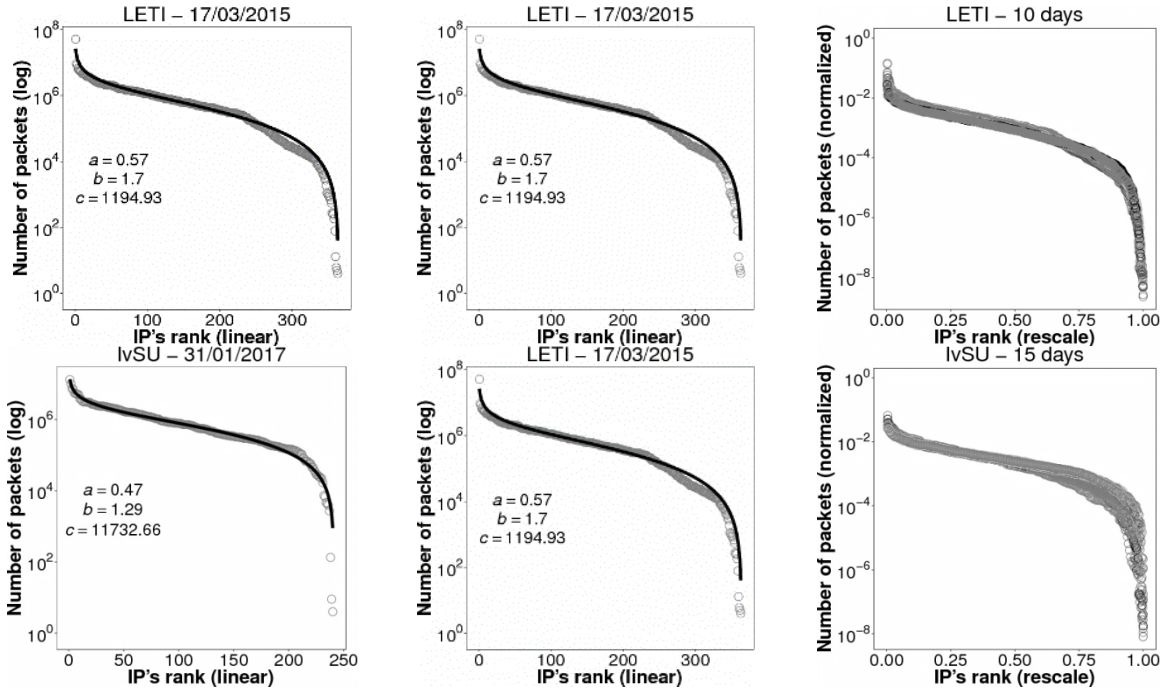


Figure 1. Rank-size distribution of internal IPs for the daily traces of LETI (upper panels) and IvSU (lower panels) local networks

To verify the universality of rank distribution of the activity of users of individual local networks, normalization was carried out. If r is replaced by $r' = r / N$, then $f(r)$ is normalized by $P(r') = f(r / N) / \int_0^1 f(r / N)\mathrm{d}r$, Simple transformations show that $P(r')$ reduces to the conventional form of the β-distribution [7, 8]:

$$P(r') = B\, r'^{\alpha-1}\,(1-r')^{\beta-1},$$

where $\alpha = 1-a$, $\beta = 1+b$ and $B = \Gamma(\alpha+\beta)/[\Gamma(\alpha)\cdot\Gamma(\beta)]$ is the normalization prefactor. Left and middle panels in Fig. 1 showed normalized rank distribution for single studied days with approximated parameter and right panels showed normalized rank distribution of internal IPs for all studied days of LETI and IvSU local networks, respectively. Clearly, after normalization for each network the rank-sized distributions of all the studied days exhibit a universal shape.

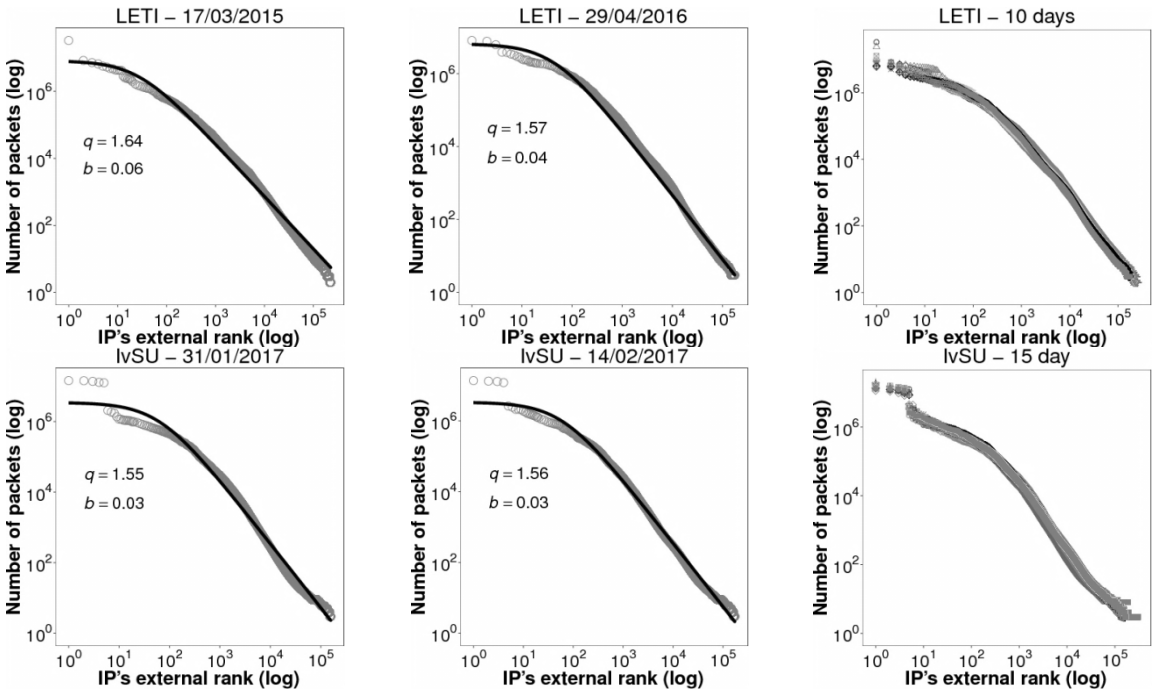


Figure 2. Rank-size distribution of external IPs fitted by *q*-exponential distributions for the daily traces of LETI (upper panels) and IvSU (lower panels) local networks

We find that the rank-size distribution of the external IPs of local networks can be approximated by the *q*-exponential distribution [9]:

$$f(r) = c[1+b(q-1)r]^{-1/(q-1)},$$

where b is the scale parameter, q is the shape parameter and c is normalized to the total traffic amount. For all 25 studied daily records of LETI and IvSU local networks the best fit for the shape parameter was $q = 1.6 \pm 0.05$ (four representative datasets shown in Fig. 2, with two right panels showing the universality of the rank-size distributions of all days for each studied network).

Analysis of the rank-size distributions of all remote users of two web-servers in Fig. 3 shows universality of these distributions, as they also could be fitted by

β-distribution. Of note, for the MAWI traffic data the observed rank-size distributions of both source and destination IPs are closer to power laws, that is more reminiscent to the conventional form of the Zipf's law.

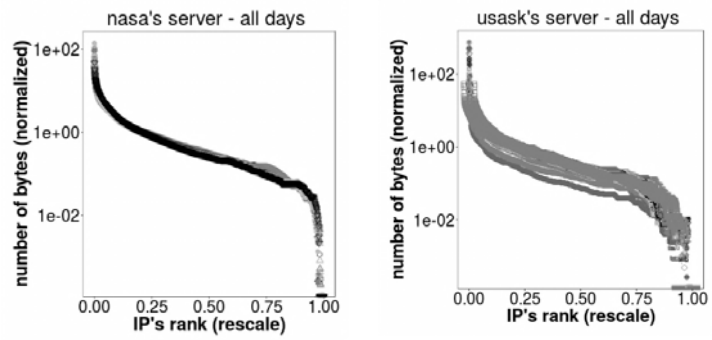


Figure 3. Rank-size distribution of users for two web-server

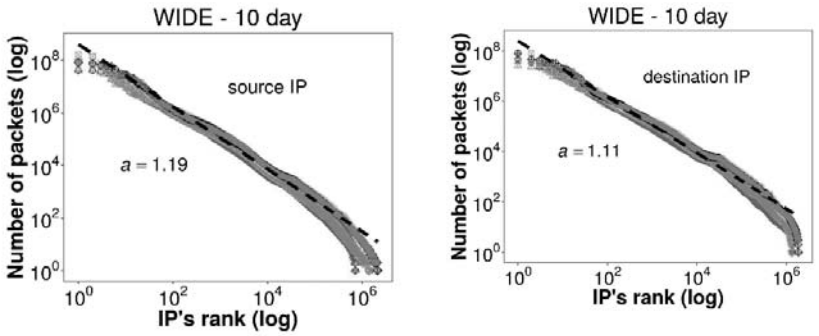


Figure 4. Rank-size distribution of source IPs and destination IPs fitted by Zipf's law (dashed line) for the 10 daily traces of backbone link WIDE

We are interested in the rank-size distribution of non-overlapping fragments of the daily aggregated traffic and their similarity with different time resolution. For this purpose, we split daily traffic record into non-overlapping fragments of different duration and consider rank-size distributions of the total downlink traffic over these time fragments. Fig. 5 shows rank-size distributions of aggregated traffic by time fragments for 10 daily traffic records of LETI local network with different time resolution. Obviously, they are universal and their behavior could be described by DGBD distribution. Similar results are obtained for 15 daily traffic records of LETI local network and for traffic of WIDE backbone link.

Conclusion

The results of the analysis showed the consistency of the description of the network traffic of multi-user local networks on the basis of rank statistics. The β-distribution provides good approximations for rank-size distribution of user activity and rank-size distribution of non-overlapping fragments of aggregated traffic at different levels and organization. Universality of rank-size

distributions can be used to find anomalous traffic patterns in the network by detecting significant deviations from the observed universal patterns characteristic for normal network operation.

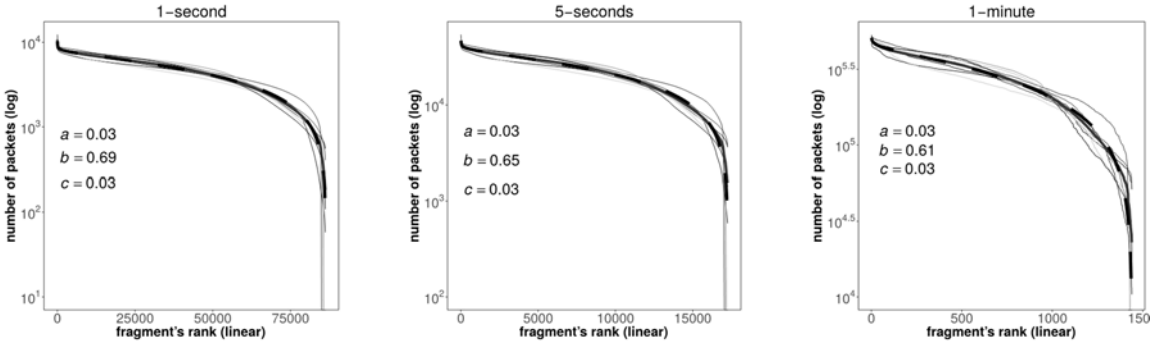


Figure 5: Rank-size distributions of non-overlapping fragments for daily traffic records of LETI local networks with different duration

References

1. Zipf, G. K. The psycho-biology of language // Oxford England (1935).

2. Breslau, L., Cao, P., Fan, L., Phillips, G. and Shenker, S., Web caching and Zipf-like distributions: Evidence and implications // In INFOCOM'99 (1999). Eighteenth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE (Vol. 1, pp. 126–134). IEEE.

3. Available at: http://ita.ee.lbl.gov (accessed: 30.06.2017).

4. Available at: http://mawi.wide.ad.jp/mawi/ (accessed: 30.06.2017).

5. Martínez-Mekler G., Martínez R. A., del Río M. B., Mansilla R., Miramontes P., Cocho G. Universality of rank-ordering distributions in the arts and sciences // PLoS One. 2009 Mar 11; 4(3):e4791.

6. Li W., Miramontes P., Cocho G. Fitting ranked linguistic data with two-parameter functions // Entropy. 2010 Jul 7; 12(7):1743–1764.

7. Wu L and Zhang J. Accelerating growth and size-dependent distribution of human online activities // Physical Review E. 2011 Aug 15;84(2):026113.

8. Naumis G. G., Cocho G. The tails of rank-size distributions due to multiplicative processes: from power laws to stretched exponentials and beta-like functions // New Journal of Physics. 2007 Aug 28; 9(8):286.

9. Yalcin G. C., Robledo A., Gell-Mann M. Incidence of q statistics in rank distributions // Proceedings of the National Academy of Sciences. 2014. Vol. 111, no. 39. pp. 14082–14087.

The article is presented by the scientific supervisor, candidate of technical Sciences, associate Professor of SPbGETU M. I. Bogachev.

УДК 621.395

ТЕХНОЛОГИИ D2D КОММУНИКАЦИЙ. ОБЛАСТИ ИХ ПРИМЕНЕНИЯ

Д. К. Нгуен, А. И. Парамонов

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

Работа посвящена анализу применимости коммуникаций типа устройство-устройство (D2D) в различных областях. В работе приведен анализ современного состояния и перспектив использования данной технологии. Приведена существующая на сегодняшний день классификация данного типа коммуникаций, рассмотрены достоинства и недостатки каждого и типов. Определены основные области и условия применения D2D, а также определен круг задач, которые требуется решить для эффективного применения данного типа связи.

D2D, устройство-устройство, D2D технологий, Inband D2D, Outband D2D, 5G.

Интенсивное развитие технологий беспроводной связи, рост количества пользователей, услуг и объемов передаваемого трафика данных, а также повышение уровня качества предоставления услуг, а также ожиданий качества со стороны пользователей являются ключевыми факторами развития сетей 4G и 5G. Их развитие сопровождается увеличением пропускной способности сетей, а также развитием новых мультимедийных приложений и услуг. Естественно, что повышение пропускной способности достигается использованием большего объема ресурсов, которым является ширина используемого радиочастотного диапазона. Величина этого ресурса, фактически, определяет потенциальные возможности сети. Естественно, что любое техническое решение следует рассматривать с точки зрения эффективности использования этих ресурсов.

Технология прямой связи устройств (D2D – *Device to Device*) – это новая технология, предлагающая беспроводные одноранговые услуги и улучшающая использование радиочастотного спектра в сетях 4G, 5G [1, 2]. Связь D2D изначально предлагалась в сотовой сети в качестве новой парадигмы, повышающей производительность сети.

Мотивация применения D2D определяется потребностями пользователя, а сама технология D2D должна отвечать его требованиям к качеству услуг. Эти потребности включают в себя новые виды услуг с относительно малым радиусом связи и приложения с ограниченными требованиями к скорости передачи данных [3]. Появление контекстно-зависимых и мультимедийных приложений стало мотивацией использования технологий D2D.

Технологии D2D позволяют реализовывать различные типы услуг, таких мультимедийных услуг, как потоковое видео, онлайн-игры и совместное использование файлов одноранговых сетей (P2P). В настоящее время данные технологии реализованы в достаточно большом количестве мобильных устройств.

В сетях сотовой связи D2D определяется как прямая связь между двумя мобильными пользователями без прохождения базовой станции или базовой сети (рис. 1). Это делает D2D ключевой технологией для решения некоторых проблем, например, таких как обеспечение покрытия территории и управление помехами.

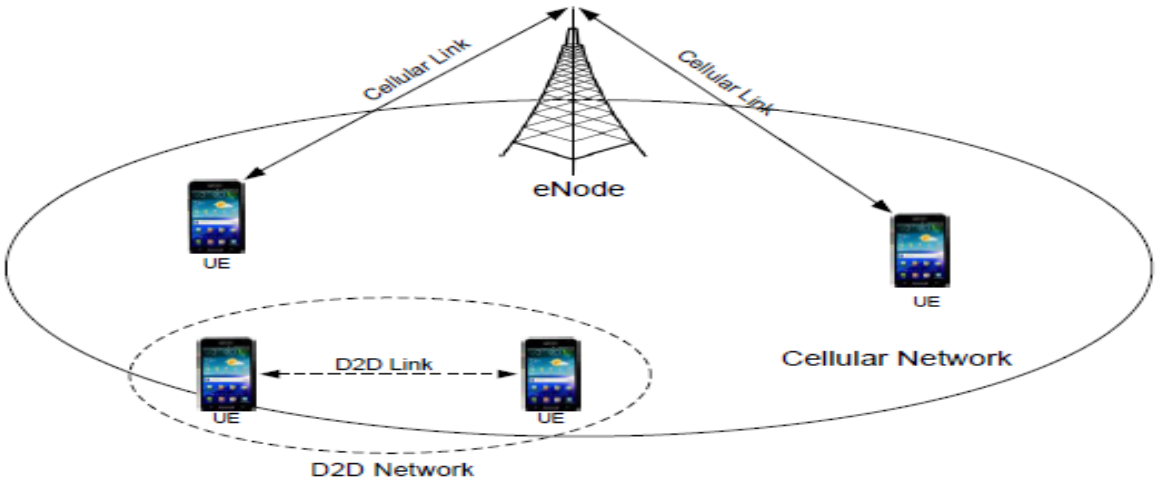


Рис. 1. Технологии D2D коммуникаций

D2D не является первым способом связи, который позволяет осуществлять прямую передачу данных между устройствами. Например, известны такие технологи, как Bluetooth, UWB, mmWave Communications, WiFi Direct. Ожидается, что разрабатываемые технологии D2D будут использовать или одни и те же ресурсы с сотовой системой, или ресурсы не лицензируемых участков радиочастотного спектра.

В настоящее время, основными достоинствами D2D являются:

– Повышенная производительность (эффективность), которая обусловлена возможностью совместного использования ресурсов сети подвижной связи и ресурсов D2D.

– Высокая скорость передачи данных пользователя, достигаемая в случае близости расположения устройств и благоприятных условий распространения.

– Малая величина задержки, которая определяется только временем передачи по каналу точка – точка.

Классификация D2D

Технологии D2D, используемые в сетях подвижной связи можно классифицировать по признаку используемого ресурса радиочастотного спектра (рис. 2). Возможна организация соединений D2D с использованием того же участка радиочастотного спектра, который используется для соединений с базовыми станциями сети (лицензируемый диапазон частот). Такой вариант в литературе называют «внутриполосный» (*Inband*) D2D. При втором варианте организации D2D соединения используются нелицензируемые участки радиочастотного спектра, которые не входят в диапазон частот, используемый сетью подвижной связи. Такой вариант называется «внеполосная» (*Outband*) D2D связь.

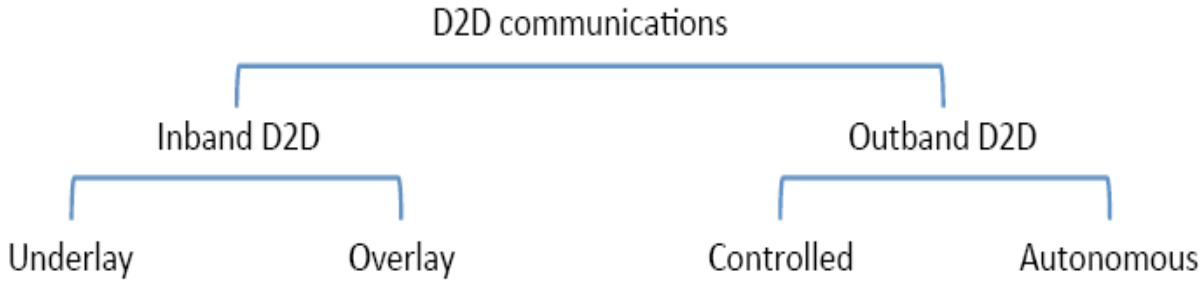


Рис. 2. Классификация D2D

Inband D2D, в свою очередь, также можно классифицировать на два типа (режима) «Inband underlay mode» и «Inband overlay mode». В режиме «Inband underlay mode» используются как ресурсы радиочастотного спектра, так и самой сети. В режиме «Inband overlay mode» используются только ресурсы радиочастотного спектра, которые резервируются для взаимодействующих устройств.

Внеполосную D2D связь также можно условно классифицировать на два вида: управляемую сетью (*Controlled*) и автономную (*Autonomous*).

В настоящее время, Outband D2D привлекает все больше внимания. Большинство новых смартфонов и новых мобильных устройств на рынке оснащены функциями, позволяющими реализовать Outband D2D.

Ряд исследователей дают обзор достоинств и недостатков коммуникаций с Outband D2D. Они возлагают большие надежды на внеполосную связь и рассматривают ее как альтернативу Inband D2D [4, 5].

Краткий обзор достоинств и недостатков Inband D2D и Outband D2D приведен в следующих таблицах 1 и 2.

ТАБЛИЦА 1 – Достоинства и недостатки Inband D2D

Достоинства	Недостатки
• Underlay D2D увеличивает эффективность использования спектра за счет использования пространственного разнесения. • Простое управление QoS, т. к. связь управляется БС. • Возможность использования D2D Inband на любом мобильном устройстве.	• Необходимо управление уровнем помех. • Отсутствует возможность одновременного использования каналов D2D и сотовой сети. • Усложнение процессов распределения ресурсов и управления мощностью.

ТАБЛИЦА 2 – Достоинства и недостатки Outband D2D

Достоинства	Недостатки
• Простое распределение ресурсов. • Возможность одновременного функционирования D2D и сотовых пользователей. • Отсутствие помех между D2D и сотовой связью. • Нет необходимости использовать сетевые ресурсы.	• Необходимо кодировать и декодировать пакеты. • используемая только для радио интерфейсов LTE и WiFi. • Необходимо эффективное управления питанием.

Перспективы использования D2D

В перспективе технологии связи устройство-устройство (D2D) будут иметь широкое распространение, в том числе в сетях 5G. Основные цели и области использования можно описать как:

– применение в локальных сетях уровня PAN для социальных приложений, передачи данных и мобильного трафика;

– применение в чрезвычайных ситуациях, когда традиционные коммуникационные инфраструктуры могут быть повреждены, и услуги сети становятся недоступными;

– при перегрузке сети коммуникации D2D позволяют произвести «выгрузку» трафика из сотовой сети;

– обслуживание трафика Интернета вещей (IoT), например, сбор данных шлюзом, передача данных в сети автомобильного транспорта (V2V) в Интернете транспортных средств (IoV);

– реализация различного рода приложений и услуг локального характера, например, локальных хранилищ данных, серверов и др.

Заключение

Технология D2D уже получила распространение в виде соответствующих функций современных мобильных устройств связи. В настоящее время ее использование ограничивается сетями уровня PAN. Ожидается, что в перспективе D2D станет ключевой технологией для расширения возможностей систем связи 4G и 5G. Для эффективного использования достоинств D2D необходимо создание механизма, обеспечивающего совместное использование ресурсов мобильной сети связи и ресурсов D2D. Из приведенного анализа можно сделать вывод о необходимости решения следующих задач: разработки механизмов управления D2D связями, разработки моделей различных видов D2D коммуникаций, методов оценки эффективности их использования и критериев выбора того или иного вида связи.

Список используемых источников

1. Asadi, A., & Mancuso, V. Wi-Fi Direct and LTE D2D in action // In Wireless Days (WD) IEEE. 2013. pp. 1–8.

2. Novoselov, K. S., et al. Electric field effect in atomically thin carbon films // Science. 2004. pp. 666–669.

3. Geim A. K., & Novoselov K. S. The rise of graphene // Nature materials. 2007. № 6 (3), p. 183.

4. Stankovich, S. Graphene-based composite materials // Nature. 2006. № 442 (7100), p. 282.

5. Prasad, A., Kunz, A., Velev, G., Samdanis, K., & Song, J. Energy-efficient D2D discovery for proximity services in 3GPP LTE-advanced networks: ProSe discovery mechanisms // IEEE vehicular technology magazine. 2014. № 9 (4), pp. 40–50.

УДК 621.391.63(075.8)

ОЦЕНКА СКОРОСТЕЙ ПЕРЕДАЧИ ПО ВОЛС В ТЕХНОЛОГИЯХ PON

Б. К. Никитин, А. Н. Сергеев, Г. М. Смирнов

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

Оценка максимальной скорости передачи по магистральным, распределительным и абонентским участкам сети на основе ВОЛС предполагает учет основных факторов, определяемых потребностями абонентов в услугах связи. Для ее надежной оценки должен быть выполнен многофакторный анализ структуры связи, однако в инженерных расчетах учитывают только основные моменты формирования структуры связи.

сети широкополосного абонентского доступа, технологии PON, FTTx, бюджет ВОЛС.

Оценка максимальной скорости передачи по магистральным участкам сети, достаточно сложная задача, так как предполагает учет всех или основных факторов, определяемых потребностями абонентов в услугах связи [1]. Для ее надежной оценки должен быть выполнен многофакторный анализ структуры связи, однако в инженерных расчетах очень часто довольствуются приближенной оценкой этого параметра, учитывая только основные моменты формирования структуры связи.

В статье предлагается учитывать схему распределения цифровых потоков по объектам, в среднем, составленную на основании сведений по количеству абонентов в заданном сегменте сети.

Объекты (дома, организации и пр. в заданном микрорайоне) – перечисляются типы объектов и их количество, например, жилые дома 12 этажей – 2, детский сад – 1, школа здание 5 этажей – 1, и т. д., по каждому объекту определяется количество абонентов:

H_{01} =……аб.;
H_{02} =……аб., и т. д.

Скорость обмена в сети, которая должна быть предоставлена одному абоненту для получения услуг Tripleplay, может бать определена из следующих соображений.

Техническое обеспечения заданного QoS (оценка качества обслуживания) – это в первую очередь реализация необходимой полосы пропускания сети абонентского доступа [2].

Безусловно, наибольшую лепту в загрузку полосы пропускания внесет видеотрафик и интернет.

С известной долей приближения можно считать, что сегодня один канал телевизионной трансляции или VoD требует скорости передачи порядка 8 Мбит/с. Ситуация заметно улучшится, когда перейдем на стандарт MPEG-4, но в любом случае для получения качественного изображения для видеотрафика нужно будет резервировать порядка 8 Мбит/с на один цифровой канал. Для передачи сигналов HDTV скорость в канале должна быть увеличена как минимум до 12 Мбит/с.

Другим ресурсоемким приложением с точки зрения пропускной способности абонентского канала является интернет и игровой сервис. Для использования интернет трафика в полном объеме со всеми приложениями требуется скорость доступа как минимум 50 Мбит/с. Для полноценного погружения в сетевые игры, особенно в ролевые, необходима скорость не менее 10 Мбит/с. Остальные приложения не столь «прожорливы»: для телефонной связи хватит 64 кбит/с, качественное радиовещание обеспечивается

128 кбит/с, различного рода рекламные ролики, интернет покупки и пр. до 10 Мбит/с. Получаем, что минимальная скорость, предоставляемая одному абоненту должна определятся суперпозицией скоростей по каждой из предоставляемых услуг.

Таким образом, оценка скорости, предоставляемой каждому абоненту в сети, может быть определена по выражению:

$$V_{\sum \text{аб}} = (N_{\text{аб}} \times 0{,}064) \times Y_{\text{тлф}} + V_{\sum \text{инт}} \times Y_{\text{инт}} + V_{\sum \text{тв}} + V_{\text{Eth}},$$

где: $N_{\text{аб}}$ – число ТЛФ каналов, предоставляемых абоненту (1–3, для организаций до 10); $Y_{\text{тлф}}$ – удельная нагрузка, т. е. средняя нагрузка, создаваемая одним абонентом, $Y_{\text{тлф}}$ = 0,01 – 0,05 Эрл; $V_{\sum\text{инт}}$ – скорость доступа абонента в интернет 25–50 Мбит/с (чем больше, тем дороже); $Y_{\text{инт}}$ – удельная нагрузка, т.е. средняя нагрузка, создаваемая одним абонентом на канал доступа интернет, $Y_{\text{инт}}$ = 0,05 – 0,2, учитывает возможное количество абонентов, выходящих одновременно в интернет и время пользования; $V_{\sum\text{ТВ}}$ – суммарная скорость для предоставления услуг ТВ вещания, можно определить из следующих соображений; все абоненты пользуются ТВ приемниками одновременно; количество ТВ приемников у абонента – макс 3; количество одновременно включенных каналов – 2 TV, 1 HDTV.

Таким образом, в приведенном варианте суммарная скорость необходимая для просмотра ТВ программ у одного абонента буде равна:

$$V_{\sum \text{тв}} = (2 \times 8 + 1 \times 12) = 28 \text{ Мбит/с}$$

где V_{Eth} – доступ к локальным ресурсам, интерактивные игры и пр., суммарную потребность в скоростях на одного абонента можно оценить в пределах 5–10 Мбит/с.

Таким образом, для предоставления основных услуг абоненту сети пропускная способность абонентского канала должна быть не менее 40 Мбит/с.

Необходимо отметить, что суммарная скорость будет распределяться по магистральным участкам сети в зависимости от технологии построения сети, количества и потребностей абонентов, обслуживаемых этим участком.

В качестве примера приведем конкретный вариант расчета скорости для микрорайона по пр. Энгельса (рис. 1)

Головная станция устанавливается в помещении почты № 194214 (по адресу пр. Энгельса, 96) и обслуживает остальные дома и учреждения.

Объекты: 18 жилых домов, 2 детских сада, 1 школа, 2 магазина, 1 почтовое отделение, 1 стоматология и 1 здание с 4 офисными помещениями.

Характеристика микрорайона по некоторым критериям представлена в таблице.

Рис. 1. Микрорайон по пр. Энгельса

ТАБЛИЦА. Характеристика микрорайона.

Наименование характеристики	Ориентировочная оценка
Количество домов в микрорайоне	26
Количество абонентов в микрорайоне	2050
Потребности в услугах связи – телефония, передача данных (интернет), каналы ТВ, сети по стандарту Ethernet	80 %

$$V_{\sum аб} = (2*0{,}064)*0{,}02 + 50*0{,}1 + 28 + 10 = 0{,}00256 + 5 + 28 + 10 =$$

$$= 43{,}00256 \text{ Мбит/с} \approx 44 \text{ Мбит/с},$$

$$V_{\sum сет} = 44*2050 = 90200 \text{ Мбит/с}.$$

Необходимо отметить что в расчете не учтены полные потребности организаций, которые размещаются в микрорайоне, поэтому реальная скорость, требуемая в структуре сети, может существенно возрасти.

В результате схема прокладки магистрального кабеля может выглядеть следующим образом (рис. 2).

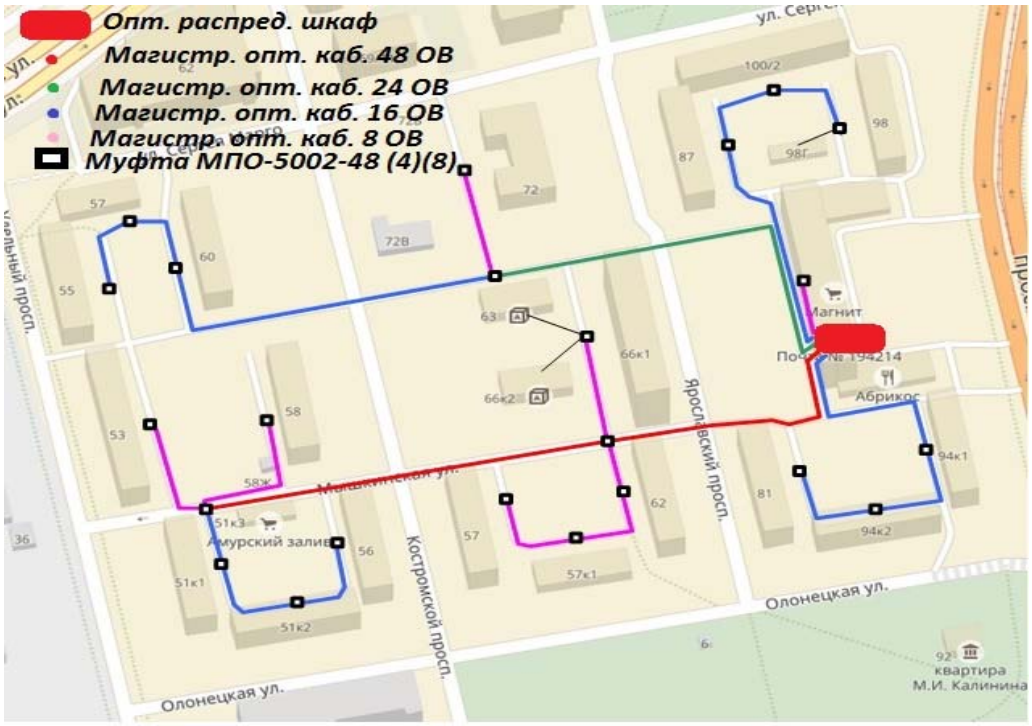


Рис. 2. Схема прокладки магистрального кабеля

В соответствии с количеством участков магистральной сети и числом абонентов, которые они должны обслуживать, определяется скорость передачи по конкретной ветви.

Однако нельзя забывать и об энергетическом потенциале оборудования, которое будет обслуживать конкретный участок. Ведь каждый участок магистральной сети имеет свою структуру и отличается от остальных как по способу реализации, так и техническим характеристикам, поэтому одновременно целесообразно привести и некоторые положения по оценке бюджета ВОЛС.

На рис. 3 представлен условный график распределения потерь на некотором участке сети.

Расчет бюджета потерь может быть выполнен по следующему выражению:

$$A_{\Sigma} = \Sigma_1^n(L_1 + L_2 + \cdots + L_i) \times \alpha + N_p \times \alpha_p + N_c \times \alpha_c + \alpha_{spi} + \alpha_{spm},$$

где A_{Σ} – суммарные потери в линии (между OLT и ONU), дБ; L– длина i-участка, км; n – количество участков; α – коэффициент затухания оптического кабеля, дБ/км; N_p – количество разъемных соединений; α_p – средние потери в разъемном соединении, дБ; N_c – количество сварных соединений; $\alpha\, a_c$ – средние потери в сварном соединении, дБ; α_{spi} – потери в i-оптическом разветвителе, установленном на магистральном участке сети, дБ; α_{spm} – потери в m-оптическом разветвителе, установленном на распределительном участке сети дБ.

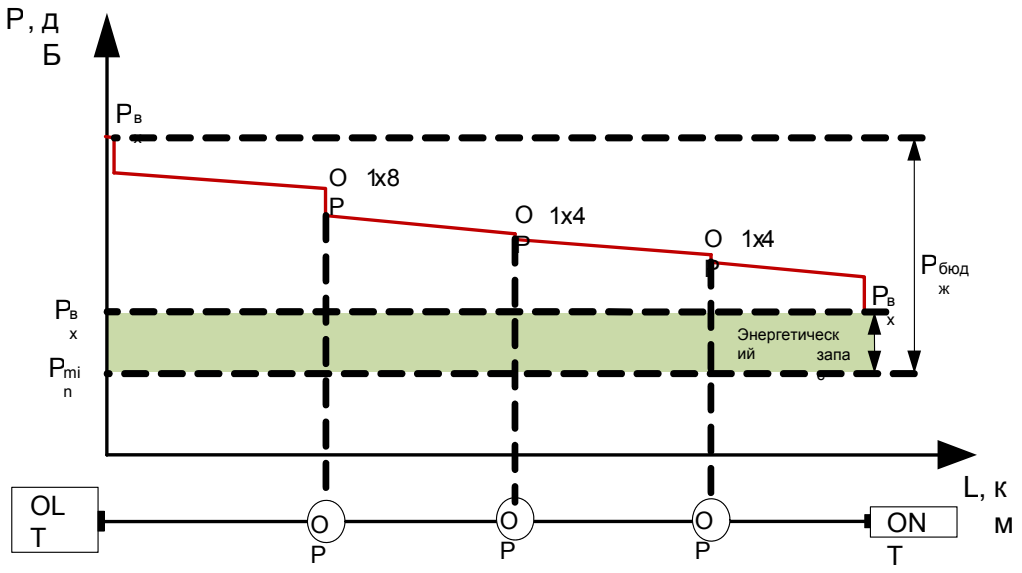


Рис. 3. График бюджета потерь

Список используемых источников

1. Иванов В. С., Никитин Б. К., Пирмагомедов Р. Я. Современные технологии и организация строительства ВОЛС: учебное пособие, СПбГУТ, 2015.

2. Петренко И. И., Убайдуллаев Р. Р. Пассивные оптические сети PON. Часть 1. Архитектура и стандарты // Lightwave Russian Edition. М. 2004.

УДК 004.056.5

АНАЛИЗ СОСТОЯНИЯ ИССЛЕДОВАНИЙ ПО МОДЕЛИРОВАНИЮ РАЗГРАНИЧЕНИЯ ДОСТУПА К ИНФОРМАЦИИ В ОБЛАЧНЫХ ИНФРАСТРУКТУРАХ КРИТИЧЕСКИ ВАЖНЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

И. Б. Паращук[1,2], И. Б. Саенко[1,2], О. И. Пантюхин[3]

[1]Санкт-Петербургский институт информатики и автоматизации Российской академии наук
[2]Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики
[3]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье предложены систематизированные результаты детального анализа состояния исследований в предметной области разграничения доступа к информации

с учетом специфики, свойственной облачным системам хранения данных, являющихся компонентами критически важных информационных систем. Приведены результаты анализа состояния исследований в области применения методов искусственного интеллекта для оптимизации, верификации и реконфигурации политик разграничения доступа. Использование результатов данного анализа позволит повысить обоснованность принимаемых решений в области разработки и применения перспективных моделей контроля доступа с целью выяснения возможностей и способов их реализации в облачных инфраструктурах.

критически важная система, информационная система, политика разграничения доступа, методы, модели, облачная инфраструктура, ресурс, нарушение безопасности, защищенность.

В соответствии с действующим «Перечнем приоритетных направлений развития науки, технологий и техники Российской Федерации», облачные инфраструктуры критически важных информационных систем и их защищенность относятся к критическим технологиям. К числу ключевых основных тенденций развития облачных инфраструктур относят дальнейшее увеличение их возможностей по обеспечению надежности, безопасности, производительности, управляемости и масштабируемости. Таким образом, вопросы обеспечения безопасности (а разграничение доступа является составной частью безопасности) стоят на одном из первых мест.

Повышение роли и стремительное распространение облачных инфраструктур в критически важных информационных системах, повышение совокупной стоимости активов устройств, программного обеспечения и критически важных данных таких систем, а также увеличение числа атак на них определяют актуальность задач разграничения доступа к информации в облачных инфраструктурах таких систем, а также обнаружения и разрешения конфликтов в используемых ими политиках разграничения доступа.

Облачные инфраструктуры представляют собой сравнительно новый вид компьютерных инфраструктур, которые привлекают к себе повышенное внимание в области информационных технологий и обладают повышенным интересом для потребителей информационных услуг и ресурсов. В то же время многие исследователи отмечают, что более широкому распространенному этой технологии препятствуют проблемы безопасности [1, 2, 3]. Недостатком большинства существующих облачных инфраструктур является отсутствие возможности гибкого управления со стороны пользователей доступом к своим данным, что вызвано универсальностью решений по контролю доступа, принимаемых поставщиками облачных услуг [1]. Многие исследователи отмечают, что неоднородность и большое разнообразие ресурсной среды облачного хранилища требуют всестороннего и детально проработанного механизма управления доступом, чтобы обеспечить динамические, постоянно расширяемые и хорошо настраиваемые требования по

защите информации пользователей [2]. Однако существующие механизмы безопасности, обеспечиваемые поставщиками облачной инфраструктуры, не удовлетворяют этим требованиям [3]. Кроме того, проблем безопасности информации в облачных инфраструктурах обостряются, если используются открытые веб-сервисы. Все это настоятельно требует проработки вопросов совершенствования политик разграничения доступа и моделей, лежащих в их основе.

Моделирование, анализ и практическая реализация компонентов систем разграничения доступа в облачных инфраструктурах критически важных информационных систем очень важна в условиях интеграции, в таких инфраструктурах частных политик разграничения доступа, которые используют разнородные модели контроля доступа с учетом повышенных требований по защищенности таких систем, высокой доступности и производительности. К таким системам относятся критически важные информационные системы, основанные на реализации облачных инфраструктур для хранения данных, применяемые в таких областях, как электроэнергетика, управление мегаполисами и крупными городами, транспорт, включая гражданскую авиацию и Российские железные дороги, системы управления нефтедобывающей и газодобывающей промышленности, банковские и коммерческие системы, образовательные и научные учреждения, средства массовой информации, системы административного управления и другие.

Анализируя модели контроля доступа к информации, которые применяются в облачных инфраструктурах, можно сделать вывод, что наибольшей популярностью обладает модель контроля доступа на основе ролей Role-Based Access Control (RBAC), в дополнение к которой предлагается использовать некоторые более перспективные модели. В [3], кроме RBAC, анализируются и предлагаются к использованию модель контроля доступа на основе атрибутов Attribute-Based Access Control (ABAC) и модель «множественной аренды» (*multi-tenancy*), являющаяся разновидностью модели организационного контроля доступа Organization-Based Access Control (OrBAC). В [1] предлагается использовать основанную на RBAC модель Amazon Web Services (AWS), позволяющую расширить возможности политик RBAC и облегчить интеграцию службы разграничения доступа в корпоративные приложения. В [2] предлагается гибкая междоменная модель разграничения доступа, основанная на механизмах преобразования ролей. В [3] среди анализируемых моделей доступа присутствуют мандатный механизм доступа Mandatory Access Control (MAC) и дискреционный механизм доступа Discretionary Access Control (DAC), но отмечается их низкая эффективность в облачных инфраструктурах. В качестве наиболее приемлемых, предлагается использование моделей RBAC и ABAC. В [1, 3] предлагается реализо-

вать новую парадигму услуг, связанную с разграничением доступа – «контроль доступа как сервис» (*Access Control as a Service*) с использованием применяемых в облачных инфраструктурах моделей доступа.

Вопросы моделирования, оценки, формирования и оптимизации политик разграничения доступа в мире в наибольшей степени проработаны для модели RBAC, поскольку она допускает строгую формализацию с выделением переменных, целевой функции и ограничений. Это позволяет выделить задачу оптимизации политики разграничения доступа на основе RBAC в отдельный класс задач интеллектуального анализа данных (Data Mining), получившего название Role Mining Problem (RMP) [4]. Разработаны различные варианты постановки этой задачи и предложен ряд методов и алгоритмов их решения [5]. В [6] разработаны простые эвристические алгоритмы, основанные на комбинаторных решениях. Для снижения сложности комбинаторных алгоритмов в [7] предложено использовать вероятностные модели. Однако вероятностный подход не гарантирует высокой точности решения задачи. Подход, основанный на кластерном анализе, предлагается в [8]. Однако это подход требует учета дополнительных параметров, характеризующих бизнес-процессы и потребности пользователей, что не всегда возможно сделать. В [9] предлагается подход, основанный на методах декомпозиции на основе булевых матриц (*Boolean Matrix Decomposition*). Однако, нигде не рассматривается задача реконфигурирования схемы RBAC. Такой же недостаток справедлив для cost-driven подхода, представленного в [10]. При подходе стоимость определяется затратами администрирования. Однако это подход распространяется только на отдельные варианты RMP. В [11] предложены метрики для оценки различных алгоритмов решения задачи проектирования схем RBAC.

В качестве более общего подхода для решения задач RMP [12, 13], предлагается использовать генетические алгоритмы. В этих работах показано, что генетические алгоритмы, как и другие алгоритмы биоинспирированной оптимизации, следует рассматривать как достаточно эффективные средства решения задач оптимизации политик разграничения доступа.

В работе [14] частично рассматриваются отдельные вопросы, связанные с задачей реконфигурирования схемы RBAC, предложен подход, согласно которому для реконфигурации схемы RMP используются метод access history logs. В [15] предложен подход к верификации политик разграничения доступ, основанный на адаптации различных ситуаций с помощью моделирования уступок, которые пользователи делают, чтобы достигнуть разрешения возможных конфликтов. Этот подход был рассмотрен применительно к социальным системам, однако он представляется применимым для облачных инфраструктур. В [16] для верификации политик разграничения

доступа предлагается использование эвристик, которые понижают сложность механизма разграничения доступа.

Таким образом, анализ имеющихся мировых научных и практических подходов к моделированию, оценке, формированию и оптимизации политик разграничения доступа к информации в облачных инфраструктурах критически важных информационных систем, позволяет сделать следующие выводы: проблема разграничения доступа в облачных инфраструктурах вызвана спецификой свойственных им угроз безопасности и является достаточно актуальной; данная проблема обостряется в критически важных информационных системах; решения этой проблемы связывается с использованием наряду с традиционной моделью контроля доступа RBAC новых перспективных моделей ABAC, OrBAC и других, построенных на их основе; разработка новых моделей, методов и алгоритмов для решения задач оценки, оптимизации, верификации и реконфигурации политик безопасности, основанных на моделях контроля доступа, является активно развивающимся научным направлением, в котором использование интеллектуальных методов, в частности генетических алгоритмов, эвристических многоагентных систем и т. д., позволит получить достаточно эффективные решения.

Результаты анализа имеющихся мировых научных и практических подходов к моделированию, оценке, формированию и оптимизации политик разграничения доступа к информации в облачных инфраструктурах критически важных информационных систем, позволят создать новые модели, методы и алгоритмы, нацеленные на повышение уровня информационной безопасности инфраструктур облачного хранения данных и, соответственно, безопасности информации в критически важных информационных системах, использующих облачные инфраструктуры для своего построения, за счет применения средств искусственного интеллекта для совершенствования моделей контроля доступа и разработки на их основе эффективных методов и алгоритмов управления политиками разграничения доступа.

Работа выполнена при финансовой поддержке РФФИ (проекты 16-29-09482, 18-07-01369 и 18-07-01488), при частичной поддержке бюджетных тем № 0073-2015-0004 и 0073-2015-0007, а также при государственной финансовой поддержке ведущих университетов Российской Федерации (субсидия 074-U01).

Список используемых источников

1. Fotiou, N., Machas, A., Polyzos, G.C. Access control as a service for the Cloud // J. Internet Serv. Appl. (2015) 6:11. doi:10.1186/s13174-015-0026-4.

2. Wu, R., Zhang, X., Ahn, G.-J. ACaaS: Access Control as a Service for IaaS Cloud // URL: http://sefcom.asu.edu/publications/science2013.pdf (дата обращения 13.09.2016).

3. Majumder, A., Namasudra, S., Nath, S. Taxonomy and Classification of Access Control Models for Cloud Environments) // Continued Rise of the Cloud, Computer Communications and Networks, DOI 10.1007/978-1-4471-6452, 2014, pp. 23–32.

4. Frank, M., Buhmann, J. M., Basin, D. On the Definition of Role Mining // Proceedings of the 15th ACM symposium on access control models and technologies (Pittsburgh, PA, USA, June 2010). SACMAT'10. ACM, New York, NY, 2010, pp. 35–44.

5. Vaidya, J., Atluri, V., Guo, Q. The Role Mining Problem: Finding a Minimal Descriptive Set of Roles // Proceedings of the 12th ACM symposium on Access control models and technologies (Sophia Antipolis, France, June 2007). SACMAT '10. ACM, New York, NY, 2007, pp. 175–184.

6. Blundo, C. and Cimato, S. A Simple Role Mining Algorithm // In Proceedings of the 2010 ACM Symposium on Applied Computing (Sierre, Switzerland, March 2010). SAC'10, ACM, New York, NY, 2010. pp. 1958–1962.

7. Frank, M., Buhmann, J.M., and Basin, D. Role Mining with Probabilistic Models // In ACM Trans. on Inf. and Syst. Security, 15, 4 (Apr. 2013), article No.: 15.

8. Lu, H., Hong, Y., Yang, Y., Duan, L., and Badar, N. Towards User-Oriented RBAC Model // In Proceedings of the 27th Annual IFIP WG 11.3 Conference (Newark, NJ, USA, July 2013). DBSec. 2013, Springer, LNCS, 7964, pp. 107–129.

9. Frank, M., Streich, A.P., and Basin, D. Multi-Assignment Clustering for Boolean Data // In The Journal of Machine Learning Research, 13, 2012. pp. 459–489.

10. Colantonio, A., Di Pietro, R., Ocello, A. A cost-driven approach to role engineering // In Proceedings of the 2008 ACM symposium on applied computing (Fortaleza, Ceara, Brazil, March 16 - 20, 2008). SAC'08, ACM, New York, NY, USA, 2008. pp. 2129–2136.

11. Molloy, I., Li, N., Li, T., and Lobo, J. Evaluating Role Mining Algorithms // In: Proceedings of the 14th ACM symposium on access control models and technologies (Stresa, Italy, June 2009). SACMAT'09, ACM, New York, NY, 2009. pp. 95–104.

12. Saenko, I. and Kotenko, I. Genetic Algorithms for Role Mining Problem. In Proceedings of the 19th International Euromicro Conference on Parallel, Distributed and Network-Based Processing (Ayia Napa, Cyprus, February 2011). PDP'2011, IEEE, pp. 646–650.

13. Saenko, I. and Kotenko, I. Design and Performance Evaluation of Improved Genetic Algorithm for Role Mining Problem. In Proceedings of the 20th International Euromicro Conference on Parallel, Distributed and Network-based Processing (Garching, Germany, February 2012). PDP'2012, IEEE, 2012. pp. 269–274.

14. Blundo, C. and Cimato, S. Constrained Role Mining. In Security and Trust Management. Proceedings of the 8th International Workshop (Pisa, Italy, September 2012), Revised Selected Papers. STM 2012, Springer, LNCS, 7783, 2012. pp. 289–304.

15. Such, J.M., Criado, N. Resolving Multi-party Privacy Conflicts in Social Media // IEEE Transactions on Knowledge and Data Engineering (July 2016), pp.1851–1863.

16. Such, J.M., Rovatsos, M. Privacy Policy Negotiation in Social Media // Journal ACM Transactions on Autonomous and Adaptive Systems (TAAS), Volume 11 Issue 1, April 2016. Article No. 4.

УДК 621.395

ИССЛЕДОВАНИЕ ИСПОЛЬЗОВАНИЯ КАНАЛОВ СТАНДАРТА 802.11 (ДИАПАЗОНА 2,4 ГГЦ) В ГОРОДСКИХ УСЛОВИЯХ

А. И. Парамонов, М. Р. Хуссейн, О. А. Хуссейн

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

Статья посвящена исследованию трафика сети беспроводного широкополосного доступа стандартов семейства IEEE 802.11 (в диапазоне 2,4 ГГц) в условиях города. Для измерения параметров использовался метод мониторинга каналов диапазона 2,4 ГГц (сниффинга). В работе получены статистические характеристики трафика такие как: распределения интервалов времени между пакетами, длины пакета. Полученные результаты могут быть использованы для построения аналитической или имитационной модели трафика.

трафик, IEEE 802.11, микроконтроллер ESP8266, точка доступа, канал, интенсивность.

Введение

Развитие технологий беспроводной связи и сетей широкополосного доступа привело к широкому их проникновению в различных областях деятельности и сетях различного масштаба. Наибольшее распространение получили стандарты семейства IEEE 802.11 [1, 2, 3, 4, 5]. В настоящее время сети на основе этих стандартов функционируют, практически, во всех учреждениях и общественных местах. Также существует большое количество сетей масштаба PAN, работающих в частных квартирах жилых домов. Количество потенциальных пользователей этих сетей, практически, определяется количеством мобильных абонентских устройств.

Такое широкое распространение данных технологий привело к высокой плотности пользователей, так и высокой плотности точек доступа. Это может привести к дефициту радиочастотного ресурса.

В связи с этим, целесообразно оценить потенциальную возможность дальнейшего развития и применения данных технологий, когда вероятность использования радиоканала сторонними системами может быть достаточно велика, чтобы существенно снизить полосу пропускания канала. С этой целью проведены исследования характеристик использования каналов стандарта IEEE 802.11 [6] в условиях города.

Постановка задачи

В работе приводится анализ использования стандартов IEEE 802.11, цель в работы – проведение статистических исследований использования радиочастотного диапазона устройствами стандартов семейства IEEE 802.11 (2,4 ГГц) в условиях города.

Условия эксперимента. В данной работе, в качестве условий, выбрана городская среда. Для исследования был выбран сценарий перемещения в городской среде со средней скоростью пешехода (3км/ч). В качестве траектории перемещения выбран случайный маршрут, проходящий через жилые, деловые и смешанные зоны. Протяженность маршрута составила 4 км, время прохождения маршрута 1 ч, средняя скорость 4 км/ч.

Показатели использования

Для характеристики использования каналов рассматриваемых стандартов были выбраны такие показатели как: количество сетей (точек доступа), интенсивность передачи пакетов, интенсивность передачи данных и уровень сигнала в точке приема, оцениваемый индикатором RSSI.

Результаты измерений

Сбор статистики о количестве сетей производился в движении сканированием всех каналов диапазона 2,4 ГГц, с периодом 5 с. Среднее количество регистрируемых в результате сканирования точек доступа составило 24,7. График изменения количества точек доступа в зоне связи приведен на рис.1.

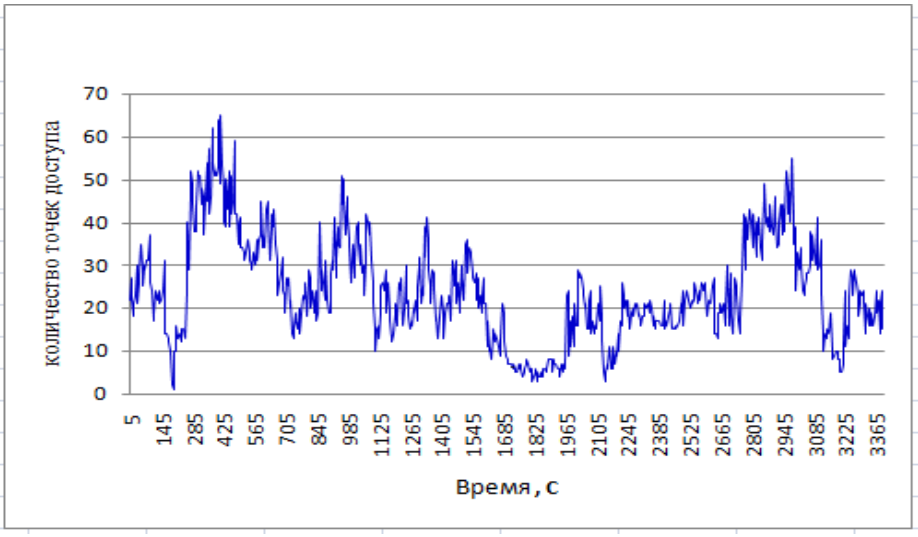


Рис. 1. Изменение количества точек доступа в зоне приема при прохождении маршрут

В режиме сканирования каналов, устройство последовательно сканирует каналы и регистрирует данные о принятых пакетах, и уровень их приема (RSSI). В этом режиме регистрируются все данные, независимо от их источника и устройства назначения без регистрации их идентификаторов (рис. 2).

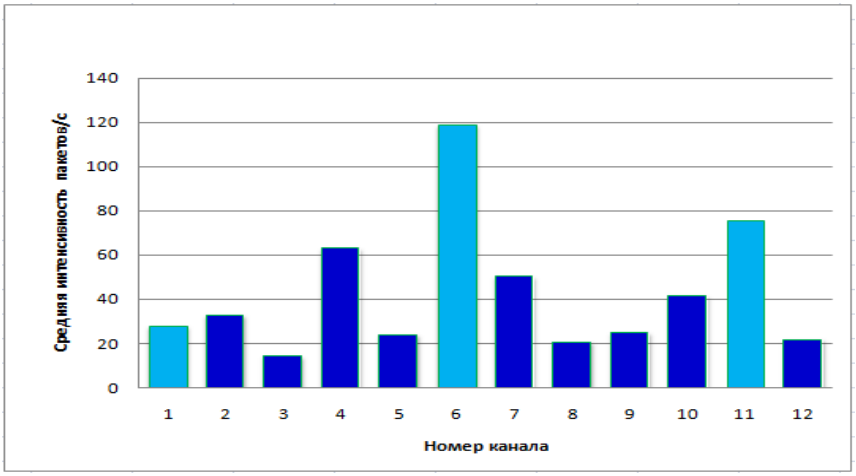


Рис. 2. Распределение интенсивности приема пакетов по каналам диапазона 2,4 ГГц стандарта IEEE 802.11b/g/n

Как видно из рис. 2 наибольшая интенсивность пакетов имеет место в каналах 6 и 11. Данный результат является отчасти ожидаемым, т. к. большинство устройств (выступающих в роли точек доступа) использует именно эти каналы, как наиболее разнесенные между собой по частоте.

На рис. 3 приведено распределение интервалов времени между пакетами для входящего (к точке доступа) потока.

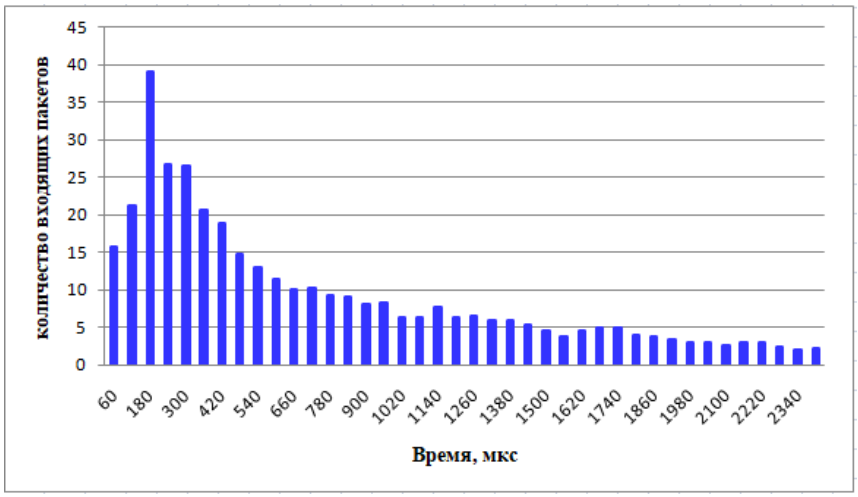


Рис. 3. Распределение интервалов времени между пакетами во входящем потоке

Во-первых, приведенное существенно отличается от экспоненциального, что позволяет сделать вывод от том, что свойства потока отличаются от свойств простейшего потока. Во-вторых, детальный анализ, показывает наличие мультимодальности, что позволяет сделать предположение о возможном наличии нескольких случайных процессов.

На рис. 4 приведено распределение дины пакетов во входящем потоке.

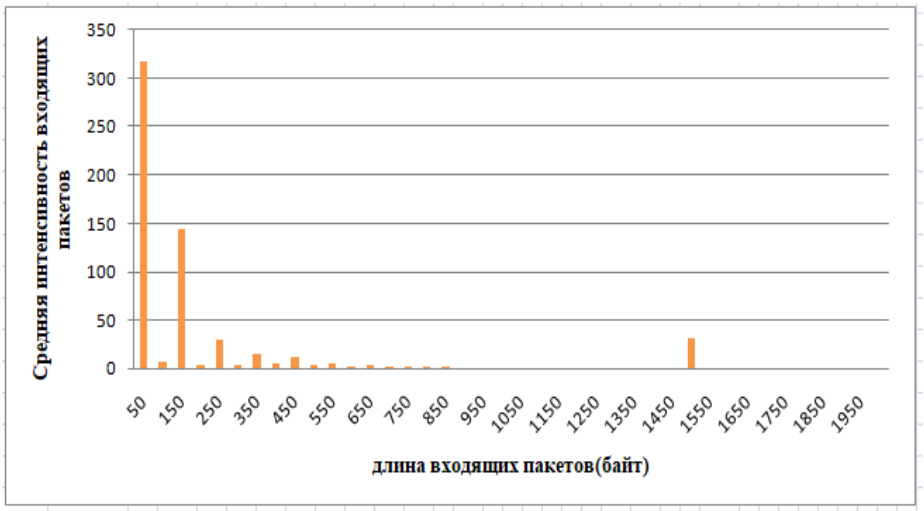


Рис. 4. Распределение длины пакета для входящих пакетов

Анализ данного распределения показывает явно выраженные моды распределения для средних длин пакетов 50, 150, 250 350 и 1500 байт. Это позволяет сделать предположение о том, что распределение длины пакета имеет дискретный характер.

Выводы

1. Результаты измерений и анализа статистических данных показали, что в диапазоне 2,4 ГГц стандартов семейства IEEE 802.11 в условиях города имеет место достаточно большое количество потенциальных источников трафика (точек доступа). Их среднее количество в зоне доступности при произвольно выбранной точке размещения приемопередающего устройства составляет 24,7.

2. Получено распределение интервалов времени между пакетами, которое позволяет судить об отличии свойств потока от свойств простейшего потока, а также дает возможность выбора его аналитической модели.

3. Получено распределение длины пакетов, которое имеет выраженные моды для нескольких длин пакетов. Данный результата так же может быть использован для построения аналитической или имитационной модели трафика.

4. Дальнейшие исследования свойств трафика могут быть направлены на выбор аналитических моделей для описания полученных распределений.

Список используемых источников

1. 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.

2. Парамонов А. И. Модели потоков трафика для сетей M2M //Электросвязь. 2014. № 4. С. 11–16.

3. Muthanna A., Masek P., Hosek J., Fujdiak R., Hussein O., Paramonov A., Koucheryavy A. Analytical Evaluation Of D2D Connectivity Potential in 5G Wireless Systems // Lecture Notes in Computer Science. 2016. Т. 9870. PP. 395–403.

4. Futahp A. Koucheryavy A., Paramonov A., Prokopiev A. Ubiquitous Sensor Networks in the Heterogeneous LTE Network // 17th International Conference on Advanced Communications Technology (ICACT) 2015. PP. 28–32.

5. Kirichek R., Paramonov A., Koucheryavy A. Swarm of Public Unmanned Aerial Vehicles as a Queuing Network // Communications in Computer and Information Science. 2016. Т. 601. PP. 111–120.

6. Стандарты семейства IEEE 802.11.

УДК 621.395

ЗАДАЧИ КЛАСТЕРИЗАЦИИ D2D КОММУНИКАЦИЙ В СЕТЯХ ПЯТОГО ПОКОЛЕНИЯ

А. И. Парамонов, О. А. Хуссейн

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

Непосредственное взаимодействие между терминалами позволяет повысить такие качества сети как надежность и устойчивость к различным деструктивным факторам, в том числе снизить интенсивность абонентской нагрузки на базовые станции сети. В данной работе рассматриваются задачи организации D2D коммуникаций в сетях связи пятого поколения и применение в этих задачах методов кластерного анализа.

5G, пятое поколение, D2D, устройство-устройство, кластеризация, энергопотребление.

С момента появления и до сегодняшнего дня сети мобильной связи прошли большой путь развития; появились новые типы пользовательских устройств. Возможности мобильных технологий сегодня, вышли за рамки голосовых услуг, создавая новые способы обмена данными. Технологии

коммуникаций развиваются в направлении к более высокой производительности и большему числу услуг. Это приводит к появлению так называемых гетерогенных зон базовых станций систем длительной эволюции [1]. При создании LTE задача поиска новых форм взаимодействия между различными составляющими гетерогенной зоны не ставилась. Сети мобильной связи 3G и 4G предназначались, в первую очередь, для повышения эффективности таких показателей, как скорость передачи данных и использование радиочастотного спектра. При разработке сети 5G, в основе которой лежит сверхплотная гетерогенная сетевая архитектура Het-Nets [2], вопрос взаимодействия разнообразных устройств между собой без участия базовой станции является одним из основных. Гетерогенные сети Het-Nets отличаются наличием множества частотных диапазонов, применением различных технологий радиодоступа и использованием базовых станций с различными размерами зон покрытия. В ряде ситуаций, например, когда пользователи находятся близко друг от друга или специфичности информации для конкретного места использования, имеет смысл организация обмена данными непосредственно между устройствами «устройство-устройство» (D2D). В рамках стандартов LTE уже делаются первые шаги к интеграции D2D в коммуникационные технологии. Кроме того, D2D сможет послужить важным компонентом, поскольку позволяет использовать локальную связь даже в случае повреждения сетевой инфраструктуры.

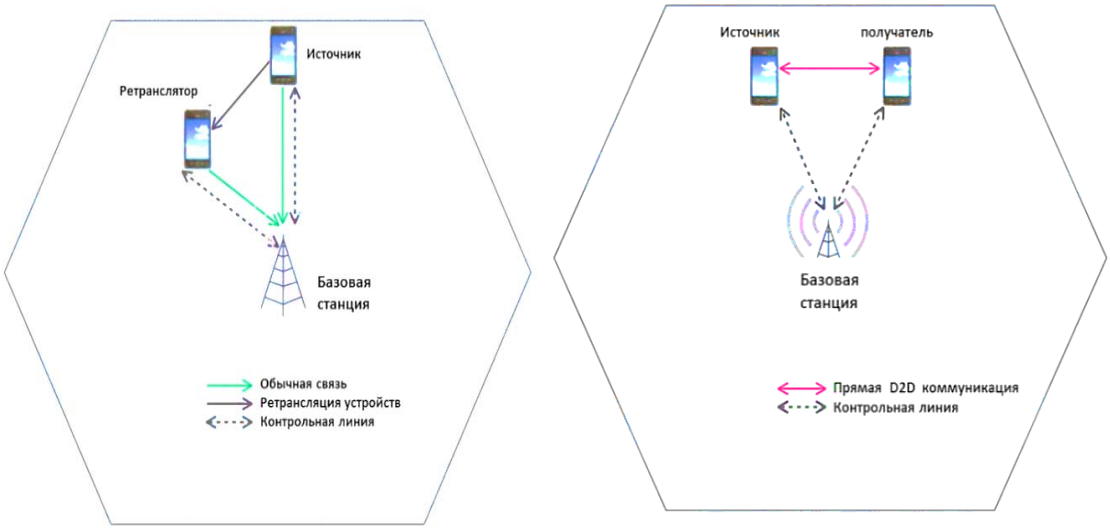
D2D-коммуникаций и основные его типы являются следующими:

D2D-коммуникации позволяют устройствам связываться друг с другом напрямую без маршрутизации данных через сетевую инфраструктуру.

Двухуровневая сеть 5G включает уровень макроячейки и уровень устройств. Макроячейка – базовая станция BS-to-device, как и в обычной сотовой системе [3]. Ниже рассматриваются четыре основных типа устройств уровня коммуникаций[4].

– Первый тип устройств уровня коммуникаций – устройства DR-OC (*Device relaying with operator controlled link establishment*). Устройства взаимодействуют с базовой станцией через ретрансляцию информации при помощи других устройств (рис. 1*а*).

– Второй тип устройств уровня коммуникаций – устройства DC-OC (*Direct D2D communication with operator controlled link establishment*). Имеет место прямое взаимодействие D2D-устройств, без участия базовой станции, но их взаимодействие координируется оператором (рис. 1*б*).

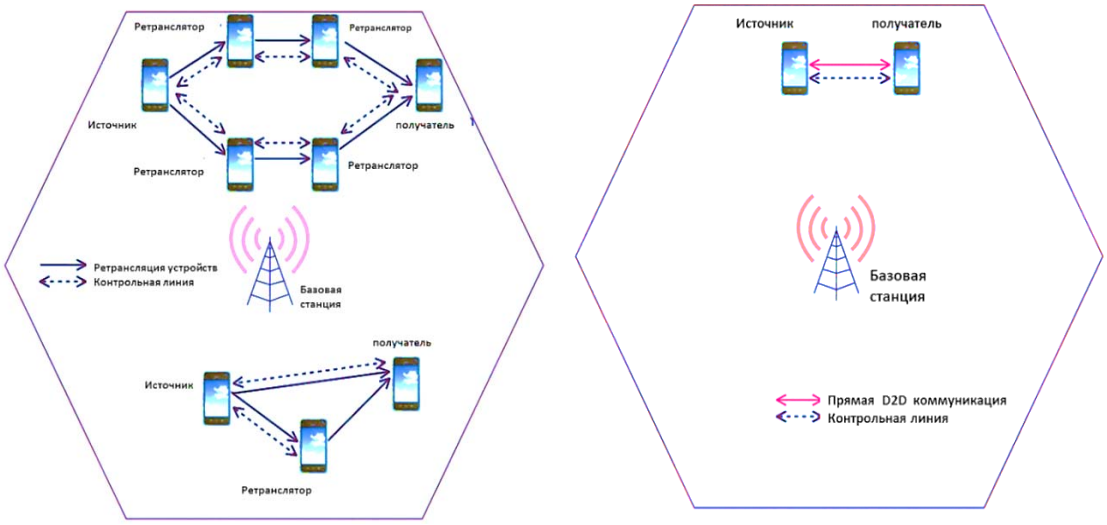


а) б)

Рис. 1. D2D-устройства: а) первого типа; б) второго типа

– Третий тип устройств уровня коммуникаций – устройства DR-DC. Устройства источника и получателя несут ответственность за координацию взаимодействия с использованием ретрансляторов. В этом случае устройства источника и потребителя имеют прямую связь друг с другом без какого-либо контроля со стороны оператора (рис. 2*а*).

– Четвертый тип устройств уровня коммуникаций – устройства DC-DC. устройства источника и назначения должны использовать ресурс таким образом, чтобы обеспечить ограниченный уровень помех для других устройств одного и того же уровня (рис. 2*б*).



а) б)

Рис. 2. D2D-устройства: а) третьего типа; б) четвертого типа

Методы кластерного анализа (КА) применимы, как в задачах научных исследований, так и в задачах прикладного характера [5]. Методы кластерного анализа дают возможность разбить исходное множество объектов на подмножества, на основе заданного критерия. Известные методы и алгоритмы кластерного анализа позволяют получить одно из возможных решений (близкое к оптимальному решению). В статье рассматриваются две задачи:

– выделение групп пользователей (мобильных терминалов) по различным критериям: расстояние BS-MS, MS-MS, загрузки каналов и др.;

– выбор головных узлов кластера по различным критериям: расстояние CH-MS (головной узел кластера – мобильный терминал), CH-BS, загрузки каналов и др. Решение задач кластеризации позволяет повысить пропускную способность и использование радиочастотного спектра, снизить загрузкуBS и величину потребляемой энергии. Выбор принципа выделения кластеров, в общем случае, представляет собой задачу, которая в конечном итоге определяет возможность решения поставленной задачи КА. Выбираемый метод кластеризации должен позволять сформулировать критерии оценки степени близости (схожести) объектов в рамках кластеров. В данной статье рассмотрены два принципа выделения кластеров;

– выделение априорно заданного числа кластеров; число кластеров может определяться на базе данных о числе локальных групп пользователей, числе предоставляемых услуг, категорий качества обслуживания и др.;

– выделение кластеров априорно заданного «размера». Размер кластера может определяться, например, радиусом связи MS-MS или MS-BS, требованиями к QoS.

Таким образом, можно сформировать следующие выводы:

1. Технология D2D в сетях 5G позволяет существенно расширить возможности по взаимодействию между пользователями сети. Что дает возможность: повышения использования радиочастотного спектра, повышения качества предоставления услуг, Снижение энергопотребления и др. возможности

2. При организации связи D2D требуется учитывать различные факторы, такие как: Расположение пользователей (групп пользователей), интенсивность трафика, требования к QoS, набор услуг и др.

3. Для решения поставленных задач могут быть использованы методы кластерного анализа (кластеризации) которые позволяют выделять группы пользователей по различным признакам. Решение задач кластеризации позволяет повысить эффективность использования D2D.

Список используемых источников

1. Футахи А., Кучерявый А. Е., Кучерявый Е. А. LTE и беспроводные сенсорные сети // Мобильные телекоммуникации. 2012. № 11. С. 38–41.
2. Koucheryavy Y., Andreev S., Pyattaev A., Johnsson K., and Galinina O. Cellular traffic offloading onto network-assisted device-to-device connections // IEEE Communications Magazine, vol. 52, no. 4. PP. 20–31, 2014.
3. Muthanna A., Masek P., Hosek J., Fujdiak R., Hussein O., Paramonov A., Koucheryavy A. Analytical Evaluation Of D2D Connectivity Potential in 5G Wireless Systems // Lecture Notes in Computer Science. 2016. T. 9870. PP. 395–403.
4. Mohsen Nader Tehrani, Murat Uysal, and Halim Yanikomeroglu. Device-to-Device Communication in 5G Cellular Networks: Challenges, Solutions, and Future Directions // IEEE Communications Magazine, vol. 52, no. 5, pp. 86–92, May 2014.
5. Кучерявый А. Е., Парамонов А. И., Кучерявый Е. А. Сети связи общего пользования. Тенденции развития и методы расчёта. М. : ФГУП ЦНИИС, 2008. 290 с.

УДК 004.056

ЗАЩИТА СЕТИ ОТ МНОГОСТУПЕНЧАТЫХ АТАК НА ОСНОВЕ Т ЕОРИИ ИГР

Р. С. Подоляк

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

Взаимодействия между злоумышленниками и сетевым администратором моделируются как несовместимая динамическая игра без нулевой суммы с неполной информацией, которая учитывает неопределенность и особые свойства многоступенчатых атак. Модель представляет собой подход с фиктивной игрой вдоль специального игрового дерева, когда атакующий является лидером, а администратор - последователем.

безопасность сетей, теория игр, деревья атак.

Повышенная зависимость от сетевых приложений и сервисов делает безопасность сети важной проблемой, а обнаружение вторжений и защита сетей от атак является централизованным. Теория игр – это подходящая методология для моделирования взаимодействия между злоумышленниками и сетевым администратором и определения лучшей стратегии противодействия атакам. Однако есть некоторые трудности в прямом применении теории классической игры, так как стратегии атакующего неясны, их шаги не мгновенны, правила игр могут со временем меняться и т. д. Поэтому любая методология, основанная на теории игр, должна учитывать эти трудности.

В последние годы интенсивно развиваются и изучаются механизмы реагирования на сетевые атаки. Например, в приведенных ниже работах используются различные способы представления сценариев атак и построения деревьев атак для анализа защищенности сети: деревья атак [1], формальные грамматики [2], раскрашенные сети Петри [3], метод анализа изменения состояний [4], описательные модели сети и злоумышленников [5], структурированное описание на базе деревьев [6], использование и создание графов атак для анализа уязвимостей [7], объектно-ориентированное дискретное событийное моделирование [8], модели, основанные на знаниях [9] и т. д.

Существует достаточно большое множество различных видов вторжений. Многоступенчатые атаки – самые разрушительные и самые сложные для любой системы защиты. Они используют интеллект для стратегической компрометации целей в запланированной последовательности действий, поэтому обычная методика, предназначенная для защиты от одноступенчатых атак, в данном случае не работает.

1 Моделирование последствий

Последствия любой атаки и любых действий во время многоступенчатой атаки основаны на следующих шести шагах:

1) Определение категории воздействия.

2) Указание важности каждой категории относительно других.

3) Определение мер воздействия для каждой категории.

4) Определение отношения между физическими эффектами и мерами воздействия.

5) Определение системы и ее пользователей.

6) Определение событий с точки зрения масштабов и влияния сетевой системы.

Категории воздействия не ограничиваются экономическими соображениями, имиджем, безопасностью и неприкосновенностью частной жизни. Их относительные факторы важности могут быть оценены с помощью любой из хорошо известных процедур из многокритериального принятия решений. Общий подход к получению весов основан на параллельных сравнениях, когда всем участникам процесса принятия решений предлагается дать относительные факторы важности для всех пар категорий. Затем результаты суммируются в окончательный набор значимых весов либо путем их усреднения, либо с использованием процесса аналитической иерархии (ПАИ). Меры воздействия в разных категориях обычно даются в разных единицах, и их можно объединить с помощью теории атрибутов с несколькими атрибутами или метода взвешивания с нормализованными оценками. Показатели эффективности могут быть определены для категорий воздействия,

и каждая оценка эффективности может быть разделена на набор построенных шкал, представляющих степень воздействия физических последствий на сеть и ее пользователей, включая упущенную выручку, ремонт и/или замещающую стоимость, ущерб от потери или кражи информации и т. д. Любая фактическая атака оказывает влияние на разные категории с разными уровнями. Используя инструмент моделирования последствий, общий результат различных типов и масштабов событий в системе и ее пользователей можно оценить в одном комбинированном значении. Это значение должно быть вычислено во всех состояниях многоступенчатой атаки и будет использоваться в анализе дерева игр.

2 Игровое дерево и узлы решений

Многоступенчатые атаки представлены особыми игровыми деревьями. На рис. показаны первые два взаимодействия в игровом дереве. Корнем дерева является начальный узел решения атакующего, а возможные начальные шаги атакующего представлены дугами, происходящими от корня. Эти действия могут включать атаку на сервер с различными уровнями интенсивности, отправку вируса группе клиентов и т. д. В конце каждой дуги администратор должен выполнить ответные действия, поэтому они являются его узлами решения.

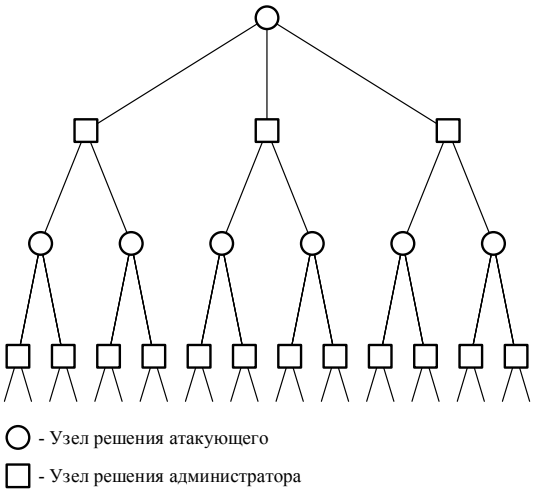


Рисунок. Специальное игровое дерево

После ответа администратора атакующий делает следующий ход и так далее. Это дерево непрерывно, пока злоумышленник не прекратит атаку или не достигнет своих целей. Это дерево может стать очень большим, а значения выигрыша в узлах решения неопределенны, поэтому классический метод, известный как обратная индукция, не может быть использован в этом случае.

3 Определение оптимальных ответов

Алгоритм, который будет описан в этом разделе, является процедурой реального времени, он обеспечивает наилучший ответ администратора на каждом из его узлов решения, когда многоступенчатая атака достигает этого конкретного узла игрового дерева. Поэтому во время атаки алгоритм можно использовать на каждом этапе, чтобы найти лучший следующий ход

администратора, начиная сразу после первого действия злоумышленника и продолжая до конца игры.

Рассмотрим теперь конкретный узел решения администратора и дерево, в котором этот узел является его корнем. График времени для этого дерева получается следующим образом – необходимо проверить все конечные точки дерева, в которых злоумышленник достигает своих целей во время наименьшего числа шагов, поэтому выбирается самый короткий путь с наименьшим количеством дуг от корня до таких конечных точек. Длина кратчайшего пути – это временной горизонт, а затем все пути, начинающиеся с корня, будут учитываться только до этого временного горизонта. Затем функция полезности атакующего оценивается во всех концах этого усеченного дерева подзаголовков. Функция полезности представляет собой линейную комбинацию ожидаемого выигрыша злоумышленника и его дисперсии, как было объяснено ранее. Коэффициент риска для злоумышленника может быть обновлен после каждой атаки, поскольку администратор оценивает ожидания и отклонения его значений полезности для всех возможных ходов, а также наблюдает за фактическим ходом. Затем администратор должен оценить распределение вероятностей действий злоумышленника на всех своих узлах решения. Значения вероятности вычисляются на основе оценочных значений полезности злоумышленника, а также предыдущих взаимодействий с атакующим. Сначала значения вероятности вычисляются пропорционально значениям полезности в концах разных дуг, представляющих следующие движения атакующего, и, если предыдущие взаимодействия обеспечивают относительные частоты, они усредняются с вычисленными вероятностями. Используя эти распределения вероятностей, математическое ожидание и дисперсия кумулятивного воздействия вплоть до временного горизонта для администратора могут быть рассчитаны для каждого из возможных ответов, а соответствующие значения полезности получаются путем объединения ожиданий и отклонений с коэффициентом приемлемости риска для администратора. Лучший ответ администратора – это дуга, которая имеет самую высокую полезную ценность.

Выводы

В этой статье была представлена многоступенчатая защита системы от вторжений, где взаимодействия между атакующим и администратором моделируется как беспроигрышная динамическая игра без нулевой суммы с неполной информацией о системе. Два игрока проводят фиктивную игру вдоль игрового дерева, которое может помочь администратору быстро найти лучшие стратегии защиты от атак, запущенных различными типами

злоумышленников. Данных алгоритм представляет собой процедуру в реальном времени, которая дает наиболее выгодный ответ администратора на любом этапе игры, поэтому его необходимо повторять на всех фактических узлах решения администратора. Данный алгоритм отличается от обычных методов, основанных на деревьях решений, так как на каждом шаге рассматривается только конечный горизонт, вместо ожидаемых результатов используются определенные эквиваленты, а вероятности разных дуг постоянно обновляются на основе новой информации.

Список используемых источников

1. Sheyner O., Haines J., Jha S., Lippmann R., Wing J. M. Automated generation and analysis of attack graphs // Proceeding of the IEEE Symposium on Security and Privacy. 2002. PP. 273–284.

2. Gorodetski V., Kotenko I. Attacks against Computer Network: Formal Grammar-based Framework and Simulation Tool // Lecture Notes in Computer Science. New York: Springer-Verlag, 2002. Vol. 2516. PP. 219–238.

3. Yuill J., Wu F., Settle J., Gong F. Intrusion-detection for incident-response, using a military battlefield-intelligence process // Computer Networks. 2000. No. 34. PP. 671–697.

4. Chung M., Mukherjee B., Olsson R. A., Puketza N. Simulating Concurrent Intrusions for Testing Intrusion Detection Systems // Proceeding of the 1995 National Information Systems Security Conference. Baltimore, Maryland, October 10–13, 1995. PP. 173–183.

5. Kumar S., Spafford E. H. An Application of Pattern Matching in Intrusion Detection. Technical Report CSDTR 94 013. Purdue University, 1994.

6. Dawkins J., Campbell C., Hale J. Modeling network attacks: Extending the attack tree paradigm // In Workshop on Statistical and Machine Learning Techniques in Computer Intrusion Detection, Johns Hopkins University, 2002.

7. Iglun K., Kemmerer R. A., Porras P. A. State Transition Analysis: A Rule-Based Intrusion Detection System // IEEE Transactions on Software Engineering. 1995. Vol. 21, no. 3. PP. 181–199.

8. Chi S.-D., Park J. S., Jung K.-C., Lee J.-S. Network Security Modeling and Cyber Attack Simulation Methodology // Lecture Notes in Computer Science. New York: Springer-Verlag, 2001. Vol. 2119. PP. 320–333.

9. Shepard B., Matuszek C., Fraser C. B., etc. A Knowledge-based approach to network security: applying Cyc in the domain of network risk assessment // The Seventeenth Innovative Applications of Artificial Intelligence Conference (IAAI-05), 2005. PP. 1563–1568.

Статья представлена научным руководителем, кандидатом технических наук, доцентом А. В. Красовым.

УДК 004.72

АНАЛИЗ ПРИМЕНЕНИЯ МЕТОДОВ МАТЕМАТИЧЕСКОГО МОДЕЛИРОВАНИЯ В ПРОГРАММНО-КОНФИГУРИРУЕМЫХ СЕТЯХ

В. С. Пряжников

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

Математическое моделирование применяется при организации любых сетей и систем, предлагая возможность протестировать аналог будущей системы, традиционно в телекоммуникациях применялись теория массового обслуживания и теория графов. Технологический прогресс упростил организацию и архитектуру сетей, но привнес дополнительные условия для эксплуатации сетей, в результате чего в инфокоммуникации были привлечены новые методы математического моделирования.

программно-конфигурируемые сети, математическое моделирование, теория графов.

Математическое моделирование в целом широко и повсеместно применяется в инфокоммуникациях, что обусловлено наличием ряда преимуществ. Возможность математического моделирования представить любой процесс в виде модели и описать её аналитически позволяет относительно быстро и с наименьшими затратами глубоко исследовать любую модель и её характеристики, изменение состояний в зависимости от вариации характеристик. Например, имитационное моделирование, применяемое при построении сетей и систем, а также для изучения влияния изменений процессов и характеристик сети или системы на ее состояние, применяется при достаточно полном описании системы и позволяет получить аналог будущей системы со всеми свойственными ей характеристиками, таким образом собирается статистика, исходя из которой можно делать выводы о устойчивости и работоспособности системы. Математическое моделирование в общем виде опирается на аналитическое описание модели, постановку задачи и ее последующее решение. Для инфокоммуникаций традиционным является применение теории массового обслуживания и теории графов [1]. В телекоммуникациях теория графов в основном применялась при проектировании сетей и систем, а также для решения задач маршрутизации, однако технологический прогресс привел к появлению новых задач, которые можно решать с помощью теории графов, среди них стоит выделить задачи алгоритмизации, оптимизации, обеспечения безопасности, в частности обнару-

жение потенциальных угроз [2]. Теория массового обслуживания, а в частности её ответвление – теория телетрафика применяется для определения количественных показателей характеристик математических моделей. Совокупность вышеперечисленных методов предлагает возможность описать любую модель, сымитировать ее и просчитать ее количественные и качественные характеристики во всевозможных состояниях, что позволяет существенно сократит расходы и время при организации сетей и систем.

Необходимость решения задач управления, алгоритмизации, оптимизации, маршрутизации, выявления угроз и т. д. повлекло за собой использование новых, для инфокоммуникаций, аналитических методов описания математических моделей, которые можно охарактеризовать, как методы нечеткого определения результата, однако гарантирующие высокую эффективность своего использования: 1) Математическая теория катастроф. 2) Теория игр. 3) Теория нечетких множеств. 4) Метод эволюционного моделирования. 5) Эвристический алгоритм.

Математическая теория катастроф [3] – метод определения состояния объекта при приближении к окрестности точки катастрофы, применяется для определения устойчивости системы. Так как, при развитии любой системы, на которую постоянно влияют внешние факторы, неизбежна встреча ряда неустойчивых точек, то необходимо исследование поведения системы при прохождении этих точек, а также возможность определять приближение таких моментов. Теория игр – это аналитический метод, позволяющий определить оптимальную стратегию действий, для реализации интересов одного из участников процесса или равновесной реализации интересов всех участников процесса. Наибольшее применение в инфокоммуникациях теория игр находит в системах обнаружения вторжения и в качестве метода определения оптимального порядка действий, при обеспечении безопасности. В настоящее время существуют стратегии, являющиеся: средствами защиты от DoS/DDoS атак [4], обеспечением безопасности узловых систем обнаружения вторжений [5], реализацией ложных информационных систем [6]. Применение в моделировании теории нечеткого множества обусловлено необходимостью смоделировать процесс, при неполной, нечеткой информации о процессе [7]. Способность нечеткой логики определять промежуточные значения между бинарными состояния позволяет прогнозировать интервалы будущих значений, таким образом достигается принятие решения с достоверной вероятностью, за наименьшее время. Нечетко-множественное моделирование используется в системах управления технологическими процессами, а также, как модель мыслительных процессов в системах с искусственным интеллектом. В основе метода эволюционного моделирования лежит идея заменить моделирование процесса моделированием

эволюции процесса, т. е. так называемой мутацией. Под мутацией понимается изменение параметров системы, с целью попытки улучшения системы. Эвристическое моделирование – метод основанный на эвристическом алгоритме, т. е. алгоритм не являющийся оптимальным, однако верный с некоторой достоверностью и более быстрый, чем методы, однозначно выявляющие результат, метод широко применяется в различных областях, в том числе в системах с искусственным интеллектом и в автоматизированных системах управления. Метод эволюционных вычислений имеет широкое применение, в частности в системах с искусственным интеллектом, а также применяется, как метод моделирования направленный на оптимизацию процесса, подход не гарантирует обнаружение идеального состояния, однако гарантирует нахождение оптимального состояния за более короткое время, чем другие методы моделирования, носящие эвристический характер поиска. В статье [8] описан эксперимент с применением метода эволюционного моделирования, который в свою очередь использует метод нечеткой логики.

В настоящее время повсеместно идет активное внедрение программно-конфигурируемых сетей, что соответственно сопряжено с различного рода математическим моделированием. Непосредственная близость программно-конфигурируемых сетей с виртуальными технологиями, а также архитектура самих сетей, предполагает пониженные затраты на развертывание, внедрение и эксплуатацию сетей, однако ни один крупный проект не обходится без математического моделирования. Все вышеперечисленные методы математического моделирования находят применение и в программно-конфигурируемых сетях. Повышенное внимание в программно-конфигурируемых сетях отводится решению следующих задач: маршрутизация, балансировка нагрузки, отказоустойчивость, безопасность, QoS. Математическое моделирование позволяет проанализировать все эти задачи на этапе планирования сети. Как любая система массового обслуживания программно-конфигурируемая сеть позволяет произвести математическое моделирование любого процесса и рассчитать необходимое количество оборудования, архитектура сети позволяет в любое время масштабировать сеть, соответственно при первоначальном развертывании сети нет необходимости рассчитывать потенциальное увеличение количества будущих пользователей. В программно-конфигурируемой сети контроллер управляет всеми коммутаторами, что дает возможность применять разные маршруты для потоков, проходящих через сеть, исходя из приоритетности трафика. Такой подход позволяет повысить пропускную способность сети, поддерживать на необходимом уровне QoS и использовать сеть максимально продуктивно. Контроллер должен одновременно обеспечивать равномерную загрузку сети, поддерживать необходимое качество и строить кратчайший маршрут.

Для реализации данной возможности необходимо использование контроллером алгоритмов, решающих задачу построения минимального пути и вычисления максимального потока [9], подобные алгоритмы имеются в математическом аппарате теории графов [10]. Так как, в небольшой сети архитектура программно-конфигурируемых сетей предполагает наличие в сети всего двух различных компонент, контроллер в свою очередь соединен со всеми коммутаторами, то моделирование архитектуры сети идеально производить при помощи теории графов, оперируя показателем связности. Во время непрерывной работы, так или иначе будут отбрасываться некоторые потоки, что будет влиять на уровень загруженности коммутаторов, в связи с этим, а также в целях безопасности контроллер должен производить иногда полную реконфигурацию маршрутов. Сосредотачивая в себе все функции управления сетью, контроллер становится потенциально наиболее уязвимым компонентов сети, соответственно его безопасности следует уделять максимальное внимание, если в сети отсутствует резервирование и контроллер выйдет из строя, то сеть будет функционировать по уже заданным правилам, однако поступающие потоки для которых ранее не было задано правило, будут отброшены после истечения тайм-аута. Использование виртуальных технологий в программно-конфигурируемых сетях позволяет просто и без дополнительных затрат осуществлять меры безопасности в виде развертывания ложных информационных сетей.

Являясь открытой динамической диссипативной системой, программно-конфигурируемые сети согласно теории катастроф, являются циклически колеблющейся системой, соответственно в каждый момент времени состояние системы зависит от изменяющихся параметров системы, которые создают колебания, значит равновесие системы зависит от постоянного изменения этих параметров, иными словами, для равновесия системы управляющее устройство, в данном случае контроллер, должен изменять управляющие параметры сети таким образом, чтобы сеть циклически колебалась [11].

Подытожив стоит отметить, что простая архитектура программно-конфигурируемой сети, наряду с упразднением числа функций коммутаторов, а также при использовании виртуальных технологий, приводит к тому, что для полноценного математического моделирования достаточно использования традиционных методов, в частности совокупность теории графов и теории массового обслуживания вполне достаточно для решения задач: расчета количества необходимого оборудования, построения схемы развертывания сети, организации маршрутизации и оптимизации. Использование более сложных методов моделирования целесообразно в процессе эксплуатации, для обеспечения безопасности и отказоустойчивости.

Список используемых источников

1. Курилов Ф. М. Моделирование систем защиты информации. Приложение теории графов [Электронный ресурс] // Технические науки: теория и практика: материалы III Междунар. науч. конф. г. Чита, апрель 2016 г. Чита : Издательство Молодой ученый, 2016. С. 6–9. URL: https://moluch.ru/conf/tech/archive/165/9766/ (дата обращения 15.01.2018).

2. Васильева М. В., Додонова Н. Л. Применение теории графов в кодировании и декодировании информации [Электронный ресурс] // Научное сообщество студентов XXI столетия. Технические науки: материалы XXIX междунар. студ. науч.-практ. конф № 2 (28). Новосибирск 26 февраля 2015 г. Новосибирск : Издательство «СибАК», 2015. С. 127–139. URL: http://sibak.info/archive/technic/2(28).pdf (дата обращения 16.01.2018).

3. Арнольд В. И. Теория катастроф. 3-е изд., доп. М. : Наука, 1990. 128 с.

4. Абденов А. Ж., Заркумова Р. Н. Выбор средства эффективной защиты с помощью методов теории игр [Электронный ресурс] // Вопросы защиты информации. 2010. № 2. С. 26–31. URL: http://elibrary.ru/item.asp&id=14571051 (дата обращения 17.01.2018).

5. Лаврентьев А. В., Зязин В. П. О применении методов теории игр для решения задач компьютерной безопасности [Электронный ресурс] // Безопасность информационных технологий. 2013. № 3. С. 19–24. URL: http://elibrary.ru/item.asp&id=21103573 (дата обращения 17.01.2018).

6. Шматова Е. С. Выбор стратегии ложной информационной системы на основе модели теории игр [Электронный ресурс] // Вопросы кибербезопасности. 2015. № 5. С. 36–40. URL: http://cyberrus.com/wp-content/uploads/2015/12/36-40-513-15_7.-Шматова.pdf (дата обращения 17.01.2018).

7. Погорелов А. С. Применение теории нечетких множеств для задачи выбора альтернатив в условии неопределенности [Электронный ресурс] // Программные продукты и системы: науч.-практ. журн. 2013. № 3. С. 28–31. URL: http://swsys.ru/index.php?page=article&id=3554 (дата обращения 16.01.2018).

8. Волканов Д. Ю. Метод сбалансированного выбора механизмов обеспечения отказоустойчивости для распределенных вычислительных систем [Электронный ресурс] // Моделирование и анализ информационных систем. 2016. № 2. С. 119–136. URL: http://elibrary.ru/item.asp&id=25810346 (дата обращения 18.01.2018).

9. Корзинков А. Д. Новый алгоритм решения задачи о максимальном потоке [Электронный ресурс] // Наука и техника. 2013. № 5. С. 70–75. URL: http://cyberleninka.ru/article/n/novyy-algoritm-reshenya-zadachi-o-maksimalnom-potoke (дата обращения 20.01.2018).

10. Черников А. С., Паус А. С. Многопоточная маршрутизация в программно-конфигурируемых сетях [Электронный ресурс] // Радиооптика. 2016. № 6. С. 35–46. URL: http://radiooptics.ru/doc/850725.html (дата обращения 10.01.2018).

11. Юрчик П. Ф., Голубкова В. Б., Гусеница Д. О. Информационная поддержка работоспособности компьютерных систем методами теории катастроф [Электронный ресурс] // Автоматизация и управление в технических системах. 2013. № 3. С. 52–56. URL: http://auts.esrae.ru/pdf/2013/3(5)/99.pdf (дата обращения 21.01.2018).

Статья представлена научным руководителем, кандидатом технических наук, доцентом В. С. Елагиным.

УДК 621.395.7

ПЕРЕХОД К ЭНЕРГОСБЕРЕГАЮЩИМ СЕТЯМ NG-PON

Б. К. Резников, А. Р. Салтыков

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

Анализ и разработка энергоэффективных решений, которые могут быть применены в пассивных оптических сетях следующего поколения, являются важными задачами. В статье рассмотрены механизмы сбережения энергии путем управления режимами сна и передачи на абонентских устройствах.

PON, пассивные оптические сети, OLT, ONT, энергосбережение, режим сна, цикл DBA.

Видео-ориентированные приложения и сервисы, такие как HDTV, VoD, активно внедряются и развиваются в сетях доступа. По сравнению с традиционными голосовым и дата-трафиком, такие мультимедийные приложения потребляют значительную часть полосы пропускания канала.

Очевидно, что с увеличением линейной скорости передачи увеличивается и потребление электроэнергии системами пассивных оптических сетей следующего поколения – NG-PON (*New Generation Passive Optic Network*). Эта проблема становится серьезным поводом для беспокойства операторов связи. Кроме этого, увеличение потребления электроэнергии затрагивает аспекты окружающей среды и, как следствие, социальные и экономические аспекты. Абонентские устройства ONU/ONT имеют самый высокий уровень потребления энергии в расчете на 1 бит передаваемой информации и суммарно потребляют более 65 % от общей потребляемой сетями PON электроэнергии.

Режимы приемопередачи

В общем, передатчик ONT работает в пакетном режиме (*burst mode*), то есть, способен быстро переключаться и включаться (*turn on/off*) в интервалах незанятости (*idle* TSL) для предотвращения добавления шумов в восходящие потоки от других ONT.

С приемником ONT данная процедура гораздо сложнее, поскольку для выполнения включения и выключения потребуются дополнительные издержки на синхронизацию для восстановления внутренних часов из информации в нисходящем потоке от OLT.

В режиме сброса энергии (*shedding*), когда ONT работает от АКБ, питание отключается, либо потребляемая мощность уменьшается до несущественного предоставления услуг (управление сетью, телефония).

В режиме дрейфа (*dozing*) ONT принимает нисходящие пакеты, но выключает передатчик и игнорирует запросы DBA OLT, когда нечего передавать.

В режиме сна (*sleeping*) ONT виртуально отключает все сервисы и достигает максимального потенциала энергосбережения.

Adaptive Link Rate – адаптивная скорость передачи (ALR) может быть достигнута за счет способности выбрать скорость передачи (из набора доступных) динамически. Что касается энергоэффективности, ALR широко используется в беспроводных сетях. Чем выше выбранная скорость, тем выше потребляемая мощность.

Сравнение режимов работы ONT-устройств показывает, что оптимальным с точки зрения энергопотребление режимом является режим сна. Полное отключение всех функций не устраивает операторов. Например, обязательно должна работать Система-112 – система обеспечения вызова экстренных оперативных служб по единому номеру «112» на территории Российской Федерации. Поэтому sleep mode не устраивает операторов связи.

Режим дрейфа dozing дает большую гибкость, так как держит активным downstream канал. В таком случае OLT может отправить отчет в любое время, чтобы ускорить пробуждение.

Способ решения задачи снижения энергопотребления

В ходе анализа проблемы энергопотребления одним из наиболее эффективных методов может являться переход абонентских устройств ONT в режим минимального потребления энергии. Вследствие этого особый акцент уделен описанию механизма управления «спящим режимом» ONT, с возможностями управления трафиком и уведомления о состоянии «сна».

Уменьшение энергопотребления системами NG-PON требует соответствующих исследований, как на физическом уровне, так и на уровне управления доступом к среде передачи (MAC). Нами рассматривается эволюционный переход от систем PON к системам NG-PON на примере 10G-EPON и обсуждаются возможности перехода ONT в режим низкого энергопотребления [1].

Помимо сценария управления нисходящим трафиком, также необходим эффективный механизм контроля режима сна для передачи сообщений протокола MPCP и восходящего трафика. Для передачи в восходящем направлении выход ONT из режима сна может быть инициирован прибывающим восходящим трафиком. При этом данный прибывающий трафик

не может быть передан до тех пор, пока ONT не информировано о времени назначения полосы пропускания со стороны OLT.

Исследования показали, что можно использовать метод сна и периодического пробуждения (*sleep and periodic wake-up* – SPW). ONT находится в режиме сна и периодически происходит обмен сообщениями между OLT и ONT для определения того, должен ли ONT пробуждаться.

Для предотвращения коллизий SPW требует время на подготовку между окончанием периода сна и сообщением подтверждения. Это происходит, так как внутренние часы ONT (внутренняя синхронизация) находятся в свободном режиме, поскольку приемник переведен в fast sleep mode. Поэтому необходимо внедрение схемы восстановления синхронизации и протокола синхронизации.

Существующие схемы восстановления синхронизации тратят миллисекунды для восстановления синхронизации с OLT. После этого ONT еще требуется синхронизироваться с сетью для того, чтобы отправлять сообщения в восходящем направлении. В общем, продолжительность периода сна, как ожидается, последние несколько циклов предоставления DBA в режиме быстрого спящего режима ONT является наиболее эффективной с точки зрения энергосбережения, когда ONT имеет очень слабый трафик. Отметим, что данный метод не накладывается на процедуру DBA.

OLT может недооценить нагрузку в нисходящем потоке и внести нежелательные задержки для нисходящего трафика, запрашивая длинный период сна. OLT также может переоценить нагрузку в нисходящем потоке и оставить ONT активными без эффективного использования полосы пропускания в нисходящем потоке. Более того, SPW независимо определяет время сна без использования информации в отчетах ONU. Как результат, SPW может часто требовать сон и пробуждение, что негативно скажется на задаче энергосбережения.

Как указано на рис. 1, два уровня мощности потребления – «all: awake» и «all: sleep» – являются результатом при полном помещении ONT в «спящий режим». В дополнение [2] можно предложить несколько новых режимов: «Rx: sleep» и «Tx: sleep». Когда ONT находится в статусе «all: awake», если нет необходимости в работе передатчика Tx, оно переходит в статус «Tx: sleep» и затем – в статус «all: sleep», если также нет необходимости в работе приемника Rx. В статусе «all: sleep», помимо Rx и Tx, в «спящий режим» также переходят ONU/ONT MAC и SERDES. Аналогично происходят переходы между состояниями «all: awake», «Tx: sleep» и «Rx: sleep». Переходы между данными статусы должны быть спроектированы таким образом, чтобы минимизировать потребление энергии без деградации предоставляемых сервисов.

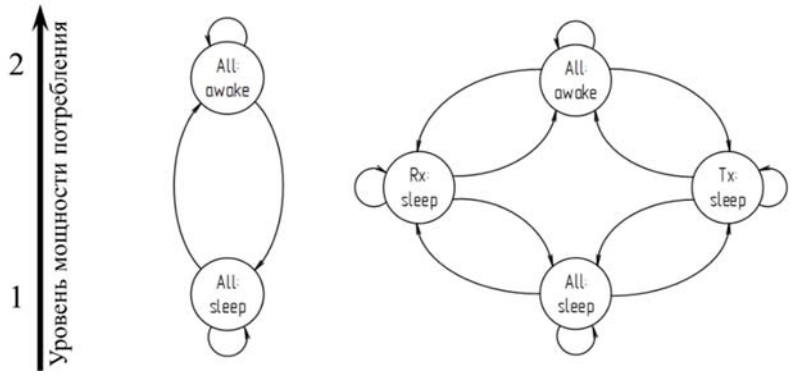


Рис. 1. Конечный автомат режимов ONU и потребление мощности:
1 – низкий уровень, 2 – высокий уровень

Схема восстановления синхронизации на ONT отличается для каждого из режимов передачи. В режиме пакетной передачи при входе в состояние энергосбережения отключается схема приемника (с фотодетектором). В непрерывном режиме все остается в активном режиме (рис. 2).

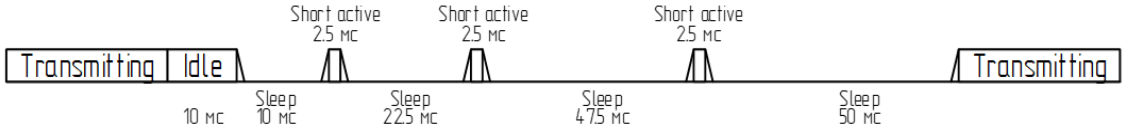


Рис. 2. Временная диаграмма активности ONT

Рассмотрим дерево PON с 64 абонентскими устройствами ONT. В период цикла DBA, в среднем, только 1/64 от общего времени предназначается для конкретного ONT. Это обозначает, что даже при наличии восходящего/нисходящего трафика, Tx/Rx будет находиться в состоянии активности только 1/64 от общего времени, а остальное время будет в состоянии сна. Поэтому может быть достигнута значительная экономия потребляемой энергии.

Чтобы разрешить ONT находиться в состоянии сна и активности в период одного цикла DBA, время перехода между состояниями sleep и awake должно быть меньшим, чем половина длительности цикла DBA. При этом чистое время состояния сна может быть значительно выше нуля – таким образом, происходит сохранение энергии (рис.2).

Планирование трафика (scheduling)

Здесь можно установить правило, согласно которому OLT не будет назначать / планировать для данного ONT трафик в течение определенного времени после окончания текущего цикла планирования трафика [3]. На рис. 3 показан пример перехода ONT в состояние сна в пределах одного

цикла DBA. В данном примере к OLT подключены 4 устройства ONT. Рассмотрим периоды сна ONU #4.

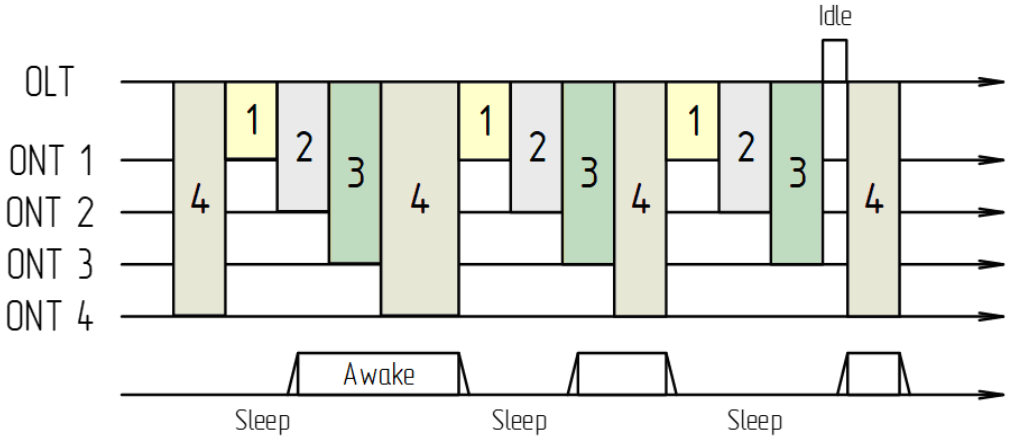


Рис. 3. Сон в период цикла DBA

Интервал между первыми двумя циклами планирования трафика для ONT #4 равен Δ. Таким образом, OLT не будет назначать / планировать для данного ONT трафик до прохождения отметки равной 0,8Δ условных временных интервала: в течение этого времени ONT может находиться в состоянии сна, а затем переходить в активное состояние. Однако данный переход в активное состояние является «ранним» переходом, поскольку фактическая передача трафика через другие ONT дольше оцененного времени и ONT до момента прихода своего трафика будет бездействовать.

При «позднем» пробуждении появится время ожидания idle, которое также является нежелательным, поскольку влияет на другие ONT-устройства сети.

В случае восходящего потока переход передатчика Tx ONT в состояние активности может быть инициирован с помощью ONU/ONT MAC в момент назначенного времени. После передачи информации Tx может переходить в состояние сна. Однако, в случае нисходящего потока достаточно сложно достигнуть такого, поскольку оптический приемник Rx не знает момента времени отправки нисходящего трафика, вследствие чего проверяет каждый нисходящий пакет.

Как было показано, «ранний» и «поздний» переходы в активное состояние являются двумя общими явлениями в данном механизме работы. «Ранний» переход подразумевает, что энергия может быть сохранена впоследствии, в то время как «поздний» переход затрагивает время ожидания, таким образом, повышая вероятность деградации сервисов. С точки зрения оператора связи преодоление «позднего» перехода с последующей деградацией сервисов более желательно, чем преодоление «раннего» перехода.

Список используемых источников

1. IEEE 802.3av Amendment: Physical Layer Specifications and Management Parameters for 10Gb/s Passive Optical Networks.
2. Raisa O. C. Hirafuji. The Watchful Sleep Mode: A New Standard for Energy Efficiency in Future Access Networks // IEEE Communications Magazine, August 2015, PP. 150–156.
3. Wong S. Sleep Mode for Energy Saving PONs: Advantages and Drawbacks. GLOBECOM Workshops, 2009 IEEE. PP. 1–6.

Статья представлена заведующим кафедрой, кандидатом технических наук, доцентом С. Ф. Глаголевым.

УДК 654.152

МЕТОД БЫСТРОЙ ОЦЕНКИ ШЕННОНОВСКОЙ ПРОПУСКНОЙ СПОСОБНОСТИ СИММЕТРИЧНОГО ТРАКТА «ДЛИННОГО» ETHERNET

А. Б. Семенов

Национальный исследовательский Московский государственный строительный университет

В предположении построения кабельной линии передачи сигналов сетевых интерфейсов Fast Ethernet на электропроводной симметричной элементной базе рассмотрен алгоритм быстрой оценки шенноновской пропускной способности. Метод применим к кабельным трактам, построенным по схеме direct connection, и востребован при разработке перспективных информационных систем на базе IP-техники для подключения к информационной системе одиночных удаленных терминальных устройств.

NEXT, шенноновская пропускная способность, симметричный кабельный тракт, сеть, Fast Ethernet.

Развитие информационных технологий и их проникновение во все сферы современной жизни сопровождается увеличением количества сервисов, предоставляемых информационно-телекоммуникационной системой (ИТС). В основу аппаратной реализации отдельных частей ИТС положена технология Ethernet. Такой подход дает возможность в полной мере использовать известные преимущества унификации.

Классические сети Ethernet как средство построения локальной сети тяготеют к многоуровневой модели построения. На их физическом уровне используются проводные каналы связи на кабелях из витых пар. Правила построения и характеристики такой проводки нормируются стандартами

на структурированные кабельные системы (СКС), содержащими ряд ограничений, в т. ч. предельную 100-метровую протяженность тракта.

Внедрение новых информационных сервисов, напротив, часто требует централизованной схемы. Переход на такую модель выгоден:

– в случае низкой плотности терминальных устройств, обслуживаемых сетью;

– при выдвижении особых требований в отношении конфиденциальности передаваемой информации;

– при работе в реальном масштабе времени, что влечет за собой ужесточение требований по задержке передаваемых пакетов.

В ситуациях ее использования необходимо увеличение протяженности симметричных трактов свыше 100 м. Подобные решения востребованы:

– в системах цифрового видеонаблюдения;

– в информационных системах крупных торговых центров и объектов проведения культурно-массовых мероприятий;

– на оконечных участках сетей доступа провайдеров Интернет, работающих в районах малоэтажной застройки.

Линии проводной связи новых сервисов обладают следующими особенностями [1]:

– от них не требуется скорость передачи свыше 100 Мбит/с;

– их реализация часто выполняется по схеме direct connection, рис. 1.

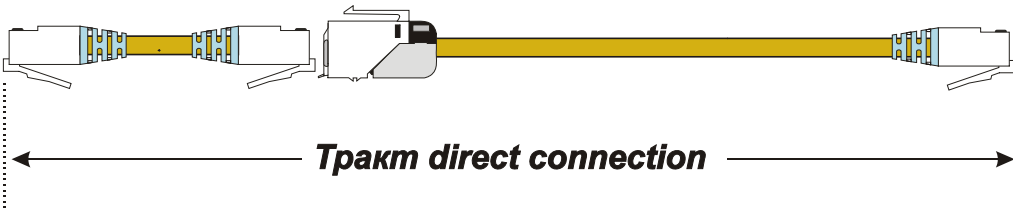


Рис. 1. Структура тракта «длинного» Ethernet

Анализ параметров таких линий часто удобно осуществлять по теории К. Шеннона.

Выходной сигнал передатчиков интерфейсов Ethernet с информационными скоростями не свыше 100 Мбит/с близок к белому шуму. Одновременно, отношение сигнала к шуму в симметричном тракте, задаваемое параметром ACR, является частотно-зависимой величиной. С учетом этой особенности шенноновская пропускная способность тракта составит:

$$W(L) = \int_0^\infty \log_2[1 + ACR(f, L)]\, df, \qquad (1)$$

где $ACR = NEXT - \alpha L$ – защищенность на ближнем конце; $NEXT$ – переходное затухание на ближнем конце; α – коэффициент затухания; L – «электрическая» длина. Нулевой нижний предел интегрирования выбран для удобства вычисления и не сказывается на точности.

На основании требований стандарта ISO/IEC 11801 [2] для трактов типа direct connection:

$$NEXT = -20\lg\left[10^{-\frac{NEXT_0}{20}} \cdot f^{0,75} + 10^{-\frac{NEXT_1}{20}} f\right] \cong$$
$$\cong NEXT_0 - 15\lg f - 20\lg\left[1 + 10^{-\frac{\Delta}{20}} \cdot f^{0,25}\right], \quad (2)$$

где $NEXT_0$ и $NEXT_1$ – переходное затухание ближнего конца кабеля и разъема, соответственно, $\Delta = NEXT_1 - NEXT_0$.

При вычислениях (1) удобно воспользоваться разбиением интервала интегрирования на две части $[0; f_b]$ и $[f_b; \infty]$ с последующим представлением результата в трехчленной форме $W = I_1 + I_2 + I_3$ согласно рис. 2.

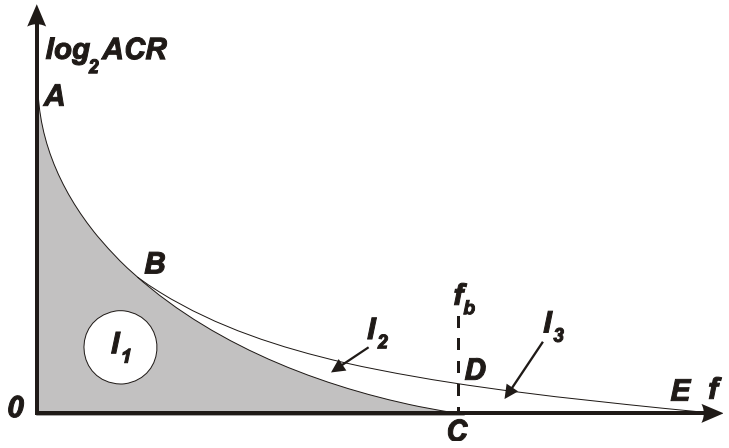


Рис. 2. К вычислению шенноновской пропускной способности симметричного тракта direct connection

Оценка $I_1 - I_3$ дает:

$I_1 = \sum_{j=1}^{4} I_{1j}$,

$I_{11} = -0,166 \cdot NEXT_0 \cdot f_b$, $I_{12} = 1,15 \cdot e^{-0,115\Delta} \cdot f_b^{1,25}$,

$I_{13} = -1,08 \cdot f_b \cdot (\ln f_b - 1)$, $I_{14} = -0,11 \cdot f_b^{1,5} \cdot \alpha L$,

$I_2 = \frac{2,88}{0,115\alpha L} \cdot 10^{-\frac{NEXT}{20}} \cdot e^{0,115\alpha L\sqrt{f_b}} \cdot [f_b - \frac{2\sqrt{f_b}}{0,115\alpha L} + \frac{2}{(0,115\alpha L)^2}]$,

$I_3 = \frac{2,88 \cdot 10^{NEXT/20}}{0,144 \cdot \alpha L \cdot f_b^{1,75}}$.

f_b как верхняя граничная частота симметричного тракта представляет собой корень уравнения [3] (рис. 3):

$$NEXT_0 - 15\lg f - 0{,}434 \cdot e^{-0{,}115\Delta} \cdot f^{0{,}25} - \alpha L\sqrt{f} = 0. \qquad (3)$$

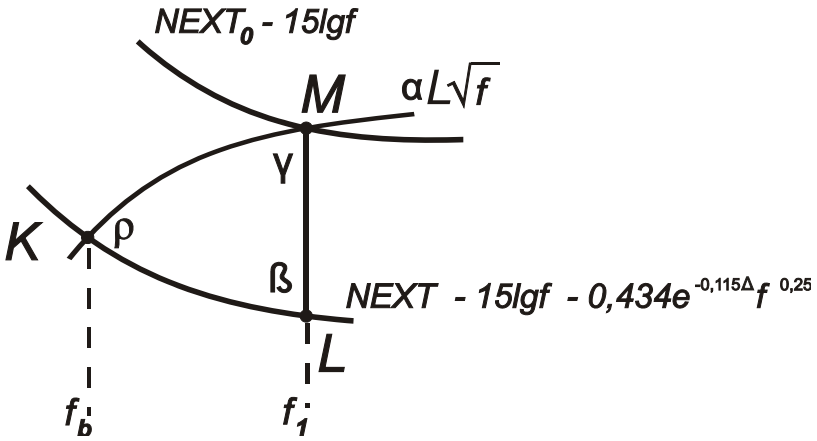


Рис. 3. К расчету верхней граничной частоты симметричного тракта

Представленные соотношения обеспечивают приемлемую для анализа ошибку, но из-за громоздкости мало пригодны для выполнения инженерных расчетов. Для устранения этого недостатка воспользуемся тем, что в диапазоне изменения параметров *NEXT,* α и *L* справедливо $I_1 : I_2 : I_3 \approx$ const. Это является прямым следствием подобия треугольников A0C, ABC и BCD. С учетом этого для трактов Fast Ethernet получаем:

$$W = 1{,}57 \cdot I_1. \qquad (4)$$

Из записи

$$I_1 = f_b \cdot \begin{pmatrix} 0{,}166 \cdot NEXT_0 - 1{,}15 \cdot e^{-0{,}115\Delta} \cdot f_b^{0{,}25} - \\ -1{,}08 \cdot (\ln f_b - 1) - 0{,}11 \cdot f_b^{0{,}5} \cdot \alpha L \end{pmatrix}$$

следует малое отличие функции $I_1(f_b)$ от линейной. Эта особенность позволяет перейти от аддитивной формы ее представления к мультипликативной. Тогда с учетом (4) имеем:

$$W = 0{,}44 I_{11} = 0{,}115 NEXT_0 f_b. \qquad (5)$$

Из (5) следует, что $\frac{\partial W}{\partial f_b} >> 1$, поэтому достижение высокой точности расчета требует минимизации ошибки определения f_b.

Для нахождения корня трансцендентного уравнения (3) применим двухшаговую процедуру. Сначала решается его «усеченный» вариант:

$$NEXT_0 - 15\lg f - \alpha L\sqrt{f} = 0.$$

Обращение к методу малого параметра после двух итераций дает:

$$f_1 = (\frac{NEXT_0}{\alpha L} + \varepsilon_1 + \varepsilon_2)^2,$$

где $\varepsilon_1 = -\frac{13}{\alpha L} \cdot \ln \frac{NEXT_0}{\alpha L} / (1 + \frac{13}{NEXT_0})$ и

$$\varepsilon_2 = -\frac{NEXT_0 - 13 \ln\left(\frac{NEXT_0}{\alpha L} + \varepsilon_1\right) - \alpha L(\frac{NEXT_0}{\alpha L} + \varepsilon_1)}{\frac{13}{\frac{NEXT_0}{\alpha L} + \varepsilon_1} + \alpha L}.$$

Далее на основании эскиза рис. 3: $f_b = f_1 - h$, где h – высота криволинейного треугольника KLM на основание LM.

Принимая во внимание небольшое отличие криволинейного треугольника KLM от обычного с привлечением теоремы синусов получаем:

$$h = ML \frac{\sin\gamma}{\sin\rho} \cos\beta.$$

Далее:

$$\gamma = \frac{\pi}{2} - \operatorname{arctg} \frac{\alpha L}{\sqrt{f_1}} \text{ и } \beta = \frac{\pi}{2} - \operatorname{arctg}(-\frac{6{,}51}{f_1} - 0{,}109 \frac{e^{-0{,}115\Delta}}{f_1^{0{,}75}}),$$

откуда:

$$\rho = \operatorname{arctg} \frac{\alpha L}{\sqrt{f_1}} + \operatorname{arctg}(-\frac{6{,}51}{f_1} - 0{,}109 \frac{e^{-0{,}115\Delta}}{f_1^{0{,}75}}).$$

Кроме того, $ML = 0{,}434 \cdot e^{-0{,}115\Delta} \cdot f_1^{0{,}25}$, что позволяет определить h. Для инженерных расчетов достаточно одной итерации.

Полученные результаты позволяют констатировать, что:

1. Шенноновская пропускная способность симметричного тракта пропорциональна произведению междупарного переходного затухания на верхнюю граничную частоту.

2. Предлагаемая процедура позволяет уменьшить количество элементарных вычислительных операций более чем в два раза.

3. Экспресс-оценка шенновской пропускной способности симметричного тракта может быть выполнена непосредственно по типовым заводским данным инсталляционного кабеля.

Список используемых источников

1. Семенов А. Б., Кандзюба Е. В, Руденко В. И. «Длинный» Ethernet – дальше, дальше и дальше // Первая миля. 2017. № 7. С. 32–36.

2. ISO/IEC 11801:2011 Information technology – Generic cabling for customer premises. International standard. 2011. – 194 p.

3. Семенов А. Б. Классические структурированные кабельные системы. М. : Горячая линия – Телеком, 2016. 462 с. ISBN 978-5-9912-0530-6.

УДК 53.087.5

ФОТОПРИЕМНЫЕ УСТРОЙСТВА БЛИЖНЕГО ИНФРАКРАСНОГО ДИАПАЗОНА ДЛЯ РАЗЛИЧНЫХ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ

К. Я. Смирнов

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

Разработки полупроводниковых приборов на основе фотокатодов, работающих в ближнем инфракрасном диапазоне, ведутся, начиная с восьмидесятых годов прошлого века. Однако, многие задачи, поставленные учеными, невозможно было реализовать по причине несовершенства технологии. В настоящее время развитие сверхвысоковакуумной техники и методов выращивания полупроводниковых структур, а также фундаментальное исследование полупроводников группы A_3B_5 позволяет изготовить конструкции фотокатодов с высокой чувствительностью, которые в дальнейшем могут быть использованы в различных приборах для решения поставленных задач.

фотоприёмник, ближний инфракрасный диапазон, гетероструктура, фотокатод.

Задача регистрации слабых оптических сигналов малой длительности на длинах волн в диапазоне 0,95 ÷ 1,65 мкм является крайне актуальной и может быть решена с помощью вакуумных фотоэлектронных приборов с фотокатодами. Заданная область спектральной чувствительности в ближнем ИК-диапазоне предопределила тип фотокатода (с междолинным переносом электронов (ФКМПЭ) и электрическим смещением), который необходимо использовать в фотоприемнике при регистрации отраженного лазерного излучения от различных объектов [1]. Такой фотокатод реализуется на основе эпитаксиальной структуры в системе фосфид индия – индий галлий арсенид. Использование гетероструктур на основе $A^{III}B^{V}$ полупроводников объясняется потребностью в материале с шириной запрещенной зоны достаточно узкой, чтобы детектировать ближний ИК диапазон (до 1,7 мкм при использовании $In_{0.53}Ga_{0.47}As$). Тем не менее, эти материалы с узкой шириной запрещенной зоны сами по себе не могут быть эффективными фотокатодами, так как не невозможно на их поверхности достигнуть состояния отрицательного электронного сродства (ОЭС). Но они идеально согласуются по кристаллической решётке с InP, который, являясь проводником электронов (эмиттером), генерированных в поглотителе InGaAs, позволяет получить на его поверхности эффективное состояние ОЭС.

Процесс создания фотокатодного узла является технологически сложной задачей и проводится в несколько этапов. На гетероструктуру InP/InGaAs, выращенную методами металлорганического осаждения из газовой фазы (MOCVD), наносится титановый сетчатый электрод методом фотолитографии. Далее следует этап довакуумной очистки фотокатодного узла. Для получения высокого уровня фотоэмиссии критически важно получить атомарно чистую поверхность гетероструктуры InP/InGaAs. На ее поверхности находится InP – материал группы A_3B_5. Традиционно такие полупроводники могут быть очищены с помощью вакуумного прогрева, однако, структуры на основе фосфида индия отличаются слабой термостойкостью и прогревы в вакуумной камере с температурой более 320 ^{0}C приводят к деградации поверхности [2]. Таким образом, крайне важным является этап химической довакуумной очистки исследуемых образцов. Он проводится на лабораторном стенде с помощью трех-стадийного метода с использованием растворов серной кислоты.

В результате травления в растворах сильных кислот на поверхности фосфида индия формируется защитный слой, позволяющий осуществить перенос гетероструктуры в вакуумную камеру без деградации поверхности. Для проведения исследований в вакууме используется сверхвысоковакуумная установка Riber-M, имеющая предельный вакуум на уровне 1×10^{-11} мм рт. ст. Установка (рис.1–2, см. ниже) предназначена для исследования фотокатодов на структурах A_3B_5 и оснащена загрузочной камерой, шиберными затворами, манипуляторами, смотровыми окнами, оснасткой, источниками цезия, кислорода и др. Установка позволяет производить запрессовку фотокатода в корпус прибора.

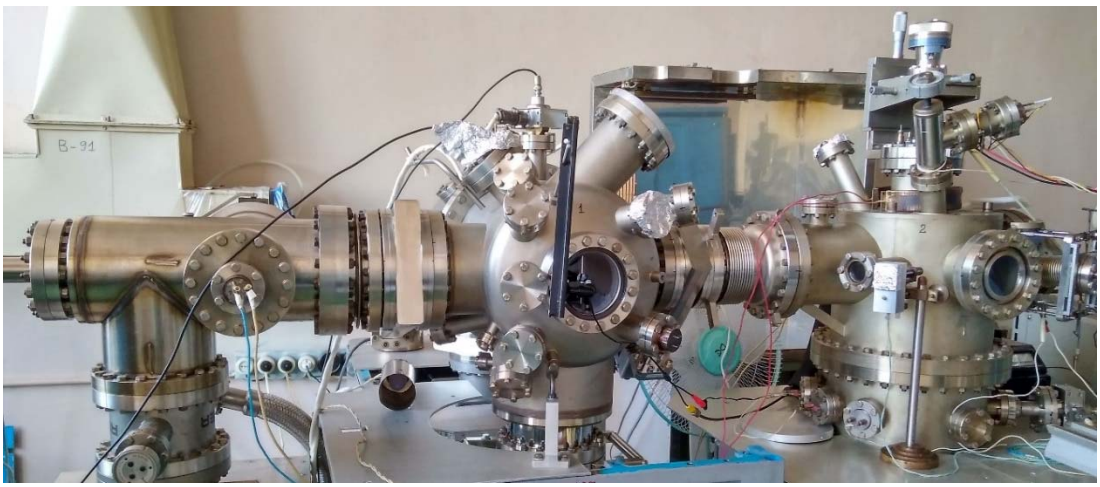


Рис. 1. Внешний вид установки переноса Riber-M

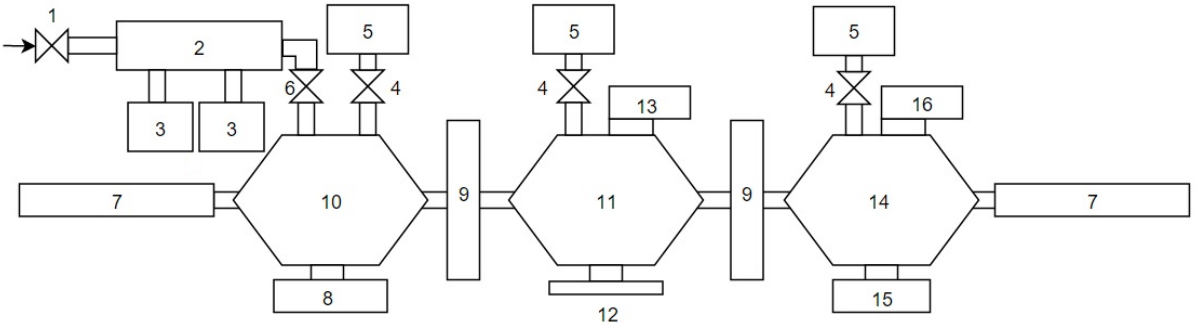


Рис. 2. Блок-схема установки Riber-M, где 1 – кран напуска, 2 – магистраль, 3 – цеолитовый насос, 4 – кран магниторазрядного насоса, 5 – насос магниторазрядный, 6 – кран магистрали, 7 – манипулятор, 8 – входное окно 9 – шиберный затвор, 10 – загрузочная камера, 11 – камера обработки корпуса и запрессовки, 12 – смотровое окно, 13 – запрессовщик, 14 – камера изготовления ФК, 15 – смотровое окно, 16 – фланец источников

Активация фотокатода состоит в осаждении на атомарно чистой поверхности фотокатодной структуры молекул Cs и O_2 [3]. В результате этого на поверхности фотокатода формируется состояние ОЭС, что позволяет электронам эффективно эмитировать в вакуум. Этот процесс крайне требователен к чистоте источников и предельному уровню вакуума в установке [4]. В результате активации InP/InGaAs гетероструктуры получается фоточувствительный элемент, готовый к запрессовке в корпус прибора. Спектральные характеристики образца с различным напряжением смещения, поданным на поверхностный электрод, представлены на рис. 3.

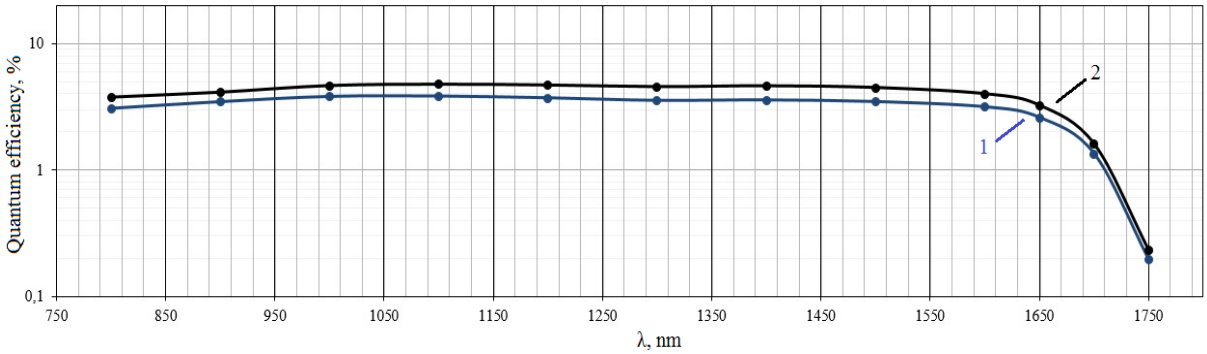


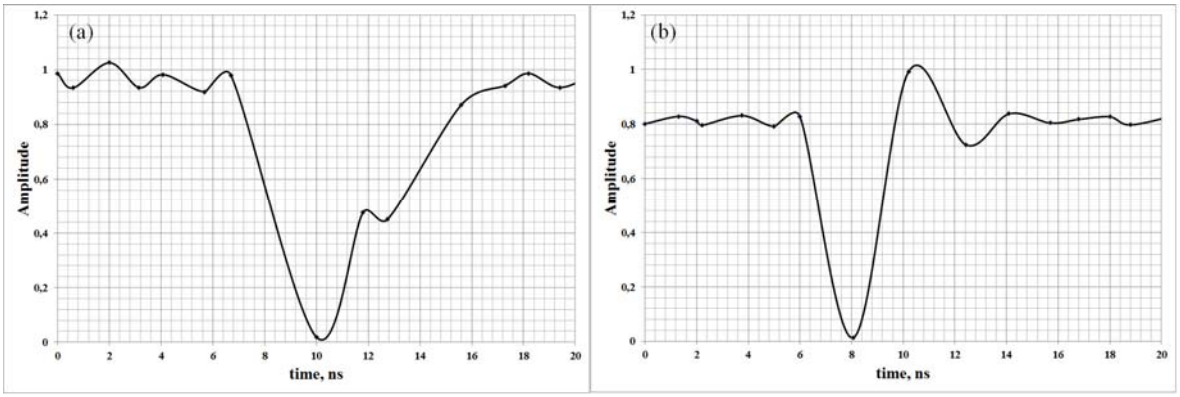
Рис. 3. Спектральные характеристики InP/InGaAs (111), 1 – напряжение поверхностного электрода 2В; 2 – напряжение поверхностного электрода 3В

Квантовая эффективность разработанных гетероструктур, работающих в режиме на отражение излучения, составила 4 % в спектральном диапазоне от 900 до 1600 нм. Результат работы образцов в режиме работы на пропускание была значительно ниже, чем в режиме работы на отражение. Это важная проблема для создания реальных фотоприёмных устройств, на основе

исследуемых гетероструктур. Полученные результаты связаны с неоптимальными параметрами подложки, на которой выращена пара поглотитель-эмиттер. Теоретические расчеты показали, что при оптимизации параметров подложки, квантовый выход InP/InGaAs гетероструктур в режиме работы на пропускание и отражение не будет отличаться более чем на 15 %.

Полученные результаты свидетельствуют о возможности создания стабильного фотокатода, работающего в ближнем ИК диапазоне. На его основе может быть создано большое многообразие приборов различного назначения. Первым шагом для этого является создание эффективного сенсора, включающего в себя фотокатод и прибор, осуществляющий регистрацию потока фотоэлектронов с фотокатода и внутреннее усиление. В зависимости от различных задач, в качестве таких приборов могут выступать матрицы pin-диодов, электронно-чувствительные приборы переноса заряда (ЭЧППЗ), микроканальные пластины (МКП).

На данный момент ведутся работы по созданию сенсора с InP/InGaAs фотокатодом, где в качестве преобразователя фотоэлектронов и элемента, обеспечивающего внутреннее усиление в приборе, используется pin-диод. Результаты исследования характеристик такого диода представлены на рис. 4 и рис. 5 (см. ниже).



a) b)

Рис. 4. Импульсная характеристика pin-диода при подаче на него напряжения:
a) U_d=190V; b) U_d=280V

На основе полученных результатов прогнозируются характеристики прибора значительно превышающие твердотельные аналоги подобных устройств. В частности, чувствительность на уровне более 5 А/Вт и быстродействие на уровне 2–3 нс.

Фотокатоды на основе InP/InGaAs гетероструктур не имеют аналогов, поскольку на данный момент не существует известных полупроводниковых соединений способных обеспечить схожий уровень фоточувствительности

в ближнем инфракрасном диапазоне. Данные структуры могут быть использованы в различных приборах специального назначения, где требуется высокая скорость обработки регистрируемого рассеянного излучения от объектов, которую не могут обеспечить их твердотельные аналоги. Внутреннее усиление, обеспечиваемое в вакуумных фотоэлектронных приборах, позволяет достигать уровня чувствительности в несколько раз большее чем у новейших InGaAs лавинных фотодиодов (APD).

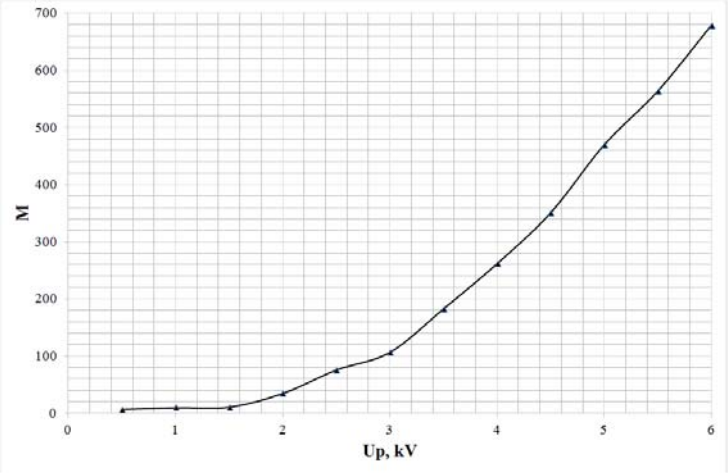


Рис. 5. Зависимость коэффициента усиления (M) от управляющего напряжения фотокатода Up (напряжение между фотокатодом и pin-диодом)

В зависимости от элемента, регистрирующего поток фотоэлектронов на выходе фотокатодной структуры, может быть разработано огромное многообразие устройств, работающих в ближнем инфракрасном диапазоне и решающих задачи локации, формирования телевизионного изображения, сканирования и поиска целей в условиях ограниченной видимости и многих других.

Список используемых источников

1. Bell R.L. Патент США N23958 143, 1974.

2. Sun Y., Liu Z., Machuca F., Pianetta P., Spicer W. Optimized cleaning method for producing device quality InP(100) surfaces // SLAC-PUB-11018. 2005.

3. Sun Y., Liu Z., Pianetta P. Formation of Cesium Peroxide and Cesium Superoxide on InP Photocathode activated by Cesium and Oxygen // SLAC-PUB-12710. 2007.

4. Chanlek N., Herbert J. D., Jones R. M., Jones L. B., Middleman K. J., Militsyn B. L. The degradation of quantum efficiency in negative electron affinity GaAs photocathodes under gas exposure // J. Phys. D: Appl. Phys. 47 055110. 2014.

Статья представлена научным руководителем, кандидатом физико-математических наук, доцентом В. В. Давыдовым

УДК621.391.1

МЕТОДИКА ОЦЕНКИ ПРОПУСКНОЙ СПОСОБНОСТИ ТРАНСПОРТНОЙ СЕТИ СВЯЗИ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

А. В. Удальцов

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

В статье предлагается методика оценки пропускной способности транспортной сети связи специального назначения.

пропускная способность, система связи специального назначения.

Одним из основных направлений совершенствования Вооруженных Сил Российской Федерации является их оснащение новыми высокоэффективными средствами и системами связи и управления, внедрение современных информационных технологий в процесс управления войсками. При стремительном развитии средств управления и увеличение объема предоставляемых услуг увеличиваться требования к объему и качеству транспортной сети специального назначения. Транспортная сеть специального назначения представляет собой сеть связи. Образованная цифровыми средствами связи, являющаяся составной часть телекоммуникационной сети и выполняющая функции каналообразования, переноса и распределения потоков сообщений между сетевыми узлами связи.

В настоящее время сети связи специального назначения строятся с применением технологий с коммутацией пакетов. Особенность данной технологии заключается в том, что единицей измерения ресурса сети является время передачи пакета.

Основными элементами транспортной сети связи специального назначения являются сетевые узлы связи, осуществляющие маршрутизацию пакетов, передавая их в соответствии с адресной информацией и правилами маршрутизации в направлениях связи.

Пропускная способность, является одной из характеристик сети связи. Ее целевое предназначение, может рассматриваться, как способность обеспечить передачу определенного объема информации в заданных направлениях связи при фиксированных вероятностно-временных ограничениях. Пропускная способность может рассматриваться как функция от двух параметров: объема передаваемой информации и вероятностно-временных показателей своевременности ее передачи.

Для передачи информации и предоставления услуг связи в сети необходима доставка пакетов от одного узла связи до другого узла связи, и она определяется временем распространения сигнала, временем передачи пакета, временем ожидания в узле связи.

$$T_{дост} = T_{рс} + T_{вп} + T_{ож},$$

где $T_{рс}$ – время распространения сигнала; $T_{вп}$ – время передачи пакета; $T_{ож}$ – время ожидания в узле связи.

В транспортной сети связи специального назначение время передачи сигнала можно не учитывать, так как задержка распространения на расстояниях применения транспортной сети связи специального назначения пренебрежимо мало по сравнению с задержкой на передачу и ожидании в узле связи.

Время передачи пакета определяется скоростью передачи данных по линии связи и длиной пакета:

$$T_{вп} = \frac{L}{v},$$

где v – скорость передачи данных (бит/с); L – размер пакета данных (бит).

Исходя из выше сказанного следует, что время передачи пакета величина постоянная. Если учитывать, что состояние канала стабильно, то время передачи будет зависеть только от длины пакета. Длина пакета для каждой услуги может быть различная.

Время ожидания в узле связи – это время в нахождения пакета в буферной памяти узла или очереди до его передачи. Время ожидания зависит от интенсивности трафика, времени передачи и других параметров.

В системе связи специального назначения виды услуг, предоставляемых через транспортную сеть связи специального назначения можно условно классифицировать на три группы: интерактивные, потоковые и фоновые [1].

Трафик создается абонентами на узлах связи, на период предоставление услуги. Назовем это время сессий. Для каждой услуги характеристики интенсивности и длительности сессии будут различны. Интенсивность нагрузки для сессии будет равна:

$$s=c\bar{t},$$

где с – интенсивность сессий (сессий/час); $\bar{t}$ – средняя продолжительность сессии (час).

Пакет доставляется получателю с некоторой задержкой, а иногда вообще не будет доставлен. Эти явления существенно влияют на качество предоставляемых услуг связи. Для обеспечения и подержания качества услуг введены показатели качества функционирования сети, определённые стандартами международного союза электросвязи (ITU-T), в рекомендациях

Y.1540[2], Y.1541[2], и в общих тактико-технических требованиях для специальных систем связи [3].

При планировании транспортной сети связи специального назначения необходимо получить точные исходные данные для расчета объема передаваемой информации от пунктов управления по каналам связи, а это достаточно сложно. Поэтому, в ходе проведения расчетов при частичном или полном отсутствие таких данных, используется подход, при котором исходными данными являются:

x – общее количество должностных лиц пункта управления, распределение их по управлениям, отделам, группам;

k^1 k^2.. k^n, – коэффициенты охвата должностных лиц пункта управления по каждому виду связи и категории.

Начавшееся широкое использование автоматизированных средств управления предопределяет увеличение потоков информации (электронная почта, передача файлов, удаленный доступ к базам данных), передаваемых по сетям передачи данных. Удельный вес передачи данных повышается и в ближайшей перспективе достигнет 80...90 % [4].

Внедрение новых видов информационного обмена (видеоконференцсвязь) занимает 30–50 % от общего трафика.

Трафик, создаваемый разными группами услуг, а также требуемая пропускная способность линий привязки рассчитывается на основе параметров абонентской нагрузки:

ν, (кбит/с) – максимальная скорость передачи информационного потока;

$\bar{t}$, (сек) – длительность сеанса;

c – количество вызовов в час*;*

s_0^j (эрл) –интенсивность сессии/

Зная число абонентов, простым арифметическим суммированием производится расчет исходящего трафика от узла связи.

Интенсивность нагрузки, производимая должностными лицами пунктов управления, включенными в узел связи *i,* зависит от спроса на услуги и набора предоставляемых услуг

$$s_i = n_i^{(1)} s_o^{(1)} + n_i^{(2)} s_o^{(2)} + \ldots + n_i^{(m)} s_o^{(m)},$$

где $n_i^{(j)}$ – количество должностных лиц j-й услуги, включенных в данный узел; n_i – общее количество должностных лиц, включенных в данный узел; m – количество предоставляемых услуг; $s_o^{(j)}$ – интенсивность сессий j-й услуги.

При построении транспортной сети связи специального назначения необходимо обеспечить баланса между трафиком, объемом ресурсов сети

связи (пропускной способностью) и качеством предоставления услуг (параметрами функционирования).

Для этого транспортную сеть связи специального назначения представить в виде графа (рис.) неориентированного, в котором узлы связи соответствуют вершинам графа, а линии связи дугам графа. В данном примере приведена структура транспортной сети связи, включающая 6 узлов связи (1ПУ, 2ПУ, 3ПУ, 4ПУ, 5ПУ, 6ПУ) и 2 сетевых узла связи (1ОУС, 2ОУС). Каждое из ребер графа характеризуется интенсивностью нагрузки $s_{i,j}$. Значения интенсивностей нагрузки определяются распределением трафика в сети связи между узлами абонентских сетей.

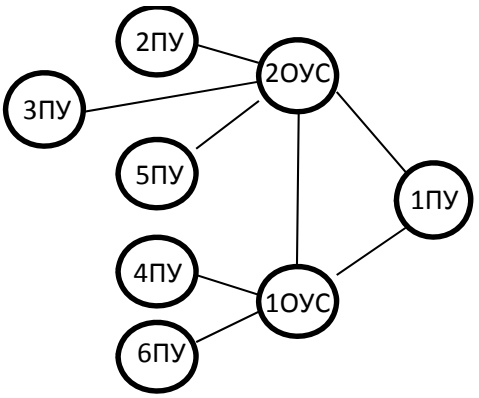


Рисунок. Фрагмент транспортной сети связи

Доля трафика, производимого абонентами узла i, направляемая на узел j определяется коэффициентами распределения k_{ij}, $j = 1...d$, где d – количество линий связи исходя из групп важности информационной направления.

Таким образом, данный граф транспортной сети связи позволяет создать описание сети в виде нагрузок между оконечными узлами связи, в которой:

$$S_{i,j} = s_i k_{ij}. \quad (1)$$

Аналогично, на основе структуры транспортной сети связи и маршрутов пропуска трафика может быть определено распределение нагрузки по линиям связи. Распределение нагрузки по линиям связи определяется по имеющимся в структуре сети связи линиям связи между узлами связи сети связи.

Для оценки необходимой пропускной способности линий связи транспортной сети связи за исходные данные расчета берется интенсивность трафика, обслуживаемого линиями связи, которая определена (1), и нормативы на качество обслуживания [1, 2].

От полученных значений нагрузки $s_{i,j}$ необходимо перейти к интенсивности трафика (бит/с).

Если известны данные о предоставляемых услугах, интенсивности трафика, производимого этими услугами $a_o^{(j)}$ – интенсивность трафика, производимого j-й услугой (во время сессии), то общая интенсивность трафика может быть получена как

$$a_{ij} = v_{ij}(\eta_1 a_o^{(1)} + \eta_2 a_o^{(2)} + \ldots.. + \eta_m a_o^{(m)}),$$

где v_{ij} – число сессий, которые требуется обслужить; $a_o^{(j)}$ – интенсивность трафика j-й услуги (бит/с); η_j – доля нагрузки сессий, производимой j-й услугой.

Значение v_{ij} фактически означает число сессий, обслуживание которого должна обеспечивать линия связи:

$$v_{ij} = k_{ij} n_i,$$

В результате чего может быть получаем распределение трафика по линиям связи.

Поток пакетов рассматривается как случайный поток заявок на обслуживание, линии связи рассматриваются как обслуживающее устройство, которые занимаются передаваемыми пакетами на некоторое случайное время, равное времени передачи пакета. Модель такой системы должна рассматривать взаимодействие двух случайных процессов: процесса поступления заявок и процесса их освобождения, т. е. она является моделью системы массового обслуживания (СМО) [5]. При поступлении заявки в момент, когда устройство занято, заявка ставится на ожидание. Когда число ожидающих заявок достигает некоторого заданного значения (размера буфера), заявка теряется. Такая дисциплина называется комбинированной дисциплиной обслуживания (с ожиданием и отказами). Цель моделирования заключается в том, чтобы связать интенсивность трафика, пропускную способность канала со временем ожидания и вероятностью потерь (отказов) [6].

Модели СМО связывают показатели качества с параметрами потока заявок и характеристиками процесса их обслуживания. Они разработаны для потоков и процессов, имеющих определенные свойства. Поэтому, выбор той или иной модели зависит от свойств тех процессов, которые она должна описывать [7].

1. Модель потока заявок. Модель потока пакетов (потока заявок) в сетях передачи данных обычно описывают моделью случайного потока.

Для простейшего потока вероятность поступления k заявок за интервал времени t является случайной величиной, имеющей распределение Пуассона:

$$p_k = \frac{(\lambda t)^k}{k!} e^{-\lambda t},$$

где λ – интенсивность потока.

Интервалы времени между заявками в таком потоке также случайны и имеют экспоненциальное распределение вероятности:

$$f(x) = 1 - e^{-\lambda x}$$

2. Модель процесса обслуживания. В этой модели предполагается, что обслуживающее устройство (канал) занимается заявкой на случайное время.

3. Время задержки пакета (в очереди на обслуживание). В условиях описанных моделей среднее время задержки пакета на участке сети определяется формулой Поячека-Хинчина:

$$T = \frac{\rho\bar{t}}{2(1-\rho)}(1 + \frac{\sigma^2}{\bar{t}^2}) + \bar{t},$$

где $\rho = a\bar{t}$; a – интенсивность пакетов; $\bar{t} = \frac{\bar{L}}{b}$ – среднее время обслуживания пакета; σ^2 – дисперсия времени обслуживания; $\bar{L}$ – средняя длина пакета (бит); b – скорость передачи (бит/с).

В частных случаях, например, когда время обслуживания имеет экспоненциальное распределение, то $\frac{\sigma^2}{\bar{t}} = 1$, тогда:

$$T_{\text{exp}} = \frac{\bar{t}}{1-\rho}.$$

Когда время обслуживания постоянно, то $\sigma^2 = 0$:

$$T_D = \frac{p\bar{t}}{2(1-\rho)} + \bar{t}.$$

Если свойства потока отличаются от простейшего, то может быть применена приближенная формула:

$$T_G = \frac{\rho\bar{t}}{2(1-\rho)}\left(\frac{\sigma_a^2+\sigma_s^2}{\bar{t}^2}\right)\left(\frac{\bar{t}^2+\sigma_s^2}{\bar{a}^2+\sigma_s^2}\right) + \bar{t},$$

где σ_a^2 и σ_s^2 – дисперсии интервалов времени между пакетами и времени обслуживания, соответственно; $\bar{a}$ – среднее значение интервала между пакетами; $\bar{t}$ – среднее время обслуживания.

4. Вероятность отказов (потерь пакетов). Для оценки вероятности потерь может быть использована приближенная формула:

$$p = \frac{1-\rho}{1-\rho^{\frac{2n_b}{C_a^2+C_s^2}+1}}\rho^{\frac{2n_b}{C_a^2+C_s^2}},$$

где C_a^2 и C_s^2 – квадратичные коэффициенты вариации соответственно распределений входящего потока и времени обслуживания; n_b – размер буфера; ρ – загрузка системы.

Методика оценки пропускной способности транспортной сети связи специального назначения (построенной по технологии коммутации пакетов) задается в следующем алгоритме [8]:

1. Определяются потребности должностных лиц пунктов управления в услугах связи и их типов, объем нагрузки, поступающей от оконечного узла на пограничный маршрутизатор транспортной сети связи специального назначения, и ее интенсивность.

2. Определяется структура транспортной сети связи специального назначения (при оценке проектируемой сети связи).

3. Определяется необходимая пропускная способность линий привязки оконечных узлов пунктов управления к транспортной сети связи специального назначения.

4. Вычисляется распределение нагрузки между оконечными узлами связи.

5. Вычисляется распределение нагрузки по имеющимся линиям связи.

6. Вычисляется распределение интенсивностей трафика по направлениям связи.

7. Для полученных значений интенсивностей трафика на линиях связи вычисляется время задержки и вероятность потери пакетов на участках сети.

8. Проверить соответствие расчетных коэффициентов потери пакетов и времени их задержки в сети с установленными требованиями и нормами для функционирования сети.

Список используемых источников

1. ГОСТ РВ 52216-2004. Связь военная. Термины и определения. Принят и введен в действие Постановлением Госстандарта России от 29.01.2004 г. № 42-ст. 11 с.

2. Рекомендации ITU-TY.1540. Рекомендации ITU-TY.1541.

3. Основные тактико-технические требования к системе связи. ВАС, 2012.

4. Гольдштейн Б. С., Соколов Н. А., Яновский Г. Г. Сети связи: учебник для вузов. СПб. : БХВ-Санкт-Петербург, 2010. 400 с.

5. Клейнрок Л. Теория массового обслуживания. М. :Машиностроение, 1979. 432 с.

6. Цыбаков Б. С. Модель телетрафика на основе самоподобного случайного процесса // Радиотехника. 1999. № 5. С. 24–31.

7. Сивоплясов Д. В. Методы анализа и оптимизации сетей связи : электронное учебное пособие, Военная академия ракетных войск стратегического назначения им. Петра Великого, 2016. 112 с.

8. Давыдов А. Е., Смирнов П. И., Парамонов А. И. Проектирование телекоммуникационных систем и сетей. Раздел Коммутируемые сети связи. Расчет параметров сетей связи и анализ трафика. СПб. : Университет ИТМО, 2016. 47 с.

Статья представлена доцентом кафедры ВАС, кандидатом военных наук, доцентом В. Г. Ивановым.

УДК 654.9, 681.5

ПРИМЕНЕНИЕ ПРОГРАММНОГО КОДА ДЛЯ ОПТИМИЗАЦИИ ЧИСЛА СЕРВЕРОВ DPI МЕТОДОМ МАКСИМАЛЬНОГО ЭЛЕМЕНТА

В. В. Фицов

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

В данной статье рассмотрено использование программного кода на языке python для оптимизации сетевой конфигурации DPI. Предметом оптимизации является число процессоров в сервере (доступные вычислительные ресурсы системы). Критериями оптимизации являются время, требуемое системе DPI для анализа и принятия решения, а так же необходимое число устройств.

DPI, QoS, python, CeMO, метод максимального элемента, ММЭ.

Введение

Система DPI (*Deep Packet Inspection*, глубокой инспекции пакетов) распознает приложения по потоку пакетов, для управления потоками этих приложений согласно политикам оператора. Полноценная система DPI дорогостоящее удовольствие. Стоимость DPI пропорционально возрастает с числом каналов связи. Для расчета аппаратных характеристик системы, с учетом информации о характере трафика на сети, производительности системы DPI и стоимости оборудования и электроэнергии можно использовать функции оптимизации и стоимости. В [1] рассматривался математический расчет DPI для двух систем массового обслуживания (СМО): аппаратного фильтра и Front-End, а также оптимизация методом максимального элемента (ММЭ) вручную. В данной статье рассмотрена программная реализация оптимизации и расчета функции стоимости. Применение для этого программного алгоритма упрощает восприятие результатов расчета и помогает задать критерии подходящего решения.

Сервер Front-End в архитектуре DPI

Ранее в [2] была определена обобщенная архитектура модели DPI. Сервера системы глубокой инспекции пакетов составляют сеть массового обслуживания (СеМО). К ним относятся аппаратный фильтр (*Hardware Filter*, HF) совместно с Bypass как одна СМО в рамках функциональной модели.

А также Front-End (FE), PCRF (*Policy and Charging Rules Function*) и Back-End (BE) (рис. 1 в [2]). Чуть подробнее их функции описаны в [2].

В данной статье, рассматривается оптимизация сервера, требующего наибольшую вычислительную мощность – Front-End. FE проводит глубокую инспекцию пакетов потока, с использованием сигнатурного, статистического и поведенческого анализа. Несколько первых пакетов нового потока, обнаруженного HF, поступают на FE как заявка. Вероятность, что FE в стационарном режиме запросит номер политики у PCRF невелика. Учитывая быстроту работы PCRF и незначительную по сравнению с FE нагрузку, эти запросы не будут рассматриваться. Таким образом, после анализа FE дает указания из своего кэша на HF.

Принято считать, что трафик пакетных сетей лучше описывают распределения: Логнормальное, Парето, Вейбулловское, Гамма, Гиперэкспоненциальное 2го порядка [3]. Согласно результатам имитационного моделирования, в [4] агрегированный самоподобный трафик с тяжелым хвостом, после обработки СМО, становится экспоненциальным. Допущение, что от HF (СМО1) поступает поток заявок, распределенный по экспоненте, значительно упрощает задачу и позволяет воспользоваться стандартными математическими моделями расчета для FE (СМО2). Исходя из того, что система должна иметь большой буфер приема и не имеет права отказать в обслуживании заявки, возьмем модель M/M/V с бесконечной очередью для СМО2.

Математическая модель

Для модели с бесконечной очередью M/M/V/□ согласно [5], вероятность свободной системы (P0):

$$P0(A) = \left[\sum_{i=0}^{V-1}\left(\frac{A^i}{i!}\right) + \left(\frac{V}{V-A}\right) \times \frac{A^V}{V!}\right]^{-1}, \quad (1)$$

где $A = \frac{\lambda}{\mu}$.

Используя формулу Эрланга и P0, получаем вероятность попадания заявки в очередь, когда все устройства заняты Poh:

$$Poh(A) = \left(\frac{A^V}{V!}\right) \times \left(\frac{V}{V-A}\right) \times P0(A). \quad (2)$$

Длина очереди Loh:

$$Loh = \left(\frac{A}{V-A}\right) \times P0(A). \quad (3)$$

Заявок в системе Lsys:

$$Lsys = Loh + Lob \text{ , где } Lob = \frac{\lambda}{\mu}.$$

Время обслуживания согласно формуле Литтла:

$$Tsys = \frac{Lsys}{\lambda},$$

$$Tsys = \frac{1}{\mu} \times \left(\frac{Poh(A)}{V-A} + 1\right). \quad (4)$$

Результаты расчета для $V = 1, 2, 3$ показаны в таблице 1.

ТАБЛИЦА 1. Параметры СМО M/M/V/□ при λ =1500, μ = 3000

Параметр СМО	$V = 1$	$V = 2$	$V = 3$
P0	0,5	0,6	0,606
Poh	0,5	0,1	0,015(15)
Tsys, с	0,0006(6)	0,0003(5)	0,0003(35)

Поиск оптимального и эффективного решения

Методы оптимизации делят на классические, неклассические (математического программирования) и случайного поиска. Их перечисление приведено в [1]. Для оптимизации применяется ММЭ, относящейся к неклассической оптимизации. Исходные данные оптимизации системы DPI: интенсивность поступающих заявок на СеМО DPI (λ), интенсивность обслуживаемых заявок (μ), вероятность завершения обработки заявки на определенном сервере (*Psmon*), число обслуживающих устройств (процессоров) – для каждого из серверов DPI. Т. к. выше расчет ведется по одному серверу – FE, то вероятность завершения обработки заявки этим сервером (*Psmo*2) равна единице.

Упрощенно задачу оптимизации можно свести к уменьшению числа обслуживающих устройств сервера (числа процессоров или выделяемой вычислительной мощности), при сохранении удовлетворительного времени обработки заявки в системе, и стоимости оборудования. Для разных значений интенсивности поступления (λ) и обработки (μ) заявок.

Наименее влияющим на QoS (*quality of service*), обрабатываемого системой DPI, проходящего трафика, является режим, когда анализ трафика завершается, после того, как трафик был пропущен. Такой режим позволяет избежать возникающую при глубокой инспекции пакетов задержку. После определения приложения, от которого поступает трафик, на системе DPI применяются соответствующие политики. Таким образом, с момента пропуска трафика до момента применения политик возникает задержка корреционных действий. Составляющая данной задержки на FE рассматривается в оптимизации и математическом расчете как *Tsys*. Особенность такого режима, что величина *Tsys* не является критичной для работы системы DPI,

до тех пор, пока она хотя бы вдвое меньше среднего времени передачи трафика типичным приложением. Предположим, что задержка коррекционных действий может находиться в диапазоне от 0 до 60 или 300 секунд. Что на три порядка больше, стандартных требований QoS. Число процессоров (*V*) может быть различным, но можно его ограничить от 0 до 120. Однако, подводным камнем может оказаться необходимость дробного значения числа процессоров. Например, увеличение вычислительной мощности на 10 % одного процессора. Такой расчет потребует дополнительной проверки используемых формул.

При оптимизации ММЭ для каждого случая загруженности системы DPI задаются величины интенсивности поступления (λ) и обработки (μ) заявок, а также различных значений числа обслуживающих устройств (*V*). Получаем функцию времени глубокой инспекции пакетов *Tsys*(*V*), при заданных λ и μ. Простым способом оценить эффективность наращивания вычислительной мощности является указание величины удельного уменьшения времени анализа *dTsys*. Это позволит значительно сократить необходимое число вычислений в случае монотонной функции *Tsys*.

Более точным подходом является применение функции стоимости использования оборудования предоставляющего вычислительные ресурсы. Обозначим стоимость владения сервером применяемым в течении 5 лет:

$$Khw = \frac{Ru}{5\times12\times30\times24\times3600},$$

где *Ru* – цена сервера с CPU (3,4 ГГц) и Bandwitch (420 GBps). Стоимость электричества Kelectro рассчитаем как 0,1 кВТ/ч по 3,4 рубля. Общая стоимость будет зависеть от числа серверов:

$$V \times (Khw + Kelectro).$$

Исходя из того, что большую часть задержки коррекционных действий составляет время анализа *Tsys*, зададим упущенную выгоду по передаче трафика взамен паразитного трафика:

$$Kb \times Ki\$ \times (Tflow - Tsys) \text{ , где } Ki\$ = \frac{3}{(30\times24\times3600)},$$

Kb = 100 кбит/с поток, *Ki*\$ – стоимость подключения (*Kb* в секунду), *Tflow* = 1800 сек. – среднее время передачи данных типичным приложением, *Tsys* – время глубокого анализа пакетов.

Получаем функцию стоимости, величина которой представлена в таблице 2:

$$\mathrm{C(Tsys, V)} = (Kb \times Ki\$ \times (Tflow - Tsys)) - \mathrm{V} \times (\mathrm{Khw} + \mathrm{Kelectro}), \quad (5)$$

$$\mathrm{C(Tsys, V)} = (1{,}1574 \times 10^6 \times (1800 - Tsys)) - \mathrm{V} \times 0{,}005.$$

ТАБЛИЦА 2. Значения функции стоимости C(*Tsys*, *V*)

Параметр СМО	*V* = 1	*V* = 2	*V* = 3
Tsys, с	0,0006(6)	0,0003(5)	0,0003(35)
C(*Tsys*, *V*)	0,000921	0,002072	0,002067

Результаты расчетов по (5) могут быть использованы для эффективного распределения аппаратных ресурсов между серверами системы DPI, в том числе в режиме реального времени.

Программная реализация

Для создания программного обеспечения (ПО) выбран язык программирования python. Он не требует среды разработки, и поддерживается без дополнительных средств в ОС Linux. Python популярный язык программирования учёных и педагогов. И применяется длительное время для обучения научной информатике в университете Осло. Python используется для изучения вычислительных методов [6].

В разработанном ПО оптимизации DPI используются библиотеки математики (*math*), вызова системных процессов (*subprocess*), и работы с файлами (*sys*). Алгоритм ПО (рис., см. ниже) содержит функции задания входных переменных, расчета параметров СМО, расчета функции стоимости, сравнения значений величины. В начале алгоритма определены входные значения и проверена устойчивость системы при заданных λ, μ и *V*.

В функции расчета согласно формулам (1)–(5) используется математическая библиотека для получения факториала math.factorial (*V*) и возведения в степень math.pow (*A*, *float*(*V*)). Подсчет сумм, входящих в формулы реализован циклом. Рассчитываются *P0*, *Poh*, *Tsys*. Функция стоимости рассчитывается отдельной функцией C(*Tsys*, *V*).

Основной исполняемый код – это цикл по массиву значений интенсивности поступающих заявок (λ) с заданным шагом (*step* λ). Для каждой λ проводится цикл по массиву числа процессоров (*V*) с заданным шагом (*step V*). Вызываются функция расчета параметров СМО и функция стоимости. Значения *Tsys и* C(*Tsys*, *V*) записываются в массив. Для каждого числа процессоров рассчитывается разница *Tsys* по сравнению с предыдущим циклом. Когда она меньше, чем заданное удельное уменьшение времени анализа *dTsys*, то расчет прекращается для данной λ. *V*++ – > *dTsys* < 0,01 : break.

В цикле по числу полученных *Tsys* ведется поиск минимального значения *Tsys* и максимального значения C(*Tsys, V*), и вывод результатов.

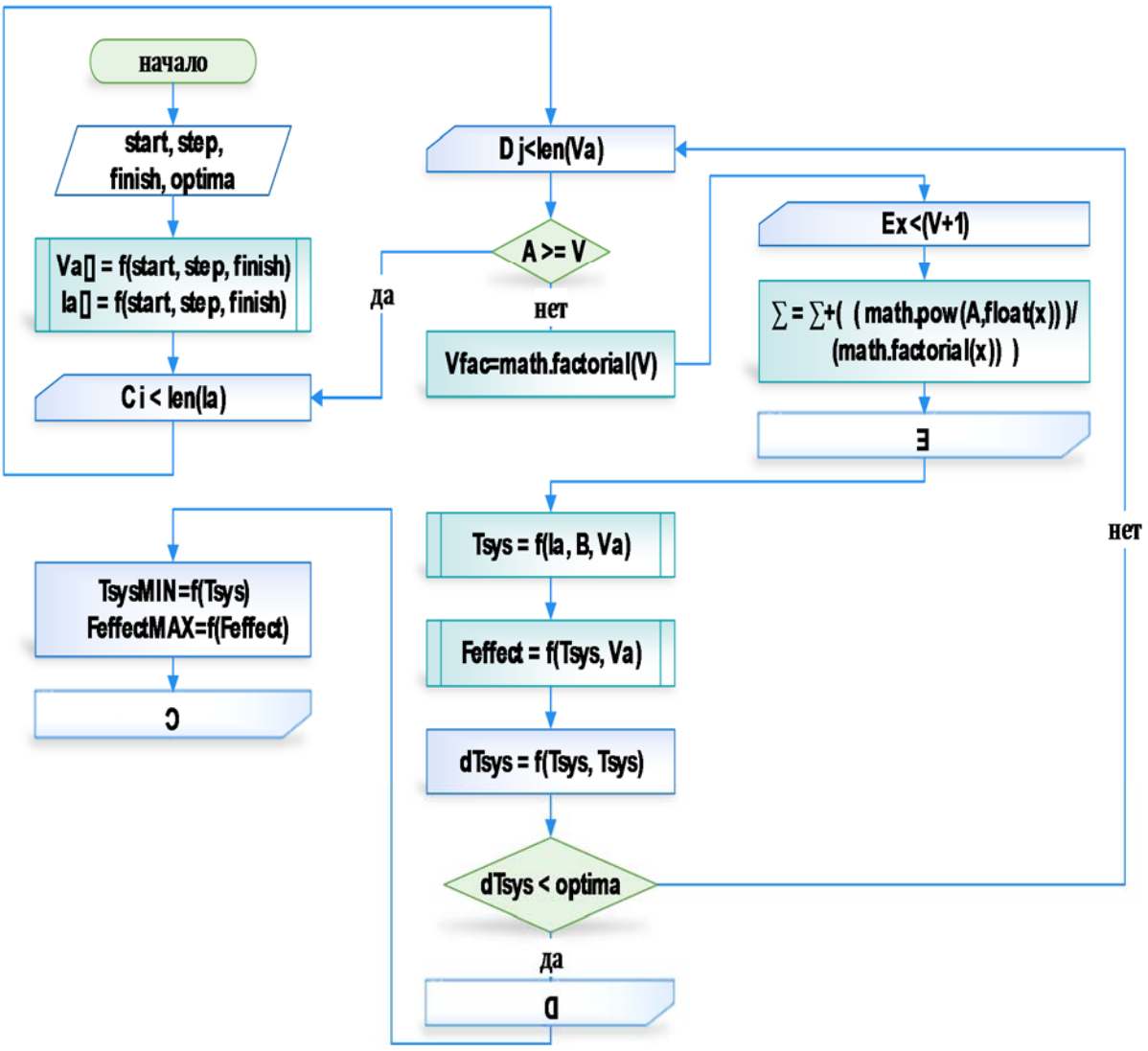


Рисунок. Алгоритм программного обеспечения по оптимизации DPI на языке python

Пример получаемых результатов

ПО выполняет необходимое число циклов для получения результатов, удовлетворяющих заданным условиям. Ценность представляют входные параметры, при которых получены значения времени анализа пакетов и стоимости. Результаты выводятся в консоль и записываются в файл.

Условные обозначения и формула расчета *Tsys*:

A = λ / μ, λ – input law (l) – its exp, μ – work law – its exp, V – count cpu or srv, Tsys – time of work in system case 1 dpi servs = FrontEnd.
Tsys = (1 / μ) * (1 + (*Poh*/(*V* – *A*)).

Входные параметры цикла расчета:

write 100 inputs Va maximum:100.0 Vnow = 1.0
if μ = 2600 and λ = 2601.0 then A = 0.999615532488

Результаты расчета для разного числа процессоров *V*:

V = 1.0 Tsys = 0.999615 with Po = 0.000384 Poh = 0.999231 C(Tsys, V) = 0.000921
V = 2.0 Tsys = 0.000494 with Po = 0.285871 Poh = 0.285541 C(Tsys, V) = 0.002072
V = 3.0 Tsys = 0.000400 with Po = 0.343009 Poh = 0.085637 C(Tsys, V) = 0.002067

Оптимальные значения:

V = 3.0 deltaTsys = 9.32*10^–05 < optimal = 0.0001
V = 2.0 --- > Tsys = 0.000494 < ---- deltaTsys = 0.999121
TsisMIN at Tsis[1] = 0.000494 V = 2.0 μ = 2601 λ = 2600 Nulim = A > 0.999
CeffMAX at C(Tsys, V) [1] = 0.002072 V = 2.0 μ = 2601 λ = 2600

Получается, что при входных параметрах $\mu = 2601$ и $\lambda = 2600$, не имеет смысла увеличивать число процессоров до 3, т. к. это незначительно повлияет на сокращение времени анализа пакетов (уменьшит на 10 мкс). Было получено время анализа пакетов при 2-х процессорах на FE, и оно составило 494 мкс. Максимум функции стоимости достигнут на 2-х процессорах. При большем числе убывает. Оборудование простаивает.

Список используемых источников

1. Фицов В. В. Методы оптимизации сетевой конфигурации системы DPI // 71-я РНТК «Студенческая весна – 2017». СПб. : СПбГУТ, 2017. Т. 1. С. 215–219.

2. Фицов В. В. Имитационная модель системы DPI на основе программного обеспечения GPSS World // Актуальные проблемы инфотелекоммуникаций в науке и образовании. V Международная научно-техническая и научно-методическая конференция. СПб. :СПбГУТ, 2016. С. 539–545.

3. Ложковский А. Г., Каптур В. А., Вербанов О. В. Математическая модель пакетного трафика // Вестник национального политехнического университета «ХПИ». 2011. № 9. С. 113–119.

4. Зайцев В. С. Анализ свойств суммарного потока заявок на входе системы массового обслуживания // АПИНО-2018.

5. Фомин Г. П. Экономико-математические методы и модели в коммерческой деятельности. – М. : Юрайт, 2013. С. 365–367.

6. Dolgopolovas V., Dahiene V., Minikevicius S., Sakalauskas L. Python for scientific computing education: Modeling of queueing systems // Scientific Programming, 2014, vol. 22, no. 1, pp. 37–51.

Статья представлена заведующим кафедрой, доктором технических наук, профессором Б. С. Гольдштейном.

УДК 004.056.53

ИССЛЕДОВАНИЕ СУЩЕСТВУЮЩИХ МЕХАНИЗМОВ ЗАЩИТЫ ОПЕРАЦИОННЫХ СИСТЕМ СЕМЕЙСТВА LINUX

А. Ю. Цветков

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

Обеспечения информационный безопасности в операционных системах является важной темой в доктрине информационной безопасности РФ. Перед разработкой новых механизмов или улучшений, требуется изучить тонкости существующих механизмов защиты данных и разграничения доступа.

права доступа, привилегии, пользователь, процесс, метка.

Существующие операционные системы (ОС) согласно принятым определениям [1], представляет из себя собой комплекс программ, обеспечивающих управление и обработки входящих заданий. ОС можно представить, как «прослойку» между пользователем и аппаратной частью. В свою очередь она предоставляет интерфейс понятный пользователю, а также эффективно и безопасно организует доступ к ресурсам вычислительной системы.

Обеспечение безопасности ОС в большей степени зависит от качества реализуемых механизмов, заложенных изначально при разработке ОС. Но также на «брешь в стене» могут повлиять алгоритмические ошибки, которые допускаются программистами при разработке, как прикладных, так и системных утилит.

Данные ошибки могут нести, как непреднамеренный характер, так и преследовать определённые цели: не задокументированный сбор информации и статистике о системе, получение доступа к вычислительным ресурсам и др.

Согласно [1], взаимодействие с аппаратной частью, в ОС GNU/Linux представляется, как взаимодействие с файловой системой. Следовательно, обеспечение безопасности строиться на разграничение доступа к файлам и системным вызовам. В ОС GNU/Linux используется система разграничения полномочий на основе выданных им разрешений [1, 2].

Для ОС каждый пользователей представлен в виде числового идентификатора UID (*User identifier*), которому установлен определенный набор привилегий. Так же пользователи могут объединяться в группы, которым

присваивается свой уникальный идентификатор GID (*Group identifier*). Любое совершенное действие, система отслеживает в соответствие с уровнем привилегий UID и GID. Следует отметить в ОС присутствует пользователь с абсолютными привилегиями (суперпользователь), его UID = 0. Данный пользователь имеет практически неограниченный доступ к ресурсам.

Существует три основные модели разграничения доступа [4, 5, 6]: дискреционная, мандатная модели и управление доступа на основе ролей. Дискреционная модель реализована в качестве базового механизма контроля доступа, две другие – расширенного. Базовые механизмы делятся на две группы: разграничение прав доступа к файлам и системным вызовам.

В качестве субъектов к которым применяется разграничение доступа являются:

– владелец файла (*UID*);
– группа владельцев (*GID*);
– остальные пользователи.

Для всех субъектов определены три операции, совершаемые над файлами:

– чтение (R – *Read*);
– запись (W – *Write*);
– исполнение (X – *eXecutable*).

Из выше сказанного следует, что доступ к файлу определяется по девяти атрибутам.

Разграничение доступа к системным вызовам построено на разделение все субъектов на две категории:

– привилегированные;
– непривилегированные.

К первой группе относиться только «суперпользователь». Он имеет неограниченный доступ ко всем системным вызовам. Важно отметить, что некоторые системные вызовы, могут быть использованы только привилегированными пользователями.

В качестве примера привилегированных операций, можно привести [3]:

– подключение и отключение раздела диска;
– изменение корневого каталога процесса;
– создание файлов устройств;

Следовательно, защита на уровне системных вызовов, осуществляется посредством того являться ли пользователь привилегированным или непривилегированным. Если он непривилегированный, то ему доступен ограниченный список системных вызовов, вызов которых не приведет к нарушениям работы системы.

В ОС существует два механизма повышения привилегий пользователя:

– запуск программы с битами SetUID (SetGID);

– использование привилегий Capability.

В первом случае при запуске процесса ядро системы выполняет определенную последовательность действий. Самое важно – это присваивание процессу два идентификатора пользователя: реальный (*RUID*) и текущий (*EUID*). *RUID* определяет пользователя, который запустил процесс, а *EUID* отражает текущий уровень привилегий данного процесса.

Обычная пользовательская программа работает при соблюдение следующего условия [1, 2]:

$$\boldsymbol{EUID = RUID = UID}. \quad (1)$$

Из выражения (1) следует, что запущенная программа имеет привилегии, которые есть пользователя запустившего ее и имеющий присвоенный системой *UID*. Так же из выражения (1) следует, что команда, требующая повышения привилегий, не может быть выполнена, так как полномочий пользователя, определяемых идентификатором *UID* (*UID* > 0), будет недостаточно.

Для обхода этого ограничения в ОС GNU\Linux введена возможность запуска процесса с *EUID*, не равным *RUID* []. Следующей механизм может быть описан выражением:

$$\boldsymbol{RUID = UID\ user}; \quad (2)$$

$$\boldsymbol{EUID = UID\ owner\ file}, \quad (3)$$

где *UID user* – идентификатор пользователя, запустившего программу, а *UID owner file* – идентификатор владельца файла.

Для выполнения такого механизма, исполняемый файл должен обладать атрибутом SetUID.

Данный механизм предоставляет полные привилегии суперпользователя, поэтому на смену ему пришел механизм разрешений POSIX (*Capability*). Он позволяет разбить привилегии суперпользователя на множество частей, которые можно разрешать и запрещать независимо друг от друга [2]. Разрешения делятся на две части:

– разрешения процессов;

– разрешения файлов.

Процесс ОС имеет три набора разрешений:

– доступные (*Permitted*);

– наследуемые (*Inheritable*);

– текущие (*Effective*).

Когда процесс порождает дочерние процессы, наборы разрешений дочерних процессов переноситься из родительского. Когда процесс порождает

дочерний процесс, его новые наборы рассчитываются по определенным формулам (4)–(6).

Наследуемый набор разрешений используется только для расчета новых наборов прав для дочерних процессов.

$$pI' = pI; \tag{4}$$

$$pP' = fP \mid (fI \& pI); \tag{5}$$

$$pE' = pP' \& fE, \tag{6}$$

где (pI', pP', pE') – наборы разрешений дочернего процесса, (*pI, pP, pE*) – наборы разрешений родительского процесса, (*fI, fP, fE*) – наборы разрешений файла.

Файловые разрешения позволяют присваивать наборы программам. Используя файловые разрешения, можно сократить количество привилегий, доступных этой программе, при ее запуске не привилегированным пользователем.

Расширенные средства (SELinux), как и использование Capability, позволяет более тонко настроить права доступа к ресурсам сети [7]. Пользователям системы назначаются роли, таким образом, что они не смогут доступ к файлам или процессам, если не установлена специальная метка. Метки расширенных средств, позволят обозначить только те файлы и процессы к котором процесс будет иметь доступ, что сузит круг возможностей злоумышленника.

Основной особенностью системы расширенной безопасности – это использования концепции наименьших привилегий [7], которые требуются пользователю или процессу для осуществления запрошенных действий. На рис. представлен алгоритм проверки права доступа.

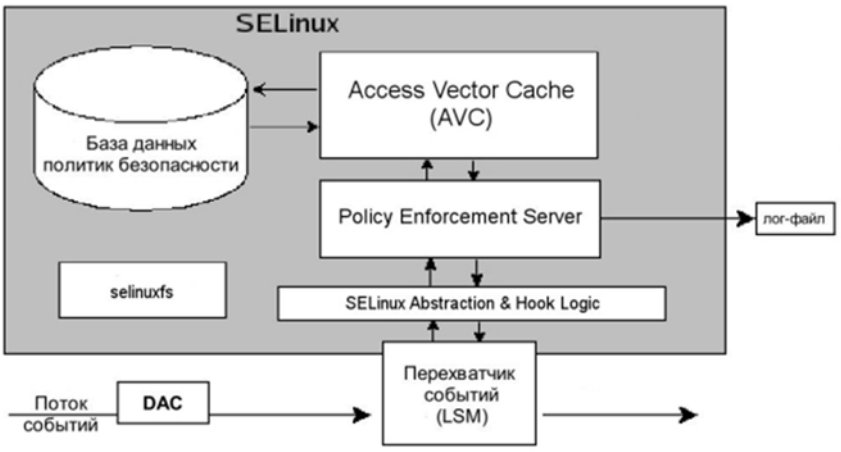


Рисунок. Схема работы системы расширенной безопасности

Система расширенной безопасности состоит из пяти основных компонентов:

– модуль взаимодействия с файловой системой;
– перехватчик событий (*Linux Security Modules*);
– модуль организации контроля доступа (*Policy Enforcement Server*);
– база данных политик;
– модуль быстрого доступ к политикам (*Access Vector Cache*).

Механизм работы организован следующим образом:

– Субъект ОС (процесс) пытается совершить определенное действие над объектом (файлом, каталогом, сокетом), которое разрешила базовая система защиты. Это приведёт к созданию потока обращений к объекту.

– Каждое обращение на выполнения действий с объектом перехватывает модуль Linux Security Modules (LSM) и вместе с контекстами безопасности субъекта и объекта предается подсистеме Abstraction & Hook Logic, отвечающая за взаимодействие с LSM.

– Информация передается Policy Enforcement Server (PES), который отвечает за принятие решения о доступе субъекта к объекту.

– Для принятия решение о запрете (разрешении) действия, модуль PES обращается к модулю Access Vector Cache (AVC) сохраняющей наиболее часто используемые правила.

– Если AVC не содержит решения для соответствующей политики, то запрос необходимой политики переходит к самой базе данных политик.

– Найденная политика передается PES, на основе которой он принимает решение.

– Если запрашиваемое действие удовлетворяет полученной политике, то операция разрешается, иначе операция запрещается.

Из рассмотренного выше следует, что базовая система управления доступом ОС GNU/Linux представляет из себя простую систему обеспечения безопасности. Однако при запуске вредоносного программного обеспечения, с привилегиями суперпользователя, ОС не способна контролировать совершаемые программой действия, в связи с тем, что привилегии суперпользователя дают неограниченные полномочия в системе. Но существует расширенные средства защиты ОС GNU/Linux, которые позволяют более тонко решить задачи по обеспечению разграничения доступа к ресурсам ОС.

Однако использование строгой политики в качестве основного, привело к множеству проблем с приложениями, использующие нестандартные настройки. Многие сервисы перестали работать, будучи заблокированы механизмом SELinux. Большинство разработчиков рекомендовало перейти к целевой политике или вообще отказаться от механизма SELinux. В свою

очередь целевая политики обеспечивала защиту только популярных сервисов. Для обеспечения безопасности дополнительных сервисов, требуется ручная модификация политики.

Список используемых источников

1. Вахалия Ю. Unix изнутри: пер. англ. СПб. : Питер, 2003. 843 с.
2. Столлингс В. Операционные системы: пер. англ. М. : Вильямс, 2002. 848 с.
3. Стивенс У. UNIX: взаимодействие процессов. СПб. : Питер, 2002. 576 с.
4. Ravi S. Sandhu, Pierangela Samarati: Access Control: Principles and Practice // IEEE Comunication Magazine 1994.
5. Гостехкомиссия России. Руководящий документ: Защита от несанкционированного доступа к информации. Термины и определения. М. : ГТК, 1992.
6. Гостехкомиссия России. Руководящий документ: Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. М. : ГТК, 1992.
7. Selinux user's and administrator's guide [Электронный ресурс]: Red Hat Enterprise Linux., 2017. URL: https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/selinux_users_and_administrators_guide/index (дата обращения 24.12.2017).

Статья представлена научным руководителем, кандидатом технических наук, доцентом А. В. Красовым.

УДК 004.056.57

ОСНОВНЫЕ ПРИНЦИПЫ ИСПОЛЬЗОВАНИЯ УНИВЕРСАЛЬНОГО КОДА ДЛЯ ПРОТИВОДЕЙСТВИЯ НЕСАНКЦИОНИРОВАННОГО КОПИРОВАНИЯ

С. И. Штеренберг

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

В данной статье будет изложены основные принципы использования универсального кода для противодействия несанкционированного копирования. Решение о использовании СМК в качестве главной системы защиты информации для именно отечественных программных разработок будет рассматриваться в рамках научного исследования на тему «Разработка метода цифровой стеганографии на основе СМК для защиты программного обеспечения».

цифровая стеганография, несанкционированное копирование, обфускация, реверс-инжиниринг, исполняемые файлы.

Как известно, операционные системы (ОС) сегодня стали играть огромную роль в мире потребительской электроники. Еще одной потребностей выступает для ОС – защита государственных и военных нужд. Показательный пример – российский дистрибутив Astra Linux SE. В данной работе не имеет место разбор всего функционала данной ОС, однако следует заметить, что на основе Astra Linux развернуты и функционируют десятки информационных систем – как в государственных, так и в коммерческих структурах [1].

Поскольку Astra Linux вовсю используется в разных проектах, связанных с обработкой информации различных уровней конфиденциальности, у разработчиков уже есть статистика, по которой можно судить о корректности реализации модели управления доступом. Не менее важны исследовательские работы, в которых формировались модели нарушителей в рамках известных уязвимостей информационной безопасности CVE (*Common Vulnerabilities and Exposures*).

Проверке подверглись известные «проблемы» модели Белла – Лападулы. К примеру, деклассификация – когда пользователь с высоким уровнем конфиденциальности случайно или намеренно помещает данные из объекта с соответствующей мандатной меткой в объект с меткой более низкого уровня. Или нарушение логики доступа к данным при обработке потока информации в распределенной среде.

Моделировалась и проблема компрометации субъекта доступа, в ходе которой повышается уровень его привилегий (включая получение привилегий PARSEC). В результате можно получить возможность управлять доступом к защищаемой информации.

Очевидное решение таких проблем – это модификация формальной модели управления доступом. В случае Linux это делается добавлением модулей LSM, которые реализуют систему PARSEC. Ее основой стала мандатная существенно-ролевая ДП-модель. Разработка ведется в рамках научной школы в Институте криптографии, связи и информатики Академии ФСБ России [2].

В общем случае эта модель (рис. 1) относится к классу ДП-моделей, то есть моделей управления доступом (Д) и информационными потоками (П), в которых учитывается не только единичный акт доступа к данным, но и направления распространения потоков информации при выполнении операций над данными.

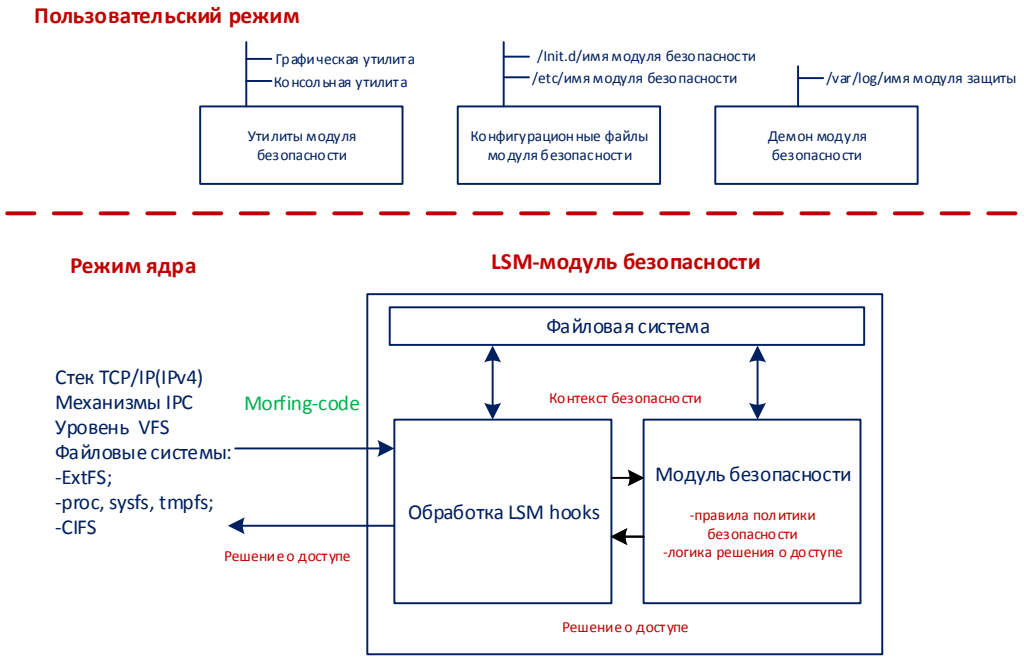


Рис. 1. Подсистема безопасности в Astra-Linux

Для защиты системных файлов, исполняемых файлов данной системы и разрабатывается на кафедре защищенных систем связи СПбГУТ сам универсальный код (СМК). В состав данного СМК входит так называемая «модель распространения СМК по защищаемой операционной системы». Состоит она из следующих алгоритмов, которые описаны ниже.

Самостоятельно, сам СМК может представиться в виде набора специального ПО [2]. В отдельных случаях механизм работы СМК напоминает отдельные элементы по части распространения, инициализации и внедрения данных. Типовые блок-схемы работы всего СМК в модели распространения как приложения представлены на блок-схемах (рис. 2–3).

Как обычно, ЗИ начинается с запуска приложения (рис. 2). СМК первоначально инициализирует свой запуск в системе, подготавливая данные для стеговложения. Этап для подготовки стеганоконтейнеров подходит следом за запуском СМК [4]. Обязательным остается подсчет количества информации, которую СМК необходимо обработать для стеганоконтейнера (рис. 3).

Первоначально СМК лишен определенной части защитных механизмов. Вопрос о СЗИ для самого СМК оставался актуальным еще долгое время, однако решением о сохранности исходных данных для самого СМК пришло в виде добавления к программе двух принципиальных модулей «Модуль уточнения сигнатуры программ» и «Модуль взаимодействия с защищенной ИС» (рис. 3).

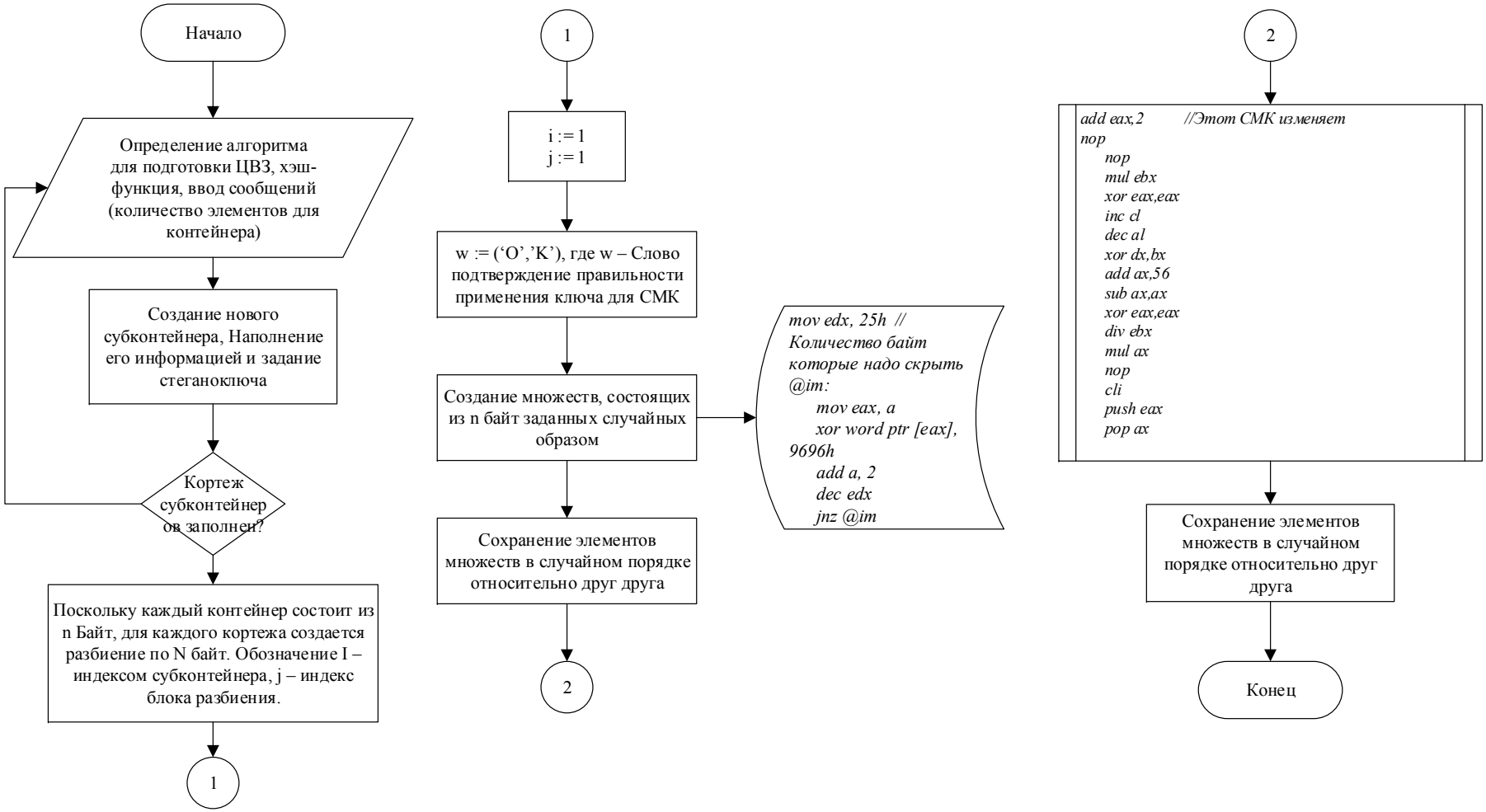


Рис. 2 – Инициализация для подготовки взаимодействия с контейнерами в защищенной ИС с компонентами решателей

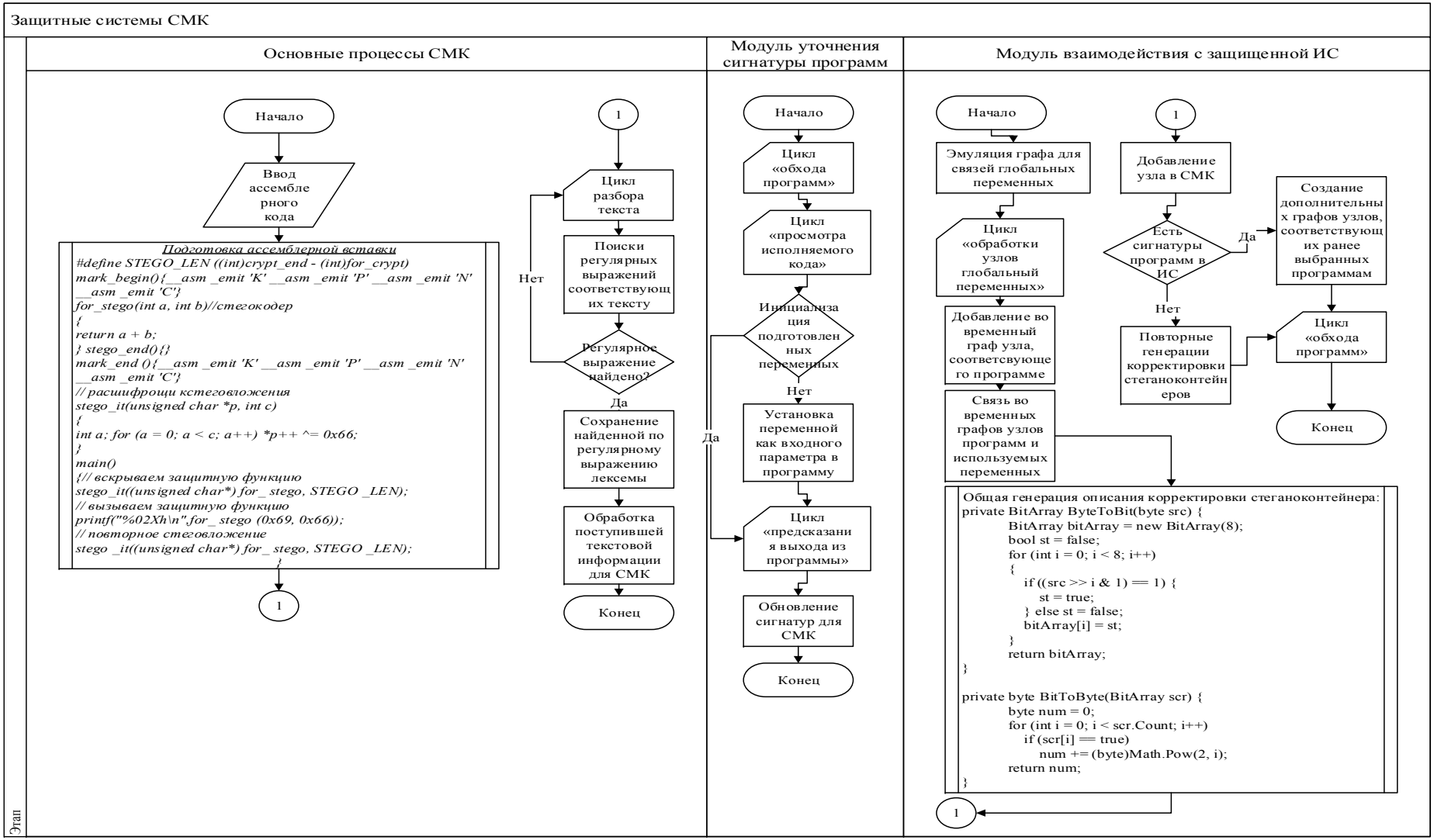


Рис. 3. Схема эмуляции защитных систем СМК с дополнительным применением стегановложений в разных ассемблерных вставках

Первый модуль сосредотачивается на обходе исполняемых файлов и просмотре их на пригодность стеганоконтейнера. Здесь механизм действия совпадает с механизмом функционирования руткита. Имеется таблица вызовов Import Address Table (IAT), где также при изменении записи в таблице вызовов контролируется исполнение программ и, при необходимости, перенаправляется на требуемые функции [5]. Общая идея захвата сходна с вредоносными программами и состоит в следующем:

1. Идентифицировать таблицу вызовов, получить её адрес;
2. Сохранить существующую в таблице запись;
3. Подменить запись новым адресом;
4. Восстановить исходную запись.

Второй модуль запускает процессы, связанные с системой графов СМК (рис 3), в которых видна демонстрация пути СМК по защищенной ИС. В ходе этого СМК должен применить алгоритм, схожий с руткитом, а именно алгоритм скрытия процесса:

1. Получение указателя на процесс, к которому принадлежит текущий поток, с помощью вызова PsGetCurrentProcess();
2. Получение PID процесса;
3. При несовпадении PID с искомым осуществляется переход по двусвязному списку (поле *ActiveProcessLinks*, тип LIST_ENTRY);

Изменение полей ActiveProcessLinks.

Список используемых источников

1. Журнал «Хакер». Спецвыпуск. # 48 [Электронный ресурс] Режим доступа: https://xakep.ru/issues/xs/048/

2. Лебеденко Е. Русский бронированный Debian. Как устроена новая модель управления доступом в Astra-Linux-SE [Электронный ресурс] // Хакер. 15.09.2015. Режим доступа https://xakep.ru/2015/09/15/astra-linux-se/

3. Штеренберг Г. И., Сагдеев А. К. Разработка методологии детектирования ботнетов с помощью software-defined networking / Информационные технологии и телекоммуникации. 2017. Т. 5. № 2. С. 106–113.

4. Красов А. В., Шариков П. И. Методика защиты байт-кода java-программы от декомпиляции и хищения исходного кода злоумышленника / Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2017. № 1. С. 47–50.

5. Яковлев В. А. Границы для оценки неопределенности в системе передачи со случайным кодированием / Радиотехника. 1996. № 12. С. 58.

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

A N N O T A T I O N S

PLENARY MEETING

Ledenev V. Experience in Building a Cable Infrastructure Monitoring System Using the Fiber-Optic Acoustic Sensor “Dunay”. – PP. 4–9.
The technology of detection of vibro-acoustic effects using distributed fiber optic sensors is increasingly used in various industries due to both a number of advantages inherent in the technology itself and the development of a number of specialized software applications. In particular, on the basis of this technology, a monitoring system of such a valuable infrastructure resource as cable sewerage can be deployed.
Key words: distributed fiber optic sensor, detection of vibro-acoustic effects, optical platform "Dunay", "T8", coherent reflectometer, cable infrastructure monitoring, access control.

Kotenko I. Cybersecurity Analytics: Analysis of the Current State and Perspective Research Directions. – PP. 10–19.
The paper analyzes a problem of constructing systems that implement advanced security analytics. It presents a status of research and development in the field of cyber security analytics. Models, techniques, methods and tools for cybersecurity analytics are considered. The promising areas of research and development of SIEM systems are outlined. The paper reviews own research in the field of developing security monitoring and incident management systems.
Key words: cybersecurity, security monitoring and incident management, cybersecurity analytics, cyber attack response, user and entity behavior analytics, security analysis, countermeasure generation, big data, machine learning, distributed and parallel data processing, distributed artificial intelligence, visual analytics.

Zikratov I. Current Issues Information Security Cyberphysical Systems. – PP. 19–22.
Development of telecommunication systems and their integration with physical objects of the external environment result appearance of new models of the information systems based on a paradigm of the Industry 4.0.
Features of construction and operation of cyberphysical systems, such as control decentralization, spatial remoteness of cyberphysical devices and finding them outside the controlled territory, need of use of telecommunication technologies for exchange of information between information objects, limitation of their idea of system, and also unpredictable dynamics of an external environment cause need of new approaches for detection and neutralization of information threats.
Key words: cyberphysical systems, telecommunication technologies, information threats.

INFORMATION AND COMMUNICATION NETWORKS AND SYSTEMS

Doynikova E, Kotenko I. Techniques and Tools of Response to Cyberattacks in the Industrial Internet of Things (invited talk). – PP. 23–28.
Development of the industrial internet of things leads to new opportunities for cybercriminals. As the result in recent years an interest to the technologies of response to cyberattacks in such systems grows considerably. In this work we analyze main research and practical solutions in the area of the industrial internet of things security. Their main advantages and disadvantages are outlined. The advantages of use of neuro-fuzzy networks and genetic algorithms are provided. In the future work we plan to develop the system of automatic response to cyberattacks in the industrial internet of things on the base of these technologies.
Keywords: industrial internet of things, cyberattacks, response to cyberattacks, decision support, neuro-fuzzy networks, genetic algorithms.

Avcharova A., Goldstein B. On the Implementation of Foggy Computations in Post-NGN Networks. – PP. 28–33.
Fog computing is a horizontal, system-level architecture that distributes computing, storage, control and networking functions closer to the users along a cloud-to-thing continuum. Fog computing is an extension of the traditional cloud-based computing model where implementations of the architecture can reside in multiple layers of a network's topology. The article covers the application areas, the OpenFog reference architecture developed by the Consortium to assist developers in creating the maintenance of hardware, software and system elements for fog computing and also an example of the implementation of OpenFog in the modern world.
Key words: Fog computing, Cloud computing, OpenFog, IoT.

Akimova A., Kovzur M. Development of Software Module for Protection of IP-PBX Elastix Against False Calls. – PP. 33–37.
IP-telephony has been widely deployed in enterprise communication networks. Nowadays Elastix is one of the most popular software IP-PBXs. The PBX is built on a modular architecture and allows the development and installation of additional software components. The purpose of the article is to develop an algorithm for protection of the IP-PBX from false calls to the numbers of the free hotline, as well as developing a software module that implements the proposed algorithm.
Key words: IP-PBX, Elastix, security algorithms, information security.

Akishin V. Evolution of Customer Relationship Management in Telecommunication Specificity. – PP. 38–42.
Today customer loyalty and churn rate are one the most important issues for telecom operators. Realities of the telecommunications market force companies to operate in a situation when the majority of customers have already divided among different telecom service providers. This situation makes telecom operators implement Customer Experience Management concept

into their processes. The paper considers premises of new approach to interaction with customers and also a variant of a functional model which describes modern aspects of Customer Experience Management in telecommunication specificity.
Key words: customer experience, Loyality, TM Forum.

Akishin V., Kormanovskaya A. Method of Estimation of Customer Experience on Various Stages of Customer Lifecycle. – PP. 42–47.
Customer experience is a concept formed from a variety of factors and represents a set of impressions and sensations received by the customer throughout the lifecycle. One of the most important aspects in the competent construction of the process of interaction with the customer is the aggregate analysis of customer experience using mathematical methods. In this article, considers various mathematical methods for evaluating customer experience, in particular, fuzzy cognitive maps.
Key words: Customer Experience, Customer Experience Management, cognitive maps, fuzzy logic.

Aleksandrova E., Ivanov G., Kovtsur M. Analysis Protection Mechanisms of Wi-Fi Networks. – PP. 47–51.
Recently, the technology of wireless Internet access has been increasingly used. Large companies, restaurants, hotels, universities, as well as public and private organizations that often have a large list of employees, instead of wired corporate networks use wireless. The most common way is to transfer data over a Wi-Fi network, which allows employees to connect anywhere in the coverage area. However, there is a problem in ensuring the confidentiality and integrity of data transmitted using the IEEE802.11 family of standards. In this paper considers the analysis of possible attacks on users by the attacker. A model of a secure wireless network is proposed, using modern technologies.
Key words: Wi-Fi networks, network attacks, phishing, spoofing, handshaking, sniffing, security of Wi-Fi networks, multifactor authentication, biometrics, model of the data protection system.

Andreeva E., Bylina M., Glagolev S. Features of Practical Realization of Quasisolitonic Fiber-Optical Communication Systems. – PP. 52–56.
Calculations and simulations of soliton fiber-optic communication systems have been carried out, in which the maintenance of the quasi-soliton mode of signal transmission is realized by the method of loss control. Two methods of loss control using discrete and distributed optical amplifiers are considered. The advantages of using distributed amplification are shown. Engineering formulas for the design of soliton communication systems are given.
Key words: Fiber-optic communication systems, optical fiber, chromatic dispersion, dispersion of group velocities, attenuation, nonlinear optical effects, optical solitons, phase self-modulation, optical amplification.

Andreeva E., Valyukhov V., Kuptsov V. Fibre Optics CCTV Systems and Security Alarms. Part 1. Active Equipment. – PP. 57–61.
We developed, researched and constructively executed a set of modulator and demodulator using a frequency modulation signal for passive optical systems. It was realised fiber optic transmission channel of a color high-quality television image with sound. The fiber-optic video

network was built, which performs the functions of managing technological processes and protection.
Key words: videosystems, security systems.

Andreeva E., Valyukhov V., Kuptsov V., Sumkin V. Fibre Optics CCTV Systems and Security Alarms. Part 2. Testing. – PP. 61–66.
Testing is one of the most important issues in maintaining an extensive fiber optic network. The monitoring system with the help of devices with extended capabilities are considered on the example of the constructed fiber-optic system, which allows for reliable observation of the territory of a distributed object, including conditions of high electromagnetic interference.
Key words: videosystems, security systems, fiber-optics test instruments.

Ateya A., Filimonova M., Muthanna A. 5G Cloud Computing Based on D2D Communication. – PP. 66–70.
The dynamic development of wireless technologies and increasing volumes of traffic create the prerequisites for the creation of all new communication standards. Currently, the development of the mobile 5G system is widely discussed. To implement this system, in addition to high reliability and good communication quality, ultra-small delay and high throughput, as well as better signal coverage. It is proposed to use technology MEC, implying the transfer of computing resources of a stationary cloud to the boundary of the radio access network (RAN). This will increase the bandwidth of the cloud and ensure network unloading. It is also proposed to use D2D-communication, which will positively affect the development of IoT. In addition, the use of foggy calculations in which certain tasks of stationary clouds are transferred to cloudlet processing, which is an ordinary user interface, is considered promising. This technology will increase the speed of decision-making by the system.
Key words: cloud, fog computing, structure.

Afanasev A., Vlasov R. Using of the Consecutive Statistical Analysis for Allocation Segments at the Speech Signal Processing – PP. 71–75.
Allocation of a speech signal processing segments on a basis of the consecutive statistical analysis parallel with nonparametric methods of probabilities distribution density estimation of the readouts instant values allows to use full statistical redundancy of speech more efficiently at it low bit rate coding. Due to the use of dependences in the speech signal which revealing is inconvenient at usually applied ways is based on the assumption of the normal law of distribution of instant values of readouts.
Key words: speech signal, segment of the analysis, sonant, criterion of Akaike, criterion of Vald.

Ahrameeva K., Popov L. Features of Application of Simple Linear Collision for Removing Supposed Covert Signals in Digital Video Sequences. – PP. 76–83.
A description of opportunity and relevance of application of the simple linear collision algorithm to obtain the original digital video sequence (covering object) from video sequence with possible presence of covert data is represented in this paper. Experiments, implementing a Type

II collision attack to remove a supposed stegosystem, evaluation of image quality, recommendations on optimal conditions and choice of parameters and so on have been represented. Tables and conclusions demonstrate all the results of the study.
Key words: steganography, steganalysis, digital video sequence, linear collision, temporal correlations, Type I and Type II collisions, decomposition into frames, linear addition, bitrate, redundancy and noise levels, compression, filter.

Balandin I., Dunaytsev R. A Wireless Site Survey of a Free Municipal Wi-Fi Network on Nevsky Prospect. – PP. 83–88.
In this paper, the results of a wireless site survey of a free municipal Wi-Fi network on Nevsky Prospect are presented. Using Ekahau Site Survey, the following information has been collected and charted: the total number of access points installed, the Wi-Fi channels used in the 2.4 GHz and 5 GHz frequency bands, the number of SSID in use, the amendments to IEEE 802.11 supported by the detected access points, and the TCP download data rates.
Key words: Wi-Fi, IEEE 802.11, WLAN, site survey, access point.

Bezborodova A., Girsh V., Staheev K., Shterenberg I. Design Atmospheric Communication Line as the Primary Network Subject to the City Building in St. Petersburg. – PP. 88–93.
Wireless laser communication systems are rapidly developing due to the intensive development of telecommunication systems. The article considers the question of the application of atmospheric optical lines for the organization of a communication network on the basis of the corporate network, with the consideration of regional factors on the example of Saint-Petersburg.
Key words: atmospheric optical lines, the influence of the atmosphere, the place of installation of equipment, the communication area.

Belova E.V., Polyakova E.V. Psychophysics of Perception: the Model of the Human Eye as a Constructive Element of Optical Instrument Engineering. – PP. 93–99.
The article deals with the engineering and psychological aspects of modeling the elements of optical instrument engineering and the human eye. A comparison is made between the elements of the device of optical instruments and the anatomical and physiological features of the construction of the visual image. On the basis of the above analogy, prospects for further improving the efficiency of the device and the operation of optical instruments are proposed.
Key words: modeling of elements of optical instrument engineering, anatomical and physiological features of the visual analyzer's structure.

Belozertsev I., Elagin V. OTT Services in LTE. – PP. 99–103.
In mobile networks LTE operators can offer their services for voice traffic. But users prefer to use the services of OTT providers. In this case, the operator is used as a transport, which affects the quality of voice traffic. Therefore, it is important to identify traffic from OTT services and to ensure transmission quality.
Key words: Quality of Service (QoS); Quality of Experience (QoE); OTT services.

Birih E., Gavrilov A., Satsuk E. Modern Problems of Maintenance of Internal Security of the Distributed Network of Government's Authority. – PP. 104–107.

When performing their tasks, a state organizations increasingly depends on the functioning of information systems and their security. The reverse side of the use of information technology are threats, the number of which in distributed networks is steadily growing. The article considers some recommendations to ensure security.
Key words: information security, distributed networks, risks of information security, external threats, internal threats, intruder model.

Birikh E., Koshurin A., Kushnir D., Starodubova D. The Research of Questions of Increase of Level of Protection of Bodies of Executive Power. – PP. 107–110.
Information security of Executive authorities includes ensuring the security of information and information resources, telecommunications and information exchange. The report deals with issues related to the provision of technical protection of information in the Executive branch.
Key words: information security, Executive power, technical protection, requirements, normative documents.

Birih E., Ferapontova S. To the Question of Audit of Personal Data. – PP. 111–114.
At the moment, the protection of personal data is one of the topical tasks of many Russian companies. This is due to an increase in the number of inspections by supervisors and an increase in complaints from subjects of personal data. The article deals with the categories of processing personal data, as well as the requirements for the processing and protection of personal data in information processing systems for personal data, presented to operators, depending on their type, for the audit of the security policy of personal data.
Key words: information security, audit, personal data, information protection, personal data operator.

Borodinskiy A., Goldshtein A. Model of Applying Neural Networks for Management of SON Network. – PP. 115–118.
In this article we analyse possibility of applying neural networks for managing SON network. Describing of functions which can do neural networks, including: network routing, distribution of channels in LTE networks, automatic configuration of network equipment, recovery of network in case of failure. Also there will be describing of proposed model, in which possible implementing neural network together with SON network and describing relevance of this technical solution.
Key words: neural network, model, neural network learning, configuration, optimization, recovery, self-organizing, network management.

Branitskiy A. Software Ways for Enhancing the Effectiveness of the Network-Based Signature Attack Detection Systems. – PP. 118–123.
Several approaches are considered to improve the effectiveness of network-based signature attack detection systems (ADS). Among the proposed approaches, we can highlight the usage of high-speed drivers for capturing the network packets, balancing of network traffic between several ADS processes, development of modified algorithms for searching the pattern substrings in signature rules, etc. The experimental results of ADS are presented.

Keywords: attack detection system, signature analysis, network card driver, network load balancing, substring search algorithm.

Bourdine A., Giniatulina A., Pashin S. Questions of Innovative Video Probe Kit Implementation. – PP. 123–128.

Today the modern video probe kit performs assessment of quality according to principle "PASS/FAIL" based to ratified standard IEC 61300-3-35. The IEC 61300-3-35 standard is a global common set of quality requirements for the surface of ferrule fiber optic connectors. This standard defines 3 zones of ferrule end face: "A" – core zone; "B" – cladding zone; "C" – ferrule zone. But it isn't enough. The forecast of key parameters would allow to draw firm conclusion about condition of the fiber-optical connector. The work presents the key questions of innovative video probe kit which allows to predict key parameters. Part of the mathematical apparatus is presented.

Keywords: fiber optic connector, insertion loss, reflection, fiber optic connector end face inspection, contamination.

Bourdine A., Evtushenko A., Sokolov Eu. Development of Fiber Optic Devices for Management of Optical Emission Mode Components Based on Optical Fibers with Written Precision Macrostructure Defects. – PP. 128–133.

This work represents results of experimental researches of implementation potentiality for optical emission mode component management devices based on optical fibers with written cascades of precision macrostructure defects "tapers" and "up-tapers" in various configureations and sequences.

Key words: optical fibers, precision macrostructure defect, up-tapers, tapers, insertion loss, cascade of macrostructure defects.

Bylina M. Interference Model of a Non-Uniform Two-Wire Communication Line. – PP. 134–138.

The paper proposes a model of the processes of propagation of electromagnetic energy through an inhomogeneous two-wire communication line in the frequency domain, based on the representation of the associated and reverse fluxes as interference of individual signals reflected from inhomogeneities. It is shown that the use of this approach makes it possible to substantially simplify the obtaining of time characteristics of inhomogeneous lines.

Key words: two-wire communication line, non-uniform two-wire communication line, concentrated heterogeneity, transfer function, impulse response, four-terminal network, matrix of A-parameters.

Bylina M., Halilov M. Optical Amplifiers Based on Stimulated Raman Scattering. – PP. 139–142.

The principle of operation, classification and parameters of Raman optical amplifiers are considered. A mathematical model is presented for the processes of amplification of optical signals in a Raman optical amplifier. The results of modeling Raman optical amplifiers are presented, which are compared with the results obtained by other researchers presented in the literature.

Key words: Raman amplification, optical amplifier, gain coefficient, forward pumping, backward pumping.

Valov A., Grebennikova N., Davydov V., Petrov A. Improvement of Metrological Characteristics of Quantum Frequency Standard on Atoms of Cesium-133. – PP. 143–147.
The development concept of modern telecommunications systems, transmission systems, satellite navigation systems, metrological service needs in modernization the currently used quantum frequency standards (QFS). The paper presents one of the directions QFS's modernization, namely, the development of a digital frequency synthesizer with the aim of improving the metrological characteristics QFS. The studies showed the effectiveness of new development application.
Key words: quantum frequency standard, data transmission system, synchronization, time, frequency stability.

Valyushkina Y., Lepeshkin M., Novikov P. Functional-Discretionary Access Control Model. Protection from Unauthorized Access Workstations of the Officials. – PP. 147–152.
In automated systems apply different access control model. For example, discretionary, mandatory, role-model integrity and others. All these models are based on the interaction between a single subject and a single object. To work effectively with any system, it is necessary to create models. In modern systems, the acute problems of security and sustainable functioning. Therefore, for its solution, consider the Union of two basic concepts of information security and functional safety, which you can use to describe safe operation in real time.
Key words: discretionary, automated systems, information security, functional safety.

Vereschagin M., Krasov A. Hidden Attachment to the Java Bytecode Using the Method of Overridden Variable Values. – PP. 152–154.
The article discusses the issues of copyright protection for software. In particular, the possibility and methods of embedding the digital watermark in executable Java files are considered. For a detailed consideration, a method based on redefining the values of variables is chosen. Consider instructions that can be replaced and data that can be successfully nested.
Key words: java, digital watermark, watermark, bytecode, hidden attachment.

Verikov A., Skorinov M. Analysis of Metrics for Assessing the Effectiveness of the First Line of Technical Support. – PP. 155–159.
The article describes about the notion of efficiency, possible goals of monitoring such a characteristic, and also allows metrics analyzing the effectiveness of the first line of technical support, which is a single entry point for customers. For the selection of indicators, open sources, TMForum specifications and COPC CX Standards were used.
Key words: metric, indicators, efficiency, assurance unit, technical support.

Vitkova L., Gavrilov A., Gerling E., Glushchenko A. The Audit of Local Computer Networks of Public Authorities. – PP. 159–163.
One of the most important stages in the management of information security it infrastructure of the enterprise is the audit of networks. The authors of the report consider the stages of the audit of local area networks of public authorities and present possible options for optimizing the process using the latest technology.
Keywords: local area networks, audit, topology, server, router, switch, network equipment, terminal devices, switching, software.

Vitkova L., Geraskina V., Yshakov I. Methods of Managing Information Safety in the Emergency Situation. – PP. 164–168.
Ensuring the safety of the city's population is one of the main tasks of the government. The article considers systems and methods for alerting the population, the effectiveness of their use, as well as excellent ways of alerting, trends in the use of various systems and devices in everyday life.
Key words: notification of emergencies, information, warning system, Internet network, information source.

Vitkova L, Glushchenko A, Sakharov D, Chmutov M. Choosing the Best Method of Assessing the Effectiveness of the Transition to Cloud Architecture. – PP. 168–171.
Cloud computing is developing all over the world, and more and more organizations are switching to cloud technology. Learning about the different methods of moving to cloud architecture allows you to choose the most efficient and reliable way. Cloud technologies have great potential, but when you switch to the cloud architecture, you can face a number of problems.
Key words: cloud architecture, OpenStack, unified information system, performance evaluation.

Vitkova L., Gorelenko V., Sakharov D., Chernoborodov I. Technology Blokchein and Its Adaptation. – PP. 171–174.
Nowadays blockchain technology becomes more popular. It has become quite popular because blockchain is used by crypto currency and precisely used with bitcoin. Various structures, including state ones, actively implement this technology for improving and optimizing their processes. In this article was analyzed detail in the "Bitcoin" crypto currency.
Key words: blockchain, cryptocurrency, BD, bitcoin, hashing, SHA256.

Vitkova L., Denisov E., Sakharov D., Ushakov I. The Questions of Formation of Safe Information System Based on the Technology of Decentralized Networks. – PP. 174–179.
The article discusses the formation of safe information system based on the technology of decentralized networks, including analysis of public and private network model, addressing vulnerability of information system elements based on the principle of peer-to-peer approaches to problems through existing concepts of the blockchain, a comparative analysis of common implementations of the formation of the blockchain circuits on the basis of the commonly marketed solutions. In the course of work were identified the advantages and disadvantages of various implementations, identified the necessary qualities of information systems based on decentralized networks.
Key words: information security, decentralized network, peer-to-peer, blockchain.

Vitkova L., Ivanov A. Review of Topical Threats and Methods of Protection in the Field of Cloud Calculations. – PP. 179–182.
Virtual infrastructure is an excellent tool for quickly and flexibly scaling IT systems, implementing experimental developments and saving in general. With a competent approach, it al-

lows you to save time and invest it in root tasks. But, it is also worth considering that the transition to the cloud entails many risks for confidential information stored in the information system. Before migration, it is necessary to compare all the advantages and disadvantages, possible losses in case of violation of the perimeter of security and develop the most effective methods of protection.
Key words: cloud computing, threats, information security, protection methods.

Vitkova L., Isakov A., Kovzur M. The Comparison of Mechanisms for Obtaining the Revocation Status of an X.509 Digital Certificate on the Certificate Authority on Astra Linux to Support PKI. –PP. 182–186.
Operating systems of the Windows family are widely used for the organization of accredited Certification Authorities (CAs) in the Russian Federation. However, one of the current trends is import substitution, both in hardware and software. So, one of the important tasks for the Ministry of Defense of the Russian Federation is a complete transition to the LINUX OS and to the hardware of domestic manufactures. However, the deployment of Certificate Authorities, based on the Russian Linux operating systems, and existing features are not described in the modern literature. This article describes comparison of certificate status checking mechanisms such as Certificate Revocation List u Online Certificate Status Protocol on the CA based on the Astra Linux operating system.
Key words: public key infrastructure, certification authority, certificate, CRL, OCSP.

Vitkova L., Mustafayev R., Sakharov D., Homin I. Using Big Data in the Processes of Security of the Information Sphere. – PP. 186–191.
The influence of information on the development of society is great. In case of its absence, humanity would remain in the stage of primitive order. Communication is considered a necessary parameter of human life and the fundamental basis for the existence of society as a whole. The process of information exchange went beyond the narrow framework of interpersonal communication and passed into the category of mass communication with the whole world. In the age of information technology, especially after the boom of social networks, a significant amount of information began to accumulate for each Internet user, which ultimately gave rise to the direction of Big Data. Big Data, to date, is one of the key drivers of the development of information technology
Key words: Big Data, security of the information environment, diagnostics and monitoring, network.

Vitkova L., Pronoza A., Sakharov D., Chechulin A. Security Problems of the Information Sphere in the Conditions of Information Warfare. – PP. 191–195.
Today, information and psychological struggle itself is very aggressive, and this struggle often generates local armed conflicts and wars, color revolutions. The high level of trust in social networks allows the enemy to model and create internal social conflicts through the use of misinformation, as well as allows the enemy to control the mass consciousness and opinion, to influence the destructive social processes within society.
Key words: Information and psychological struggle, social networks, information confrontation, information security, BigData.

Vladimirov S. Different Hardware Implementations of Maximum Length Codes Majoritary Decoder Based on the Dual Basis. – PP. 196–200.
In clause the features of constructing the hardware schemes of the error-correcting maximum length codes majority decoder based on the dual basis are considered. The performance of the decoder hardware implementation in terms of the clock cycles number required for decoding one codeword is estimated, taking into account the implementation options. An analysis is made of the hardware implementation of the decoder for various variants of the electrical circuit using the Logisim digital electrical circuit simulation system. A comparison is made with the hardware decoders of the maximum length code, based on another decoding principle.
Key words: maximum length code, majority decoding, minimum distance decoding, dual basis, hardware decoder, Logisim.

Vladimirov S., Kognovitsky O. The Small Set of Kasami Sequences and Their Decoding Based on the Dual Basis. – PP. 201–206.
In clause the dual basis based method of processing and decoding of a small set of Kasami composite sequences is analyzed. The advantages of this method are shown in comparison with other known methods. Probabilistic characteristics of the decoding method considered for BSC and AWGN channel models are determined.
Key words: Kasami sequence, small set of Kasami sequences, dual basis, error probability.

Volkogonov V., Ivanov A. Strategies for Protecting Cloud Privacy. – PP. 206–209.
This article discusses cloud privacy issues. As with other security systems, cloud confidentiality is understood as the confidentiality of data and calculations. Violation of cloud privacy can lead to the leakage of personal information of customers. Preservation of confidentiality is a more strict form of the original term, as it also prevents information leakage. Therefore, if the confidentiality of the cloud is violated, preservation of confidentiality is also violated. There are several basic approaches to maintaining cloud privacy. Use the security information center, trusted computing, and cryptographic protocols. Based on these approaches, the defense strategies proposed by the authors of the article are built.
Key words: privacy, cloud, cryptographic protocols, defense.

Volkogonov V., Radynskaya V. Methods of Attachments of Digital Watermarks in 32-bit PE-Files. – PP. 210–213.
At the heart of any software product is the intellectual property of its developers, so there is a question of copyright protection. The article is devoted to methods of introduction of digital watermarks in PE-files, with the purpose of their protection. Watermarks are embedded using equivalent changes in the source code of the program. It is assumed that such watermarks will not be noticeable to the attacker, and as a consequence, are resistant to attacks.
Key words: digital watermarks, PE-files.

Gagarina S., Kuznetsov V., Mikutavichaite D. Investigation of the Possibility of the Expansion of the EDFA's Gain Spectral Range. – PP. 213–217.
The article discusses the expansion of the EDFA's gain spectral range, which is one the most important tasks in the field of infocommunication. The spectral range shifting methods by using

several optical amplifiers are determined, the amplifier configuration effect on the amplification bands shifting are considered, the optimum power levels of the amplified signals and the parameters of the amplifiers for each of the ranges are selected in the simulation program. The obtained results can be used as a recommendation for amplifier developers and communication line designers.
Key words: erbium optical amplifiers, spectral range, offset, channel compaction.

Glagolev S, Dotsenko S, Kotov V. Comparative Analysis of Fiber-Optic Long-Range Communication Systems the Wavelength Division Multiplexing. – PP.218–222.
In the report, modeling of fiber-optic long-range communication systems with wavelength division (DWDM), consisting of separate amplifying sections, was carried out. Research fiber-optic communication system with various types of single-mode optical fibers and fibers compensating chromatic dispersion.
Key words: modeling of fiber-optic communication systems, DWDM, optical fiber, chromatic dispersion compensation.

Goihman V., Masiukaite A. An Overview of the Key Features of the QUIC Protocol. – PP. 222–226.
The world famous company Google has developed a new protocol QUIC, which combines the advantages of HTTP / 2, TCP and TLS. As a transport, the UDP protocol is used. Work on top of UDP allows users to speed up the execution of operations in the browser several times, compared with the use of traditional technologies.
The article considers the important advantages of the QUIC protocol and the basis for its implementation.
Key words: QUIC, Google, protocol.

Goikhman V., Pomogalova A. Development of Protected Voting System on the Basis of Blockchain Technology for the Bonch-Bruevich Saint-Petersburg University of Telecommunications. – PP. 227–231.
Blockchain technology is gaining popularity, expanding the area of its own applicability. Initially, the technology was developed as a financial system and had a rather narrow direction of development. With the development and launch of the Ethereum software platform, the view of technology has changed drastically, allowing it to be used in completely new areas, such as a variety of decentralized applications or a voting system, the development of which is the subject of this work.
Key words: Blockchain technology, voting system, Ethereum, smart contract, token, cryptocurrency.

Goikhman V., Pomogalova A. Blockchain Technology – a New Generation of Internet Network: Internet of Values. – PP. 231–235.
Centralized management nodes - are extremely vulnerable places in any system. There is one effective decision to protect it – decentralized systems. If there is no central management node it means, that the system is safe and there is no single point of failure. Blockchain technology allows not only to move to decentralization, but also look at the Internet from a new perspective.

Security, openness and prevalence are the three main advantages combined together in one technology that opens new sphere of Internet – Internet of Values.
Key words: Blockchain technology, Internet of Values, Ethereum, smart contract, token, cryptocurrency.

Goldstein A. Telecommunications Management as a Technical System. – PP. 236–242.
The goal of this paper is to provide a new telecommunications network management analytic and engineering approach that will be adequate to the modern and future NGN/IMS and post-NGN telecommunications networks instead of traditional OSS/BSS approaches.
Key words: OSS/BSS, business intelligence, post-NGN, multi-agent system, queuing network, network management.

Goldstein A., Pozdnyakov V., Skorinov M. – Analysis of Effectiveness of Ensemble Methods for Churn Prediction. – PP. 243–247.
Churn is the actual problem for service providers. They use different ways for determining risk of the churn and it's reduction. Usage of effective model of churn prediction is the very popular way to solve this problem. The article describes details of the ensemble methods and comparison of their effectiveness. ROC-analysis and set of business metrics are used for comparison.
Key words: ensemble methods, random forest, boosting, bagging, decision tree, churn, prediction, analysis of effectiveness, ROC-analysis.

Goldshteyn A., Shestakova A. Forecasting with Application of Neural Network in the Class BI Control Systems. – PP. 247–252.
The class BI control systems are especially in demand for the companies, which underscore customer focus of their business and are working in the conditions of the high competitiveness and dynamics. It give tools for the detailed analysis of root causes of the current situation in the company. Means of the class BI control systems transform information into knowledge, which allows to make decisions quickly.
The class BI control systems in combination with neural networks become the most powerful tool for business. The ability of neural network to study make it the most attractive tool. Process of training of neural network is in fine tuning of its internal parameters for to achievement specific targets. Process of training is performed out on the training set. The training set includes input meanings and relevant to it output meanings. In the systems of the class BI neural networks are most often used for forecasting.
Such parameters as loyalty of clients, outflow of clients and probability of adoption of the offer can be subject to the forecast in the sphere of telecommunications.
Key words: Business intelligence, neural networks, loyalty, outflow of clients, probability of adoption of the offer.

Goldstein B., Grineva A. Virtualization of Network Functions and Real-Time OSS. NEW Aspects of Network Management. – PP. 252–255.
The article is devoted to two modern directions of development of networks construction. The SDN (Software Defined Network) technology and NFV (Network Function Virtualization) are becoming increasingly popular due to the fact that they offer dynamic, flexible and, more

importantly, cheaper deployment of software network functions of OSS systems on the operator's network. The article discusses the architecture of SDNFV, which combines the advantages of both technologies and provides an opportunity to consider the task of network management in a different way.
Key words: virtualization, sdn, nfv, OSS systems.

Goldstein B., Eliseev S. About Fog Computing in the World of the Internet of Everything. The FoE Paradigm. – PP. 256–260.
Fog Computing is a completely new computing paradigm that aims to move Cloud computing objects and services to the access network. The ultimate goal is to increase the computing and network resources of the endpoint devices served, without increasing too large resulting service delays. The report examines the main technical aspects, the principles of building network architecture, examples of practical application and assessment of the actual effectiveness of this technological paradigm.
Key words: fog computing, internet of everything, cloud computing, IoT, fog of everything.

Goldstein B., Zhukovskiy I. Engineering Aspects of Software-Defined Networks. Interfaces, Standardization and Implementation Options. – PP. 260–263.
Software-defined networks are now becoming an increasingly popular topic. A great deal of effort is devoted to research and standardization in this field. And this is not surprising, because the use of software-defined networks based on open standards promises not only technical, but also economic benefits to all players in the telecommunications market. However, in software-defined networks, there are still a sufficient number of interfaces that do not have certain standards. The introduction of such standards will increase the attractiveness of SDN technology, as technologies ready for implementation on the network.
Key words: Software-defined networks, standardization, Interfaces.

Goncharov A., Petrenko M., Ukraintsev Y., Yushkevich A. Increase in Noise Stability on Lines of Modern Tropospheric Communication. – PP. 264–267.
In modern radio-receiving devices the threshold of the decisive scheme is defined on the basis of the classical Bayesian approach assuming that statistical characteristics of a signal and hindrances (their mixes) submit to a priori known normal density of distribution of probabilities (DDP) of instant values which is bending around, observed on his entrance. It not always meets the real situation demanding assessment not only parameters, but also PRV. In work application of the "naive" Bayes method allowing to restore PRV that is connected with need of processing of the statistical data which are taken off from a certain element of the radio-receiving path is offered.
Key words: analyzer of an interfering situation, probability of wrong reception, Parzen procedure of restoration of PRV.

Grebenshchikova A., Mahmood O., Muthanna A., Paramonov A. Overview of Various Methods of Data Collection for the Intelligent Transport System in Smart City. – PP. 267–272.
The paper considers a revolutionary technology that involves providing every technical device capable of connecting to the Internet. This concept is based on the combination of various

technologies, for the possible creation of inter-machine interaction, and not the relationship between the user and the machine. A smart city is a broader approach, the purpose of which is to raise the quality of life level for each person by combining modern information and communication technologies and the Internet of things. Devices used in a smart city can generate a huge amount of data, which in turn should be accumulated in time, processed and stored for later analysis. It follows that data collection is an important aspect in building a smart city. The proposed work presents various methods of data accumulation for an intelligent transport system.
Key words: smart city; internet of things; smart transport system.

Gudkov A., Malishev A., Malishev S. Multifactor Analysis of the Process of Forming of the System of Radiomonitoring and Radiotechnical Control. – PP. 272–276.
The article discusses the optimization problem of multifactor analysis of separate centers of radiomonitoring and radiotechnical control based on a formal approach, the stages of building these systems, defining performance indicators, including requirements for efficiency and criteria for its evaluation.
Key words: multifactor analysis; optimization; radiomonitoring; radiotechnical control.

Guseynov Z., Muradov P., Suleymanov A. Optimization of the Characteristics of Multiuser Telecommunication Networks. – PP. 276–280..
The main distinguished feature of modern telecommunication networks is the delivery of various types of information packets to the destination point on various routes. The main purpose of this study is to determine the dependence of packet loss on downloads and network resources. Mathematical models for calculating the probability of service failures in multichannel single node and multichannel multi node networks with a limited queue and absolute priority are proposed.
Key words: quality of service, Internet protocol, queuing system, multinode, singlenode, multichannel network.

Desnitsky V., Dumenko P. An Approach to Development and Evaluation of a Protocol for Remote Attestation of Java Programs. – PP. 280–285.
The paper proposes an approach to development and evaluation of a protocol of remote attestation and an example of a program developed in the Java programming language. The proposed protection is based on organization of two security methods, namely a method of checking control points and checking checksums of critical data structures involved in the code of our Java-program.
Key words: remote attestation, control point, checksum, critical structures.

Dobryanskiy V., KushnirD. Research of Introduction of Encryption and Authentication on the Functioning of Cryptocurrency. – PP. 285–290.
Supply the confidentiality of information is part of the vast majority of information systems. However, only at the present time methods of providing the encrypted authenticated channel in cryptocurrencies are being introduced. Without such protection, network monitoring and analysis of unencrypted data can compromise the confidentiality of information. The paper

discusses the features of implementing BIP 151 – the proposal to create a secure connection using incomplete nodes, which avoids a number of attacks on the system.
Key words: bitcoin, cryptocurrency, SPV, encryption, authentication, security.

Doynikova E., Savkov S., Chumak E. Information Security for the Bodynets: Main Trends. – PP. 290–295.
The paper reviews main research trends in the information security for the bodynets. This topic is highly relevant since such systems are directly connected with human body. Therefore the attacks on these systems can result in the serious damage to health. To specify the main requirements to the security of bodynets the key features of these systems and of the embedded devices are provided. The paper outlines and classifies the weaknesses of these systems and relevant security threats. Existing security assessment techniques and security measures, their advantages and disadvantages are analyzed. In the future research the authors plan to develop the technique of security assessment and awareness for the bodynets considering the disadvantages of existing systems.
Key words: bodynet**,** embedded devices, security, security assessment, security measures, efficiency.

Dolgun V., Litvinov V. Intellectual Storage Systems Research. – PP. 295–299.
The article considers modern systems of data archiving in automated process control systems. The principle of construction of multilevel and distributed systems of data collection and archiving, as well as aggregation and hot backup is described. The requirements for intelligent data storage systems are given. The relevance and necessity of studying this direction was stressed.
Key words: storage system, automated management system, intelligent system.

Dolgushev R., Kirichek R. Development of Models and Methods of Testing IoT Devices and Applications Based on the Model Network. – PP. 299–304.
The article is devoted to a review of the main stages of testing IoT devices and applications based on the model network. The research provides an analysis of existing approaches to testing, which are currently used in communication networks. Platforms that automate the testing process depending on the used system/architecture are also described here.
Key words: Internet of Things, IoT, testing, model network.

Donskov E., Ushakov I. Security Analysis of Virtual Infrastructure Using Software vGate. – PP. 304–310.
The article compares the offers from the Russian manufacturers on the protection of virtual infrastructure. As discussed in more detail on the company's decision to "Security code" to ensure the security of virtual machines - software vGate. As part of the article was the purpose of the software to review vGate with functional and practical point of view, the virtual infrastructure by deploying and installing the software on it. Also, the results of testing the main declared functionality of the vGate software are presented.
Keywords: virtualization, protection of virtual machines, vGate.

Donskoy D., Karev A., Saharov D. Social Engineering and the Human Factor in Information Security. – PP. 310–316.
Information can constitute a trade secret of the company, i.e. under existing or possible circumstances to increase incomes to avoid unjustified costs to save a market position. Social engineering is a set of measures and methods to gain unauthorized access to information. The complex is based on the use of human weaknesses and is very effective. In their work the authors investigate the existing social engineering techniques, as well as the influence of human factors on information security issues.
Keywords: social engineering, the human factor, the offender, information security.

Dunayev P., Ryabtsunov S. Analysis of Methods of Estimation of Bandwidth Throughput of Multiservice Network. – PP. 316–320.
Methods for modeling the bandwidth throughput of a multiservice network are considered, taking into account packet delay time. The DelayProg program was implemented to calculate the bandwidth throughput of the channel for a given probability of failure-free operation (licence No. 1105), which confirms the scientific novelty of this work.
Keywords: simulation methods, delay time, bandwidth throughput, IP packet.

Dunaytsev R., Egorova A., Analysis of High-Density Wi-Fi Design Principles. – PP. 321–325.
In this paper, we discuss features of the operation of Wi-Fi networks with a large number of users and devices in a limited space. A comparative analysis of high-density Wi-Fi design principles from different vendors is provided.
Key words: Wi-Fi, high-density wireless network, network design.

Dunaytsev R., Kulebiakina O. Analysis of Characteristics of Real-Time Traffic on the Sending and Receiving Sides. – PP. 325–328.
When transmitting traffic over communication networks, its characteristics change. This happens due to delays, collisions, various transmission errors, etc. As a result, the self-similarity property of traffic can change, which may adversely affect the quality of service.
Key words: network traffic, self-similarity, antipersistency, Hurst index.

Dunaytsev R., Moskalyuk A. Analysis of Characteristics of Aggregated Traffic. – PP. 328–332.
One of important properties of network traffic is its self-similarity. Once we know the Hurst index of network traffic, we can predict its behavior in the future. In this paper, we compare the results of estimation of the Hurst index for traffic from multiple users and traffic from one of those users summed with itself several times to simulate the aggregated traffic.
Key words: network traffic, self-similarity, antipersistency, Hurst index.

Dunaytsev R., Ovchinnikova P., Petrenko A. A Wireless Site Survey of a Wi-Fi Network of the Saint-Petersburg Metro. – PP. 332–336.

In this paper, the results of a wireless site survey of a free Wi-Fi network of the Saint-Petersburg metro are presented. Using Ekahau Site Survey, the following data have been collected and analyzed: the Wi-Fi channels used in the 2.4 GHz and 5 GHz frequency bands, the amendments to IEEE 802.11 supported by the detected access points, and the placement of access points inside trains.
Key words: Wi-Fi, IEEE 802.11, WLAN, site survey, access point.

Diubov A., Mokretsova M. Computer Simulation of AWG Wavelength Multiplexer. – PP. 336–340.
The design and operation of the AWG (Arrayed Waveguide Grating) multiplexer is considered. Multiplexers AWG are based on the diffraction grating formed by an array of waveguides. Multiplexers such as AWG are widely used in DWDM (dense wavelength-division multiplexing) networks. The report considers a program for calculating and computerizing the operation of multiplexers built on AWG technologies. The description and functionality of the program are given, the results of the multiplexer operation simulation are given. The prospect of using this software in the educational process when studying the technology of spectral multiplexing is considered.
Key words: multiplexer of wavelengths, dense wavelength-division multiplexing, array of waveguides, fiber-optic communication systems, computer simulation.

Elagin V., Mahura A. Applying the Social Graph for the Post-Processing of Lawful Interception Data. – PP. 340–344.
Currently, SORM have a problem with the visualization of data coming from SORM systems, for their rapid analysis by the end user. As one of the solutions for analyzing data from legitimate interception systems, a social graph can act. The graph will act as the programming object of the pointing connection of objects in the file through the edges, and for ease of display and analysis, each object will have distinctive properties depending on the identifier: shape, color, size. In addition to the graph itself, standard forms of reports will be used, such as excel tables and the ability to store data on a graph using the tab: File Save all / Save IPDR object. In the interface of the program it will be possible to get acquainted with the instructions for working with this program through the help instruction tab, which opens as a web page in the default browser.
Key words: graph, social graph, SORM system, SORM-2/3, IPDR, adjacency matrix, MATHLAB, biograph.

Elagin V., Onufrienko A. The Efficiency of the DPI System for Identifying Traffic and Providing the Quality of OTT Services. – PP. 345–349.
In this article, the authors introduce the definition of the term OTT service, compare them with traditional attendance. In this article, the authors identify the problems related to the data transfer through the telecom operator networks. DPI-technology procedures that provide the necessary requirements for Quality of Service when they make provision of services for its network for OTT-services. In this paper, we got the graphs of the results of the experiment and estimated the effectiveness of signatures, derived formulas for estimating the probability of events, and applied them to the appropriate statistical analysis.
Key words: Over The Top, OTT-service, DPI, Deep Packet Inspection, QoS, quality of service**.**

Elagin V., Frik P. Analysis of the ENUM System in the Realization of VoLTE. – PP. 350–354.
The article considers an example of a VoLTE connection setup scenario, as well as an ENUM system application in this scenario.
Key words: ENUM, VoLTE, LTE, IMS.

Ermolaev M., Ushakov I. Analysis of the Performance Encryption Algorithms in LTE Networks. – PP. 255–358.
In this work, the results of implementation of encryption algorithms in LTE networks are presented: KASUMI, 128-EEA1 (based on SNOW 3G), 128-EEA2 (based on AES), 128-EEA3 (based on ZUC). All algorithms are implemented in the programming language Python. In addition, the performance of these algorithms (the time taken in seconds to encrypt different data blocks) on different processors (Corei7-3610QM with a clock speed of 3.3 GHz, Corei5-3230M / 2.6 GHz and Corei3-2350M / 2.3 GHz) are analyzed. Recommendations are given on the use of algorithms for data encryption in LTE networks.
Key words: LTE, KASUMI, SNOW 3G, AES, ZUC, encryption.

Ermolaev M., Ushakov I. The Main Types of vulNerability in the Architecture SDN. – PP. 359–362.
Software-defined Networking is an actual solution in building the architecture of computer networks now. One of the main reasons for this - to make the network centrally programmable, the management functions in which will be transferred from the switches and routers to software applications implemented on a separate server-controller. However, such a decision, like many others, has its own types of vulnerabilities. They will be considered in this article.
Key words: SDN, software-defined networks, SDN architecture, vulnerability.

Esalov K., Kislyakov S., Parkhomenko A., Frolova Y. Analysis of Options for the Building of the Infocommunication Network for Operational Environmental Control on the Basis of SDN Technology. – PP. 362–367.
The article is devoted to the investigation of possible approaches to the management of SDN networks. To assess the capabilities of this technology, a model network has been developed that combines the Internet's controllers of things, the SDN segment, the Cloud storage for data received from sensors. The article describes the network model, its software and hardware implementation with justification of the choice of programs and devices.
Key words: IoT (Internet of Things), SDN, OpenDaylight, Open Network Operating System, OpenFlow, OpenvSwitch, Raspberry Pi.

Yesalov K., Maslyukhin S., Pavlenko M. Analysis of Architectures of Neural Networks for Solving Traffic Classification Problems. – PP. 367–372.
Classification of network traffic has become an important task due to the rapid growth in traffic volume transmitted over the Internet. There are many different approaches that solve this problem. Most of these approaches use the signatures extracted by the expert to classify network traffic. At present, new methods of traffic classification are emerging, based on machine learn-

ing and deep neural network architectures. This study analyzes the existing deep neural networks that solve the problem of classification of traffic and their comparison with established approaches.
Key words: classification of traffic, deep learning, neural networks.

Zarubin A., Koval A., **Moshkin V., Filippov A.** Analysis of Internal Wiki Resources Building an Ontological Knowledge Base. – PP. 372–377.
The author's research is devoted to solving the problem of developing intelligent algorithms and techniques for processing and analyzing intracorporate wiki resources that allow you to dynamically create the contents of a single knowledge store. Extraction of the fuzzy syntagmatic structure from the wiki-resources and the further presentation of the extracted semantically-determined knowledge in the form of a single unified subject ontology allow you to access the obtained knowledge base when solving complex expert tasks.
Key words: semantics, ontology, wiki-resources, knowledge base.

Zarubin A., Redguina N., Tarlykov A. Methods of in-Object Positioning of Objects and Personnel. – PP. 377–382.
Search for the best solution for the system of in-object positioning of objects and personnel. The solution is achieved by comparing the ways of monitoring the employment of staff, identifying their pros and cons. The report considers such systems as RTLS, RFID, biometric systems, video-fixation systems, and systems using special software.
Key words: monitoring, positioning, sensors, radio tags, RFID, RTLS.

Zakharova T., Ushakov I., Kholodenko V. TrustSec Technology as the Tool of Ensuring Information Security. – PP. 382–387.
This report is devoted to questions support of information security with use TrustSec technology. The architecture safety of TrustSec as the tool provides complex protection of networks is considered. This component allows to create a uniform, generalized policy for access to a network for all types of devices and connections, providing protection of transmission channels in the switched environments by means of the standard of encryption IEEE 802.1AE. The analysis of operation of TrustSec on the basis of the equipment of the Cisco company is made: routers, switches, which this technology is built-in.
Key words: TrustSec, information security, segmentation, networks, authentication, authorization, IEEE 802.1, SGT.

Zuyev I., Kovzur M. Elastix Performance Estimating Depending on the Used Services. – PP. 387–391.
IP-telephony is widely used in the corporate sector. Companies can use both hardware and software IP-PBXs to organize VoIP services. However, load testing methods are described insufficiently. The article describes the development of the load testing method for estimating the performance of IP-PBX. Recommendations on hardware configuration for IP-PBXs are provided.
Key words: IP-PBX, Elastix, methods of load testing, information security.

Zueva E., Yakovlev V. The Analysis of the Authentication key Distribution Protocol Based on the Magnetometric Data Using AVISPA Program. – PP. 392–396.
This article describes the AVISPA program used to test data transmission protocols for different types of attacks. There are four modules of this program, which allow you to determine the possible attacks on the protocols. The analysis of the authentication key dictribution protocol MagParing, distributed between two correspondents using Diffie-Hellman method, was done. Interactive schemes are constructed, proving the vulnerability of «MagPairing» to the "man in the middle" attack.
Key words: AVISPA, HLPSL, «man in the middle» attack.

Zueva E., Yakovlev V. The Analysis of the Authentication Key Distribution Protocol MagParing Based on the Magnetometric Data. – PP. 396–401.
The analysis of the authentication key dictribution protocol MagParing, distributed between two correspondents using Diffie-Hellman method, was done. The protocol is based on the exchange of random data between users, obtained from magnetometric sensors of smartphones. Security of MagPairing lies in dividing a random data block into two parts and alternately exchanging these parts. The article provides evidence that this protocol has vulnerabilities to man-in-the-middle attack during synchronization.
Key words: mobile devices, authentication, magnetometric date.

Zueva E., Yakovlev V. Development of a Noise-Resistant Authentication Method for Diffie-Hellman Key Distribution Protocol Based on the Magnetometric Data. – PP. 401–406.
In this article, method of authentication key, distributed between two correspondents using Diffie-Hellman method, was proposed. The method is based on using random sequences to authenticate keys generated by the magnetometers of smartphones. Protocol sensitive analysis was done for man-in-the-middle attack. Probability of the false removal of the key although the adversary does not intervene at all and probability of deception false key were calculated basing on the coefficient of discrepancy between the magnetometers data of users.
Key words: authentication, magnetometric data, Diffie-Hellman protocol.

Ivanov V., Koryakyn D., Holt-Winters Method for Increasing Reliability of Telecommunication Network. – PP. 406–409.
The actual problem of the functioning of information and telecommunication networks for special purposes remains the issue of monitoring both the components of networks and its individual elements. A promising method of data processing at the moment is the Holt-Winters method, the analysis of which this article is devoted to.
Key words: communication networks, Holt-Winters method.

Ivanov V., Nikitin B., Sergeev A. The Performance Requirements for Cross-Domain Optical Interfaces (Irda) Modern Digital Transport Networks. – PP. 409–414.
In the article the questions of regulation of components of fiber-optic communication line with optical amplifiers. The basic requirements for technical characteristics of the optical signals at points of regulation, transmitter and receiver devices, as well as to the optic tract. Considers the issues claimed in the design of communication lines. In addition, knowledge of rules, with

the technical operation of fiber-optic transmission lines, working on the technologies of synchronous digital hierachie STM, ATM and IP.
Key words: SDH, WDM, IP, amplifier, interface, transmitter, receiver, fiber-optic transmitter line.

Gnatenko K., Levin Yu., Martynyuk I., Shtanenko V. Technical Channels of the Console of Confidential Information. – PP. 414–418.
Possible options for the formation of technical channels for information leakage are considered. The operation of infocommunication systems for special purposes and information using is accompanied by the formation of electromagnetic, acoustic fields and electrical signals. In this regard, certain prerequisites are created for the formation of technical channels for information leakage when working with different technical means.
Key words: technical channels, information retrieval, information carriers, composite channel, capacity physical nature of the medium.

Imankul M. Actual Means of Increasing the Productivity of Infocommunication Systems and Networks. – PP. 419–423.
Today in the market of network technologies there is an accelerating race of speeds. Infocommunication technologies continue their development towards higher productivity and an increasing number of opportunities. The performance of infocommunication systems (ICS) is manifested in the speed of processing tasks and in the degree of utilization of system resources. SDN effectively solves problems at the interface between virtual and physical environments.
Key words: infocommunication system, bandwidth, resource, virtualization.

Kazakevich A., Stepanova E. The Monitoring System of the Current Network Synchronization in the Telecommunication System. – PP. 423–427.
Digital switching equipment must be synchronized to prevent slippage in the elastic memory. Slippage does not have a noticeable effect on ordinary telephone conversations, but it has a significant impact on the data transmission. That is why the network synchronization need to be equipped with monitoring systems, which allow real-time signal quality verification.
Key words: monitoring, monitoring system, synchronization, network-clock synchronization.

Kazakov D., Kovtsur M., Kozmyan A. Development of Integrated Solution of Secure IP-Telephony for a University-Scale Network with Remote Branches. – PP. 423–427.
IP-telephony allows to reduce the cost of communication and provides a wide range of additional services. In article the possibility of integration of IP-PBX to the existing network of the university. The solution provides fault tolerance, supports protocols for information security of IP telephony, video telephony, and also has a module for collecting statistics for individual university user groups.
Key words: VoIP, asterisk, billing, high-availability.

Kalyashov E., Savelieva A., Tarlykov A. Synthetic Data Generation for Neuron Network Training in Aircrafts' Classification Problem. – PP. 427–432.

The article describes a method to generate training data for neural network used in aircrafts' classification, localization and parameters' estimation problem. Common description of the approach used, top level algorithms and their configuration details are provided. Simplified problem is described, modeled and solved, results are also included.
Key words: neutral network, training, synthetic data generation, augmentation.

Karpov A., Lepeshkin O., Novikov P., Shostak R. Monitoring of the Transport Communication Network. – PP. 437–442.
Monitoring of the transport communication network in modern conditions of a variety and high complexity of network functioning becomes more actual. To date, monitoring is one of the most important tasks necessary for the organization of a full-fledged management of the transport network. Transport networks require a more accurate and flexible approach to monitoring, which is carried out by the advance installation of monitoring tools on the elements of the transport network. It is necessary to develop a universal monitoring system that will allow to solve in a complex all the most important problems of the transport network.
Key words: monitoring of, transport communication network, network management system, security incidents, control over network security.

Karpov A.V., Lepeshkin O.M., Novikov P.A., Shostak R.K. Method of Network Monitoring Facilities and Communication Systems. – PP. 442–445.
The article considers the issues of monitoring of objects and systems of communication and control to ensure their availability, reliability and efficiency. Under the existing principles of control systems and communication networks of the mobile segment for their functional cooperation in a single information space and implementation of sustainable information, sharing requires a new approach to the monitoring of mobile objects of communication.

Key words: monitoring, availability, reliability, efficiency, the mobile segment, single information space, sustainable information exchange, mobile objects of communication.

Karelsky P., Kovzur M., Ryazantsev K. Development of the Project for the Upgrading of the Provider's Network with the Implementation of MPLS Based Services. – PP. 446–450.
MPLS technology is widely used for the development of new networks of the service providers. However, there is a need to provide MPLS services over existing networks, which leads to partial network upgrade. The report defines the quantitative characteristics which play an important role in the selection of equipment for the provision of L2 / L3 VPN services.
Key words: multiprotocol label switching, MPLS, L2/L3 VPN, equipment characteristics, protection of MPLS services.

Kirichek R., Shklyaeva A. Development of Models and Methods of Interaction Between Unmanned Vehicle in Smart Cities and Communities. – PP. 450–454.
For several years, the interest in the production and use of unmanned vehicles has increased. It is the part of the future, where "smart" cars will transport us to different places without any drivers. That`s why it is necessary to develop an infrastructure that will allow the unmanned vehicles to interact with all road users 24 hours a day using network technologies with minimal delays.

Key words: unmanned vehicle, networking technology, infrastructure, V2V, V2I, intelligent transportation system.

Kislyakov S., Krasnov N. IoT-Platform for Management Housing and Utilities as SaaS Product of Telecom Operators. – PP. 455–458.
The article describes a model of a comprehensive solution for a telecom operator designed to monitor and account for the flow of various resources, as well as to manage and support the operation of telecommunications and terminal equipment. The solution can be provided to management companies as a PaaS product.
Key word: OSS/BSS, NRI, PaaS, IoT, Smart home.

Kislyakov S., Pletneva N. Analysis of Control Points from the OSS Module to a Software-Defined Networking (SDN). – PP. 458–461.
This article discusses main interaction model of OSS/BSS with SDN environment and technical characteristics of those network. Relevance of the subject is determined by SDN network popularity boost and lack of configured OSS-processes.
Keywords: Software-defined Networking, controller, communications service provider, business model.

Kislyakov S., Ryazanov D. Features of the Implementation of Middleware System as Part of the OSS-Landscape for Discovering and Testing. – PP. 462–466.
The article describes the experience of implementing a middleware system for discovering and testing.
Keywords: OSS/BSS, network discovering, business process automation, eTOM, STC ARGUS.

Kovtsur M., Polyanicheva A. Method for IPTV Service Authentication with RADIUS-Server. – PP. 466–471.
In the modern world, most devices have access to the Internet. Service providers offer additional services like IP-TV to users. Providers use different mechanisms to control users' access to this service. RADIUS servers are widely used to implement AAA services. This paper presents a scenario for using a RADIUS server to solve the task of authorizing users when accessing IPTV services.
Key words: RADIUS, multicast, IGMP, IPTV.

Kozlov S., Kuzmin V., Udaltsov N. Identification of Objects of Radiomonitoring in Multi-Level Structures Control Application of the Correlation Characteristic Evaluation Algorithm. – PP. 471–476.
The article under consideration deals with algorithms that define the structure of organization in space and the place of its objects in the system of levels of management in hierarchical systems. While modeling the organization structure in space the use of suggested algorithms allows to make alternative decisions on the construction of the organization and define its place in the levels of management.
Keywords: algorithm, structure, organization, object.

Kozyrev A., Shirokov G., Shumakov P. Comparison of Active Equipment GPON Class B+ and C+. – PP. 476–479.
The article presents a comparative analysis of the characteristics of widely used today active equipment class B+ for the deployment of passive optical networks GPON access and recently appeared on the market of similar equipment class C+. We provide the calculations that demonstrate the benefits of using the grade C+ is the grade B+. The report also reflects the ways to solve the problem of capacity building of the existing passive optical network, as well as the possibility of sharing equipment of class B+ and C+ in different variations.
Key words: access networks, last mile, GPON, optical budget.

Kolomeec M., Kotenko I., Chechulin A. Computer-Human Interaction Techniques for Improving the Effectiveness of Decision-Making Processes in Information Security. – PP. 479–483.
Given the constant growth in the amount and complexity of security information, it is necessary to develop data-management technologies and new methods of computer-human interaction. Solutions based on using non-standard methods of information representation and input (such as voice assistants, multitouch screens, virtual and augmented reality technologies and computer vision systems) have large potential. But despite the availability of devices, the systems based on these technologies are not widely used. This is due to the lack of fundamental principles for user interaction and data for these types of technologies. The paper presents the basic principles of construction of computer-human interaction systems, and outlines the potential of their use in information security systems.
Key words: computer-human interaction, information security, decision-making processes.

Komashinsky N., Kotenko I. Problems of Detecting Targeted Attacks (APT) Against Critically Important Information Systems. – PP. 483–488.
The paper presents difficulties in detecting targeted computer attacks against critically important objects, examines tools for detection and response against this type of attacks, develops recommendations and techniques to prevent uch attacks. Knowing the basic principles of organizing and conducting targeted attacks, as well as using the results of this analysis, will help to identify complex computer attacks at the initial stage, preventing the global consequences of malware infections and attempts to unauthorized access to critical infrastructure resources.

Key words: targeted attack, critically important information system, threat intelligence, malicious software, cybercrime.

Korpusov V., Olkhovoy O., Yakovlev V. The Research of the Random Number Generator Based on the Magnetometer. – PP. 488–493.
For the Android operating system an algorithm and a program, that allows you to output the data of the magnetometer smartphone on an external data storage, are developed. A method of constructing a random number generator based on a magnetometer is presented (MRNG). Statistical characteristics MRNG were researched using the graphical evaluation and NIST STS test group. The possibility of applying MRNG for cryptographic applications was tested.
Key words: random number generator, magnetometric data, statistical tests.

Kotenko I., Merkushev E. Data and Computation Integrity Mechanisms in Cloud Environments. – PP. 493–498.
The article is concerned with the existing integrity issues in cloud environments. Vulnerabilities that can be exploited by attackers, the threat models, as well as existing defense strategies in a cloud scenario are discussed. It gives a comprehensive review of both data and computation integrity mechanisms.
Key words: cloud systems, data integrity, computation integrity.

Kotenko I., Ushakov I. Models of NoSQL Databases for Cybersecurity Monitoring. – PP. 498–501.
The paper presents the main NoSQL databases (DB) models, including DB-models of key-value type, document databases, column-family databases, graph databases. A comparative analysis of existing models is conducted and a conclusion is made about the appropriateness of using existing data models for monitoring cybersecurity.
Key words: Big Data, NoSQL Data Bases, information security, monitoring.

Kotenko I., Ushakov I. Methods of Searching Insiders in Computer Networks Based on Big Data Technologies. – PP. 501–506.
The task of identifying insiders in modern computer networks (CN) is one of the main. Identifying insiders in the CN is a difficult task, especially in view of the huge flow of information, generated by users in the CN. It is necessary to select from the general flow of information and events information that allows to identify internal violators. The paper analyzes the approach of protection from insiders in computer networks, based on the use of the Cisco ISE corporate security control platform and its integration with Big Data processing technology implemented by the authors
Keywords: Big Data, insider detection, insider, computer networks.

Krasov A., Rogova A. Risks in the Implementation of BYOD Technologies in Organizations and Solutions to Minimize Them. – PP. 506–510.
This article examines the risks that can arise when implementing BYOD technology in organizations. These risks include violations of security and confidentiality. Tools were considered to minimize them. Practical solutions for organizations to reduce the previously described risks are given.
Key words: BYOD, risks, mobile devices, security issues.

Krasov A., Stepanov E. Network Steganography for ICMP protocol. – PP. 510–513.
With approach of an era of permanent wiretap of a traffic on the side of the states, providers and companies, information transfer on a network stopped being imperceptible. In case of a certain combination of circumstances the channel of which existence will not be known can be necessary.
Key words: steganography, network steganography, security, icmp.

Krasov A., Surmina M. Research and Development of Methods for Detecting Malicious Activity of Automated Botnet Construction Master's. – PP. 513–517.

In this article, we study the history, origins and architecture of building botnet networks. Methods of infection of end devices, ways of protection from infection, mechanisms of destruction of botnet networks are studied.
Key words: botnet, network steganography, hidden channels, DDoS.

Krasov A., Sharikov P. Security of the Java Programs by Meaning of the Program Water Sign. – PP. 517–520.
An important advantage of Java is its cross-platform, by using bytecode. However, using bytecode allows you to decompile Java programs to access their source code. This simplifies the appearance of pirated copies of Java programs, violates their copyright. This is a drawback of Java compared to other programming languages that compile into your own object code. The creation of digital watermark software is a relatively new approach to the problem of copyright protection, which includes the embedding of information about the ownership of the program in the program itself. The creation of watermarks has been extensively investigated and significant progress has been made in the development of sustainable and safe methods. In this article, the authors explore a new method for creating digital watermarks for software. The method is based on the signal detection theory, which is used to create multimedia digital watermarks.
Key words: java, digital watermark, watermark, bytecode, hidden attachment.

Krasov A., Yagudin I. Analysis of Active Network Attack: ARP Spoofing and DNS Spoofing. – PP. 520–526.
This article discusses the most common types of network attacks, the implementation of which is used to intercept traffic between nodes, and the substitution of the network address. Also proposed various methods of protecting against certain types of network attacks.
Key words: Active network attack, the attacker changes the network traffic, redirect traffic, and LAN.

Kurmazov A., Turkov N., Fedoseev O. Using the DSCP Code for Allowing a High-Priority Traffic. – PP. 526–531.
The priority of traffic (QoS) is the function of certain models of access routers, which analyzes traffic passing through and defines IP-telephony packets in it, and then gives such packets the highest priority for ensuring the guaranteed bandwidth of the network. This mechanism allows improving the quality of real-time services, especially in the conditions of a "narrow" channel. The use of the DSCP code is the most convenient and practical way of prioritization, which is confirmed in this article.
Key words: *priority of traffic, routers, DSCP code, Quality of Service.*

Kushnir D., Pavlukovich M. The Method of Authentication Ban Payment Card and Terminal Based on Quantum Cryptography. – PP. 531–535.
Bank payment cards represent an alternative to cash circulation. The number of bank cards and bank terminals is increasing, so there is a need for reliable protection of such systems that can combine the authentication capabilities of the card and the bank terminal. The article gives an example of the operation of a quantum label, various advantages and disadvantages of such an introduction are given.

Key words: quantum banknote, quantum optical money, quantum cryptography quantum cryptography, quantum banknote, quantum optical money.

Lauta O., Soloviev D. Using Mesh Networks to Ensure the Security of Data Transfer. – PP. 536–540.

The questions of the device of self-organizing mesh-networks, as well as the topology of their construction are considered. The main advantages of using such networks, their capabilities to organize wireless services for mobile subscribers, as well as problems of designing such networks are highlighted.

Key words: mesh networks, self-organizing networks, security in networks.

Fostach E., Levin M. Safety Problems of Cloud Computing. – PP. 540–544.

Cloud computing is a new computational paradigm that offers a distributed infrastructure. Despite the potential gains achieved from the cloud computing, the model security is still questionable which impacts the cloud model adoption. The security problem becomes more complicated under the cloud model as new dimensions have entered into the problem scope related to the model architecture, multi-tenancy and elasticity. Cloud computing security concerns, especially data security and privacy protection issues, remain the first problem of cloud computing services.

In the actual article we introduce a detailed analysis of the cloud security problem. We investigated the problem from the cloud architecture. Based on this analysis we offers a detailed specification of the cloud security problem and key features that should be covered by any proposed security solution.

Key words: privacy protection, cloud architecture, cloud computing, cloud computing security, data segregation, data security.

Leykin A. Safe Transport of Messages Using the SECURE SCTP Protocol. – PP. 544–549.

The Secure SCTP protocol provides transport-level security functions without the need for other security protocols, such as TLS or IPSec. In this article we will continue its consideration and dwell in more detail on the procedures necessary to integrate cryptographic functions into the basic SCTP protocol. The article presents an MSC scenario for the process of establishing, transport encrypted data, and destroying a secure session with explanatory comments.

Key words: SCTP, S-SCTP, Secure SCTP, Information Security.

Lepechkin O., Khudainazarov Yu. Development of the Requirements to System of the Provision to Information Safety. – PP. 550–555.

Change the requirements to system of the provision to information safety occurs nearly continuously. This depends on developments in methodologies of management organizing and technical system and developments in technology relationship and automations of management. The Conditions of the provision to information safety change. Is it For this reason required change the requirements to system of the provision to information safety. Change not always obvious.

Key words: provision to information safety, modeling, requirements on safety of the system.

Letavin D., Trifanov D. Microstrip Band-Pass Filter with Greatly Reduced Size. – PP. 555–559.
In this paper, a microstrip filter was simulated and fabricated, with triangular resonators identical in design. The power is located on the opposite side of the substrate from the resonators. The central frequency is 1790 MHz, and the bandwidth is 10.5%. The filter measures 16x15x1.5 mm.
Key words: *microstrip line resonator, band-pass filter.*

Letavin D., Trifanov D. Miniature Bandpass Filter in Microstrip Design. – PP. 560–563.
In this work, in the electrodynamic modeling program Ansys HFSS 3D, a microstrip bandpass filter operating at 5.2 GHz with a band of 1240 MHz was designed. This filter is realized on a substrate with a dielectric conductivity ε = 4.4 and a thickness h = 1.5 mm. This topology is technically simple to implement.
Key words: *microstrip line resonator, band-pass filter.*

Lipatnikov V., Malyshev B., Shevchenko A. Method of Adaptive Management of Progect Data-Processing Networks Based on Analyzing Intruders Dynamic Actions. – PP. 563–568.
The automated organization management system of integrated structure (AOM SIS) is perspective trend. There are two contradiction between modern requirements in new resources of informational invasion included realizing methods of communication and it is necessary to save system integrity of management in planning and entering modifications into system in situation of information opposition. It is necessary to design method for which documentary information of AOM SIS will be situated under control for supplying: a) Accessibility and appropriateness for applying in the right time and place; b) Protection (from lost confidentiality, integrity and improper using).
Key words: the automated organization management system of integrated structure (AOMSIS), data-processing network (DPN), computer attacks (CA), information security (IS), risk assessment, container virtualization, proactive management, scaling, protectability index.

Lipatnikov V., Shevchenko A. Model of Information Security System of Distributed Information Net Based on Controlling Net Vulnerabilities. – PP. 569–574.
In this title shown a model of information security system of distributed information net based on controlling net vulnerabilities. This model takes into account attack-and-defense process parameters, internal and external factors affecting the state of the system. A general structure of model is proposed. The structure is a set of modules that perform permanent scanning for the emergence of new vulnerabilities. It will allow attaining accurate detection and assessment of vulnerabilities by timely recording and analyzing real attempts of computer attacks. The aggregate of these modules performs the basic function of improving information security based on vulnerability analysis.
Key words: distributed information net, information security, computer attack, security index, vulnerability detection and valuation, risk estimation, probability graph.

Lobastova M., Matyukhin A. An Analytical Description of the Method for Detecting the Closed Loops in the Clock Network Synchronization Networks. – PP. 574–577.

There are listed the main problems, which could appear in the clock network synchronization networks. An analytical description of the method for detecting closed loops in synchronization networks is given. Discusses the computational complexity of the proposed algorithm.
Key words: clock network synchronization, loops in the synchronization network, adjacency matrix.

Lokhan'ko N., Ushakov I., Chekhutsky V. A Software-Defined Solution for VPN Service Providers. – PP. 578–581.
BGP/MPLS IP VPN and VPLS services are considered to be widely used in IP/MPLS networks for connecting customers' remote sites. However, service providers struggle with many challenges to provide these services. Management complexity, equipment costs, and last but not least, scalability issues emerging as the customers increase in number, are just some of these problems. Software-defined networking (SDN) is an emerging paradigm that can solve aforementioned issues using a logically centralized controller for network devices. SDN-based solution which considerably lowers the complexity of VPN service definition and management. This method eliminates complex and costly device interactions.
Key words: SDN, VPN, MPLS, VPLS, PE.

Morozov D., Petrova O. Information System for Department on the Basis of Infrastructure of Docker Containers. – PP. 582–585.
Every year, the popularity of the Docker virtualization system is growing. Interest in Docker is shown by both end users and software developers, which ensures its dynamic development. The article presents the implementation of the information system of the department on the basis of Docker containers. The interaction of containers in the system is shown.
Key words: virtualization, docker, isolated environment, containers, images, teaching materials, the site of the department.

Nabiev E. Problems of Introduction of NGN Networks. – PP. 586–589.
The development of telecommunications has led to the formation of a new conceptual model for building networks called the NGN (Next Generation Network). However, it, like any new direction, is characterized by shortcomings, underestimation of which is fraught with serious consequences for the market of telecommunications services. This work is devoted to the analysis of problems of implementation and operation of NGN networks and interactions of their components depending on the set of equipment suppliers .
Key words: telecommunications, next-generation network, microprocessor technology, computer logic, multiservice, multiprotocol label switching, asynchronous transfer mode.

Nguyen V. Universal Rank-Size Distributions in Network Traffic. – PP. 590–594.
In this paper network traffic rank-size statistics at different levels and organization are analyzed. Obtained results indicate that the rank-size traffic distributions of internal IPs in the local network and web servers can be described by beta distribution; rank-size traffic distributions of external IPs of the local network can qualitatively be approximated by the q-exponential distribution; rank-size traffic distribution of source and destination IPs of the backbone link closer to power law that is conventional form of Zipf's law.
Key words: Internet traffic, Local network, Rank distribution, Zipf's Law.

Nguyen D. Paramonov A. Application Areas of Device-to-Device Communications (D2D). – PP. 595–599.
The number of devices is expected to radically increase in near future, with an estimate of above 50 billion connected devices by 2020. The subscribers demand improved data rates, with reduced latency and increased system capacity. To endure the rising demands, cellular networks need to undergo suitable changes. For fulfillment of the rising needs of users and efficient utilization of the available scarce resources, device-to-device (D2D) communication is being looked upon as an important emerging technology for present and future cellular networks. It allows peer-to-peer communication between users, with improved spectral efficiency, energy efficiency and system throughput. In this paper, a survey on D2D communications has been offered, along with its major applications which make D2D become a successful paradigm of wireless networks.
Key words: D2D, device-to-device, D2D communications, Inband D2D, Outband D2D, 5G.

Nikitin B., Sergeev A., Smirnov G. Score Speed fiber PON Technologies. – PP. 599–604.
Score the maximum transfer rate for trunk, distribution and Subscriber stations network based on VOLS integrates key factors defined by the needs of subscribers to telecommunication services. For its reliable assessment must be performed multivariate analysis communication structures, however, engineers take into account only highlights the formation of communication structures.
Key words: broadband subscriber access, technology FTTx, PON, budget of VOLS.

Pantyukhin O., **Parashchuk I., Saenko I.** Analysis of the State of Research on the Modeling of Access Control to Information in Cloud Infrastructures of Critical Information Systems. – PP. 604–609.
The article offers systematic results of a detailed analysis of the state of research in the field of access control to information, taking into account the specific features of cloud storage systems that are components of critical information systems. The results of the analysis of the state of research in the field of application of artificial intelligence methods for optimization, verification and reconfiguration of access control policies are presented. The use of the results of this analysis will make it possible to increase the validity of decisions taken in the development and application of perspective models of access control in order to find out the possibilities and ways of their implementation in cloud infrastructures.
Key words: critical system, information system, access policy, methods, models, cloud infrastructure, resource, security breach, security.

Paramonov A., Houssein M., HusseinO. Research of the Use of Channels of the Standard 802.11 (2,4 GHz Band) in Urban Conditions. – PP. 610–614.
The article is devoted to the investigation of the traffic of the wireless broadband access network of the IEEE 802.11 family standards (in the 2.4 GHz band) in city conditions. The method of monitoring the 2.4 GHz channels (sniffing) was used to measure the parameters. The statistical traffic characteristics such as the distribution of time intervals between packets, packet lengths are obtained. The results obtained can be used to construct an analytical or simulation model of traffic.
Key words: traffic, IEEE 802.11, microcontroller ESP8266, access point, channel, intensity.

Paramonov A., Hussein O. Tasks of Clustering D2d Communications in the Networks of the Fifth Generation. – PP. 614–618.
Direct interaction between terminals (hereinafter referred to as D2D) makes it possible to improve such network qualities as reliability and resistance to various destructive factors, including reducing the intensity of subscriber load on base stations of the network. In this paper, we consider the tasks of organizing D2D communications in fifth-generation communication networks and the use of cluster analysis methods in these problems.
Key words: 5G, fifth generation, D2D, device-device, clustering, power consumption.

Podolyak R. Protection of the Network from Multi-Stage Attacks baSed on the Theory of Games. – PP. 618–622.
Interactions between intruders and the network administrator are modeled as an incompatible dynamic game without a zero sum with incomplete information, which takes into account the uncertainty and special properties of multistage attacks. The model is an approach with a fictitious game along a special game tree, where the attacker is the leader, and the administrator is the follower.
Key words: network security, game theory, attack trees.

Pryazhnikov V. The Analysis of the Method of Mathematical Modeling in a Software-Defined Networking. – PP. 623–627.
Mathematical modeling is used in the organization of any networks and systems, offering the opportunity to test an analogue of a future system, traditionally in telecommunications, the theory of mass service and the theory of graphs were used. Technological progress simplified the organization and architecture of networks, but brought additional conditions for the operation of networks, as a result of which new methods of mathematical modeling were involved in infocommunication.
Key words: software-defined networking, mathematical modeling, graph theory.

Rezhikov B., Saltykov A. Toward to Energy Saving NG-PON Networks. – PP. 628–633.
Analysis and development of energy-efficient solutions that can be used in next-generation passive optical networks (NG-PON) are important tasks. In the article mechanisms of energy saving by means of management of sleeping and transmitting modes on customer premises devices (ONT) are considered.
Key words: PON, OLT, ONT, Energy saving, Sleeping mode, DBA cycle.

Semenov A. A Method for Quickly Assessing the SHANNON Bandwidth of a Symmetric "Long" Ethernet. – PP. 633–637.
An algorithm for the rapid evaluation of the Shannon capacity is considered. The method is applicable to cable paths built using the direct connection scheme and is in demand when developing advanced information systems based on IP-technology for connection to the information system of single remote terminal devices.
Key words: Shannon transmission capacity, symmetric cable path, network, Fast Ethernet.

Smirnov K. Near-Infrared Range Photodetectors for Various Infocommunication Systems. – PP. 638–642.

Development of semiconductor device based on photocathodes, which work in near-infrared range, has been conducted since the eighties of the twentieth century. However, many problems posed by researches was unable to solve because of the level of technologies. At present time, development of super-high vacuum technologies, methods of growth semiconductor structures and fundamental researches of semiconductor A_3B_5 group allows to create high-sensitive photocathodes. Such photocathodes could be used in various fields of the applications.
Key words: photodetector, near-infrared range, heterostructure, photocathode.

Udaltsov A. Method of Estimating Bandwidth of a Transport Network of Military District in the Operation. – PP. 643–649.
In article the technique of calculation of throughputs of a communication system special purpose.
Key words: bandwidth, special purpose communication system.

Fitsov V. Employment Software Code for Optimization the Number of DPI-Servers by Maximal Element Method. – PP. 650–656.
This article describes employment python code for optimization network configuration of the DPI-system. The optimization subject is the number of CPU in the server (available computing resources). The optimization criteria are the time and number of CPU required by the DPI for analysis and making decision.
Key words: DPI, QoS, python, queuing network, maximal element method.

Tcvetkov A. Research of Existing Mechanisms of Protection of Linux Operation Systems. – PP. 657–662.
Enhance existing security solutions in operating systems is an important topic in the doctrine of information security of the Russian Federation. Before developing new mechanisms, it is necessary to research of existing mechanisms for protecting data and access control.
Key words: access control, capability, user, process, label.

Shterenberg S. The Basic Principles of Using the Universal Code for Countering Unauthorized Copying. – PP. 662–667.
This article will outline the basic principles of using the universal code (also called "SMC") to counter unauthorized copying. The decision to use the SMC as the main information security system for the domestic software development will be considered in the framework of the scientific research on the topic "Development of a method of digital steganography based on SMC for software protection".
Key words: digital steganography, unauthorized copying, obfuscation, reverse engineering, executables files.

АВТОРЫ СТАТЕЙ

NGUYEN Duc Viet — Postgraduate for Radio Systems Department, Saint Petersburg Electrotechnical University, ndvietleti@gmail.com

АВЧАРОВА Алёна Олеговна — выпускница кафедры инфокоммуникационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, iliazhukovski@gmail.com

АКИМОВА Александра Игоревна — студентка группы ИКТЗ-43 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, kodaine@bk.ru

АКИШИН Владимир Андреевич — аспирант кафедры инфокоммуникационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ведущий системный аналитик ООО НТЦ Аргус, akishin_vova@mail.ru

АЛЕКСАНДРОВА Екатерина Сергеевна — магистрант кафедры безопасности информационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, meowmewmeowmew@gmail.com

АНДРЕЕВА Елена Ивановна — кандидат физико-математических наук, доцент кафедры фотоники и линий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, andreevaelenafils@gmail.com

АТЕЯ Абдельмоталеб Абдельхамид Ашраф — аспирант кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, eng.abdelhamied@hotmail.com

АФАНАСЬЕВ Андрей Алексеевич — кандидат технических наук, доцент, сотрудник Академии Федеральной службы охраны Российской Федерации, fromnet@yandex.ru

АХРАМЕЕВА
Ксения Андреевна
кандидат технических наук, доцент кафедры защищённых систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, oklaba@mail.ru

БАЛАНДИН
Иван Андреевич
студент Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, balandinniv@gmail.com

БЕЗБОРОДОВА
Алена Сергеевна
студентка Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, alena.bezborodova2013@yandex.ru

БЕЛОВА
Елизавета Васильевна
кандидат психологических наук, доцент кафедры социально-политических наук Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, limax3@yandex.ru

БЕЛОЗЕРЦЕВ
Илья Алексеевич
магистрант кафедры инфокоммуникационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ilya.belozercev@outlook.com

БИРИХ
Эрнест Владимирович
аспирант кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, E.Birih@rkn.gov.ru

БОРОДИНСКИЙ
Антон Алексеевич
студент Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, borodinskiy26@yandex.ru

БРАНИЦКИЙ
Александр Александрович
младший научный сотрудник Санкт-Петербургского института информатики и автоматизации Российской академии наук, инженер лаборатории Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптики, branitskiy@comsec.spb.ru

БУРДИН
Антон Владимирович
доктор технических наук, доцент, помощник ректора по инновациям, профессор кафедры линий связи и измерений в технике связи Поволжского государственного университета телекоммуникаций и информатики, bourdine@yandex.ru

БЫЛИНА
Мария Сергеевна
кандидат технических наук, доцент кафедры фотоники и линий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, BylinaMaria@mail.ru

ВАЛОВ
Антон Петрович — студент кафедры фотоники и линий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, tony.valov2015@yandex.ru

ВАЛЮХОВ
Владимир Петрович — доктор технических наук, профессор Санкт-Петербургского политехнического университета Петра Великого, Valyukhov@yandex.ru

ВАЛЮШКИНА
Юлия Андреевна — курсант Военной академии связи им. Маршала Советского Союза С. М. Буденного, julia381995@mail.ru

ВЕРЕЩАГИН
Михаил Владимирович — студент Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, mvereschaginm@gmail.com

ВЕРИКОВ
Александр Юрьевич — студент Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, verikov.alex@gmail.com

ВИТКОВА
Лидия Андреевна — аспирант, ассистент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, iskinlidia@gmail.com

ВЛАДИМИРОВ
Сергей Сергеевич — кандидат технических наук, доцент, доцент кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, vladimirov.opds@gmail.com

ВЛАСОВ
Роман Сергеевич — сотрудник Академии Федеральной службы охраны Российской Федерации, vlasrsv@mail.ru

ВОЛКОГОНОВ
Владимир Никитич — кандидат технически наук, доцент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, legoloptim@gmail.com

ГАВРИЛОВ
Александр Сергеевич — магистрант кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, killervsspree@gmail.com

ГАГАРИНА
Софья Андреевна — студентка Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, sonka1603@mail.ru

ГЕРАСЬКИНА
Вероника Сергеевна
студентка группы ИКТЗ-44 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, geraskinaVeronika@yandex.ru

ГЕРЛИНГ
Екатерина Юрьевна
кандидат технических наук, доцент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, gerlingeu@gmail.com

ГИНИАТУЛИНА
Алина Маратовна
бакалавр Поволжского государственного университета телекоммуникаций и информатики, тестировщик программного обеспечения, Netcracker, alinaginiatulina@yandex.ru

ГИРШ
Виталий Александрович
начальник учебного военного центра Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, vgirsh@yandex.ru

ГЛАГОЛЕВ
Сергей Федорович
кандидат технических наук, доцент, заведующий кафедрой фотоники и линий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, glagolevsf@yandex.ru

ГЛУЩЕНКО
Александр Анатольевич
студент Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, Antivirys7@yandex.ru

ГОЙХМАН
Вадим Юрьевич
кандидат технических наук, доцент кафедры инфокоммуникационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича», vg@sotsbi.ru

ГОЛЬДШТЕЙН
Александр Борисович
кандидат технических наук, доцент кафедры инфокоммуникационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, генеральный директор НТЦ «Аргус», agold@niits.ru

ГОЛЬДШТЕЙН
Борис Соломонович
доктор технических наук, профессор, заведующий кафедрой инфокоммуникационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, bgold@sut.ru

ГОНЧАРОВ
Антон Васильевич — старший оператор научной роты Военной академии связи им. Маршала Советского Союза С. М. Буденного, anton0430@mail.ru

ГОРЕЛЕНКО
Виталий Витальевич — магистр кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, titov.vitaliy2014@yandex.ru

ГРЕБЕННИКОВА
Надежда Михайловна — студентка кафедры квантовой электроники Санкт-Петербургского политехнического университета Петра Великого, Alexandrpetrov.spb@yandex.ru

ГРЕБЕНЩИКОВА
Александра Андреевна — студентка Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, sgreben1@mail.ru

ГРИНЁВА
Анна Константиновна — студентка Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, greenevaanna@gmail.com

ГУДКОВ
Алексей Александрович — магистр, адъюнкт Военной академии связи им. Маршала Советского союза С. М. Буденного, gudkov_aa@rambler.ru

ГУСЕЙНОВ
Закир Насиб оглу — доктор философии по технике, и. о. доцента кафедры компьютерная инженерия и телекоммуникация Азербайджанского технологического университета, huseynov.z.n@mail.ru

ДАВЫДОВ
Вадим Владимирович — кандидатом физико-математических наук, доцент кафедры фотоники и линий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, davydov_vadim66@mail.ru

ДЕНИСОВ
Егор Игоревич — студент Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, egor.denisov16@gmail.com

ДЕСНИЦКИЙ
Василий Алексеевич — кандидат технических наук, старший научный сотрудник Санкт-Петербургского института информатики и автоматизации Российской академии наук, доцент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, vasily.desnitsky@mail.ru

ДОБРЯНСКИЙ
Виталий Валериевич
магистрант кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, dobryanskiyvv@gmail.com

ДОЙНИКОВА
Елена Владимировна
кандидат технических наук, научный сотрудник Санкт-Петербургского института информатики и автоматизации Российской академии наук, инженер Международной лаборатории «Информационная безопасность киберфизических систем» Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптики, doynikova@comsec.spb.ru

ДОЛГУН
Владислав Олегович
магистрант кафедры информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, dolgun.vlad@mail.ru

ДОЛГУШЕВ
Роман Андреевич
магистрант кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, r.dolgushev@gmail.com

ДОНСКОВ
Евгений Андреевич
студент группы ИКТК-45 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, radion2002@gmail.com

ДОНСКОЙ
Денис Михайлович
магистрант кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, dbondbon@yandex.ru

ДОЦЕНКО
Сергей Эдуардович
аспирант кафедры фотоники и линий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, 0472895@gmail.com

ДУМЕНКО
Павел Игоревич
студент Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, pasha-dumenko@yandex.ru

ДУНАЕВ
Павел Александрович
старший преподаватель кафедры радиотехники, электроники и телекоммуникаций Казахского агротехнического университета им. С. Сейфуллина, dunayev.kz@mail.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@spbgut.ru

ДЮБОВ
Андрей Сергеевич — кандидат технических наук, доцент кафедры фотоники и линий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, blip@bk.ru

ЕВТУШЕНКО
Александр Сергеевич — магистрант кафедры линий связи и измерений в технике связи Поволжского государственного университета телекоммуникаций и информатики, alex2194ru@yandex.com

ЕГОРОВА
Айсена Александровна — студентка Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, egorovaaysena1996@mail.ru

ЕЛАГИН
Василий Сергеевич — кандидат технических наук, доцент кафедры инфокоммуникационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, v.elagin@spbgut.ru

ЕЛИСЕЕВ
Сергей Михайлович — студент Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, iliazhukovski@gmail.com

ЕРМОЛАЕВ
Марк Игоревич — магистрант кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, marcermolaev@gmail.com

ЕСАЛОВ
Кирилл Эдуардович — начальник НОЦ «Исследование проблем инфокоммуникационных технологий и протоколов» Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, yk@bonch-ikt.ru

ЖУКОВСКИЙ
Илья Игоревич — студент Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, iliazhukovski@gmail.com

ЗАРУБИН
Антон Александрович — кандидат технических наук, проректор по информатизации, доцент кафедры инфокоммуникационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, azarubin@sut.ru

ЗАХАРОВА Татьяна Евгеньевна — магистрант кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, zakharova.tatiana95@gmail.com

ЗИКРАТОВ Игорь Алексеевич — доктор технических наук, профессор, декан факультета информационных систем и технологий Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, zikratov.ia@spbgut.ru

ЗУЕВ Игорь Павлович — студент группы ИКТЗ-43 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, walop9606@gmail.com

ЗУЕВА Елена Олеговна — магистрант кафедры защищенных систем связи Санкт-Петербургского государственного университета им. проф. М.А. Бонч-Бруевича, zuevaelation94@mail.ru

ИВАНОВ Александр Игоревич — магистрант кафедры защищенных систем связи Санкт-Петербургского государственного университета им. проф. М. А. Бонч-Бруевича, ivalex70@gmail.com

ИВАНОВ Артём Викторович — студент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, legoloptim@gmail.com

ИВАНОВ Василий Геннадьевич — кандидат военных наук, доцент кафедры «Организации связи» Военной академии связи им. Маршала Советского Союза С. М. Буденного, wasj2006@yandex.ru

ИВАНОВ Владимир Степанович — кандидат технических наук, доцент кафедры фотоники и линий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, vsivanovspb@yandex.ru

ИВАНОВ Генрих Николаевич — студент Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, genrikhivanovikt405@gmail.com

ИГНАТЕНКО Константин Анатольевич — слушатель Военной академии связи им. Маршала Советского Союза С.М. Буденного, ivanmartin88@yandex.ru

ИМАНКУЛ Манат Насиркызы — кандидат технических наук, доцент кафедры радиотехника, электроника и телекоммуникации Казахского агротехнического университета им. С. Сейфуллина, mimankul57@gmail.com

ИСАКОВ
Артём Сергеевич — студент группы ИКТБ-68м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, isakowww@yandex.ru

КАЗАКЕВИЧ
Андрей Анатольевич — старший оператор научной роты Военной академии связи им. Маршала Советского Союза С. М. Буденного, 89052585288@mail.ru

КАЗАКОВ
Дмитрий Борисович — аспирант кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, dkazakov@spbgut.ru

КАЛЯШОВ
Евгений Владимирович — инженер-программист научно-образовательного центра «Лаборатория программирования» Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ekalyshov@gmail.com,

КАРЕВ
Андрей Сергеевич — магистрант кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, fufelhmertz@gmail.com

КАРЕЛЬСКИЙ
Павел Владимирович — студент группы ИКТЗ-43 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, pasha.karelscky@yandex.ru

КАРПОВ
Александр Владимирович — адъюнкт Военной академии связи им. Маршала Советского Союза С. М. Буденного, Novikov.p.ark@yandex.ru

КИРИЧЁК
Руслан Валентинович — кандидат технических наук, доцент кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, kirichek@sut.ru

КИСЛЯКОВ
Сергей Викторович — кандидат технических наук, доцент кафедры инфокоммуникационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, бизнес-аналитик ООО «НТЦ Аргус», s.v.kislyakov@gmail.com

КОВАЛЬ
Альбина Радиковна — главный специалист управления информатизации Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, akoval@sut.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

КОГНОВИЦКИЙ
Олег Станиславович — доктор технических наук, профессор кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, kogn@yandex.ru

КОЗЛОВ
Сергей Юрьевич — адъюнкт Военной академия связи им. маршала Советского Союза С. М. Буденного, freeman35@mail.ru

КОЗЫРЕВ
Андрей Александрович — студент группы ИКТВ-34 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, kozyrev753@gmail.com

КОЗЬМЯН
Александр Владимирович — студент Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, avk96@list.ru

КОЛОМЕЕЦ
Максим Вадимович — младший научный сотрудник лаборатории проблем компьютерной безопасности Санкт-Петербургского института информатики и автоматизации Российской академии наук, kolomeec@comsec.spb.ru

КОМАШИНСКИЙ
Николай Александрович — аспирант лаборатории проблем компьютерной безопасности Санкт-Петербургского института информатики и автоматизации Российской академии наук, nckkm@ya.ru

КОРМАНОВСКАЯ
Анастасия Александровна — магистрант кафедры инфокоммуникационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, Stacy35@mail.ru

КОРПУСОВ
Василий Дмитриевич — магистрант кафедры автоматизации производственных средств Санкт-Петербургского государственного университета им. оф. М.А. Бонч-Бруевича, korpus95@mail.ru

КОРЯКИН
Денис Дмитриевич — командир научного взвода – младший научный сотрудник Военной академии связи им. Маршала Советского Союза С. М. Буденного, koryakinen@gmail.com

КОТЕНКО
Игорь Витальевич
доктор технических наук, профессор, заведующий лабораторией проблем компьютерной безопасности Санкт-Петербургского института информатики и автоматизации Российской академии наук, руководитель Международной лаборатории «Информационная безопасность киберфизических систем» Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптики, ivkote@comsec.spb.ru

КОТОВ
Владимир Владимирович
доктор технических наук, старший научный сотрудник, заведующий кафедрой специальные средства связи Института военного образования Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, kotov_vv@supertel.ru

КОШУРИН
Артем Дмитриевич
студент Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, akoshurin@inbox.ru

КРАСНОВ
Никита Эдуардович
студент Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, специалист ОСИС НТЦ «Аргус», vcshark84@gmail.com

КРАСОВ
Андрей Владимирович
кандидат технических наук, доцент, заведующий кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, krasov@inbox.ru

КУЗНЕЦОВ
Вячеслав Сергеевич
ассистент, аспирант кафедры фотоники и линий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, slava_kuznetsov@inbox.ru

КУЗЬМИН
Виталий Владимирович
адъюнкт Военной академия связи им. маршала Советского Союза С. М. Буденного, vitalij.kuzmin.1987@mail.ru

КУЛЕБЯКИНА
Ольга Романовна
студентка Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, olgaromanovn@mail.ru

КУПЦОВ
Владимир Дмитриевич
кандидат технических наук, доцент, Санкт-Петербургского политехнического университета Петра Великого, vdkuptsov@yandex.ru

КУРМАЗОВ
Александр Владимирович — старший оператор научной роты Военной академии связи им. Маршала Советского Союза С.М. Будённого, kurmasov-super@yandex.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

ЛАУТА
Олег Сергеевич — кандидат технических наук, преподаватель кафедры защиты автоматизированных систем специального назначения Военной академии связи им. Маршала Советского Союза С. М. Буденного, laos-82@yandex.ru

ЛЕВИН
Марк Вадимович — аспирант кафедры защищенных сетей связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, m.va.levin@gmail.com

ЛЕВИН
Юрий Владимирович — слушатель Военной академии связи им. Маршала Советского Союза С.М. Буденного, ivanmartin88@yandex.ru

ЛЕДЕНЕВ
Владимир Геннадьевич — ведущий менеджер отдела продаж ООО «Т8», ledenev@t8.ru

ЛЕЙКИН
Антон Владиславович — старший преподаватель кафедры инфокоммуникационных системы Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, a.v.leykin@gmail.com

ЛЕПЕШКИН
Михаил Олегович — студент Санкт-Петербургского политехнического университета Петра Великого, Novikov.p.ark@yandex.ru

ЛЕПЕШКИН
Олег Михайлович — доктор технических наук, доцент, старший преподаватель кафедры Военной академии связи им. Маршала Советского Союза С. М. Буденного, Novikov.p.ark@yandex.ru

ЛЕТАВИН
Денис Александрович — ассистент института радиоэлектроники и информационных технологий Уральского федерального университета им. первого Президента России Б. Н. Ельцина, d.a.letavin@urfu.ru

ЛИПАТНИКОВ
Валерий Алексеевич — доктор технических наук, профессор, старший научный сотрудник научно-исследовательского центра Военной академии связи им. Маршала Советского Союза С. М. Буденного, lipatnikovanl@mail.ru

ЛИТВИНОВ
Владислав Леонидович — кандидат технических наук, доцент кафедры информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, vlad-l@nm.ru

ЛОБАСТОВА
Мария Викторовна — ассистент, аспирант кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, mlobastovabk1@rambler.ru

ЛОХАНЬКО
Никита Олегович — магистрант кафедры защищенных сетей связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, byorn.gosu@gmail.com

МАЛЫШЕВ
Александр Сергеевич — ведущий инженер ООО «Девелопонбокс», malyshev14021988@gmail.com

МАЛЫШЕВ
Богдан Юрьевич — старший оператор научной роты Военной академии связи имени Маршала Советского Союза С. М. Буденного, bogdan160596@bk.ru

МАЛЫШЕВ
Сергей Романович — заслуженный изобретатель РФ, кандидат технических наук, доцент Военной академии связи им. Маршала Советского союза С. М. Буденного, malishevsr56@ya.ru

МАРТЫНЮК
Иван Анатольевич — адъюнкт Военной академии связи им. Маршала Советского Союза С. М. Буденного, ivanmartin88@yandex.ru

МАСЛЮХИН
Сергей Михайлович — инженер НОЦ «Исследование проблем инфокоммуникационных технологий и протоколов» Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, sermasl2009@gmail.com

МАСЮКАЙТЕ
Анастасия Владимировна — студентка Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича», anastasyvladova@mail.ru

МАТЮХИН
Александр Юрьевич — кандидат технических наук, доцент кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, sani@ton.net.ru

МАХМУД
Омар Абдулкарим
аспирант кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, comm_447@yahoo.com

МАХУРА
Андрей Александрович
магистрант кафедры инфокоммуникационных систем Санкт-Петербургского государственного университета телекоммуникаций им. Проф. М.А. Бонч-Бруевича, Andrey.Mahura@yandex.ru

МЕРКУШЕВ
Евгений Сергеевич
аспирант Санкт-Петербургского института информатики и автоматизации Российской академии наук, eugenemerkushev@gmail.com

МИКУТАВИЧАЙТЕ
Диана Сергеевна
студент Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, mikutavichaite@bk.ru

МОКРЕЦОВА
Маргарита Юрьевна
магистрант Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, margo-deva67@mail.ru

МОРОЗОВ
Денис Павлович
инженер-программист кафедры программной инженерии и вычислительной техники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, morozoff.py@gmail.com

МОСКАЛЮК
Алексей Алексеевич
студент Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича,
arzengard@mail.ru

МОШКИН
Вадим Сергеевич
кандидат технических наук, доцент кафедры «Информационные системы» Ульяновского государственного технического университета, v.moshkin@ulstu.ru

МУРАДОВ
Полад Джангир оглу
кандидат технических наук, доцент кафедры компьютерная инженерия и телекоммуникация Азербайджанского технологического университета, polad1942@gmail.com

МУСТАФАЕВ
Рафаэль Азадович
студент Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича,
martini_96.09@mail.ru

МУТХАННА
Аммар Салех Али
кандидат технических наук, доцент кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ammarexpress@gmail.com

НАБИЕВ
Етибар Ага оглы
старший преподаватель кафедры компьютерная инженерия и телекоммуникация Азербайджанского Технологического Университета, etibar63@yandex.ru

НГУЕН
Данг Куинь
магистрант кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, dangquynhd09vt2@gmail.com

НИКИТИН
Борис Константинович
кандидат технических наук, доцент кафедры фотоники и линий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, nbk117@mail.ru

НОВИКОВ
Павел Аркадьевич
адъюнкт Военной академии связи им. Маршала Советского Союза С. М. Буденного, Novikov.p.ark@yandex.ru

ОВЧИННИКОВА
Полина Андреевна
студентка Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, maana5@yandex.ru

ОЛЬХОВОЙ
Олег Олегович
студент Санкт-Петербургского государственного университета им. проф. М.А. Бонч-Бруевича, olkhovoy99@gmail.com

ОНУФРИЕНКО
Анастасия Валентиновна
магистрант кафедры инфокоммуникационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, anastasia.4991@mail.com

ПАВЛЕНКО
Михаил Евгеньевич
инженер НОЦ «Исследование проблем инфокоммуникационных технологий и протоколов» Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, tarke7773@gmail.com

ПАВЛЮКОВИЧ
Мария Вячеславовна
магистрант кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, zetterstrom000@gmail.com

ПАНТЮХИН
Олег Игоревич — кандидат технических наук, доцент кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, p_oleg99@mail.ru

ПАРАМОНОВ
Александр Иванович — доктор технических наук, профессор кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, alex-in-spb@yandex.ru

ПАРАЩУК
Игорь Борисович — доктор технических наук, профессор, Заслуженный изобретатель РФ, ведущий научный сотрудник Санкт-Петербургского института информатики и автоматизации Российской академии наук, инженер лаборатории Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптики, shchuk@rambler.ru

ПАРХОМЕНКО
Антон Олегович — студент Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, специалист ОСИС ООО «НТЦ Аргус», sponecs73@gmail.com

ПАШИН
Станислав Сергеевич — аспирант кафедры линий связи и измерения в технике связи, заместитель директора студенческого конструкторского бюро по инновациям Поволжского государственного университета телекоммуникаций и информатики, pashinstanislav@outlook.com

ПЕТРЕНКО
Алексей Сергеевич — студент Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, curvedside@gmail.com

ПЕТРЕНКО
Михаил Игоревич — командир взвода (научного) Военной академии связи им. Маршала Советского Союза С. М. Буденного, anton0430@mail.ru

ПЕТРОВ
Александр Анатольевич — аспирант кафедры квантовой электроники Санкт-Петербургского политехнического университета Петра Великого, Alexandrpetrov.spb@yandex.ru

ПЕТРОВА
Ольга Борисовна — старший преподаватель кафедры программной инженерии и вычислительной техники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, petromay@yandex.ru

ПЛЕТНЕВА
Наталья Сергеевна
студентка Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ytyta@yandex.ru

ПОДОЛЯК
Родион Сергеевич
аспирант кафедры защищённых систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, podolyak.rs@gmail.com

ПОЗДНЯКОВ
Виталий Александрович
магистрант группы ИКТС-63м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, pozdnyackov.vitaliy@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

ПОЛЯНИЧЕВА
Анна Валерьевна
студентка группы ИКТЗ-61м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, anna1993polyanicheva@gmail.com

ПОМОГАЛОВА
Альбина Владимировна
студентка группы ИКТК-45 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, alya.pomo@gmail.com

ПОПОВ
Леонид Геннадьевич
студент Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, leonidlitvinovo1994@mail.ru

ПРОНОЗА
Антон Александрович
аспирант лаборатории проблем компьютерной безопасности Санкт-Петербургского института информатики и автоматизации Российской академии наук, pronoza@gmail.com

ПРЯЖНИКОВ
Владимир Сергеевич
аспирант кафедры инфокоммуникационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, avyeloc1@gmail.com

РАДЫНСКАЯ
Виктория Евгеньевна
студентка Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, radynskaya.v@gmail.com

РЕДРУГИНА
Наталия Михайловна
студентка Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, quine97@mail.ru

РЕЗНИКОВ
Богдан Константинович
студент Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, rznkff@gmail.com

РОГОВА
Арина Николаевна
студентка Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, arinamymail@gmail.com

РЯБЦУНОВ
Сергей Юрьевич
кандидат технических наук, старший преподаватель кафедры радиотехники, электроники и телекоммуникаций Казахского агротехнического университета им. С. Сейфуллина, ryabtsunov@yandex.kz

РЯЗАНОВ
Дмитрий Ильич
студент Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, assanirvana@yandex.ru

РЯЗАНЦЕВ
Кирилл Сергеевич
студент группы ИКТБ-77М Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, kirillryazancev1995@yandex.ru

САВЕЛЬЕВА
Анастасия Андреевна
магистрант кафедры инфокоммуникационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, saa@spbgut.ru

САВКОВ
Сергей Витальевич
ассистент кафедры безопасности киберфизических систем Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптики, sergsavkov@gmail.com

САЕНКО
Игорь Борисович
доктор технических наук, профессор, ведущий научный сотрудник Санкт-Петербургского института информатики и автоматизации Российской академии наук, инженер Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптики, ibsaen@mail.ru

САЛТЫКОВ
Антон Радиевич
старший преподаватель кафедры фотоники и линий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, anton.saltykov@gmail.com

САХАРОВ
Дмитрий Владимирович — кандидат технических наук, доцент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, d.sakharov@rkn.gov.ru

САЦУК
Евгения Николаевна — специалист 1-го разряда отдела по защите прав субъектов персональных данных и надзора в сфере информационных технологий Управления Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций, sk_evgeniya@mail.ru

СЕМЕНОВ
Андрей Борисович — доктор технических наук, профессор кафедры автоматизации и электроснабжения Национального исследовательского Московского государственного строительного университета, andre52.55@mail.ru

СЕРГЕЕВ
Алексей Николаевич — старший преподаватель кафедры фотоники и линий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, a32@bk.ru

СКОРИНОВ
Максим Юрьевич — аспирант, ассистент кафедры инфокоммуникационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, skorinov@iks.sut.ru

СМИРНОВ
Геннадий Михайлович — старший преподаватель кафедры фотоники и линий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, Smirnov_G@bk.ru

СМИРНОВ
Константин Яковлевич — аспирант кафедры фотоники и линий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, konstantinsmirnov10@gmail.com

СОКОЛОВ
Евгений Дмитриевич — магистрант кафедры линий связи и измерений в технике связи Поволжского государственного университета телекоммуникаций и информатики, carlcarlson@list.ru

СОЛОВЬЕВ
Дмитрий Владимирович — оператор научной роты Военной академии связи им. Маршала Советского Союза С. М. Буденного, laos-82@yandex.ru

СТАРОДУБОВА
Дарья Дмитриевна — студентка Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, starodubova.95@mail.ru

СТАХЕЕВ
Константин Иванович — студент факультета ИВО Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, kos-leopold@mail.ru

СТЕПАНОВ
Егор Иванович — магистрант кафедры защищённых систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, egorstepanov@openmailbox.org

СТЕПАНОВА
Елена Александровна — начальник лаборатории ФГБУ «16 Центральный научно-исследовательский испытательный институт» МО РФ, Stepanovaelena-84@mail.ru

СУЛЕЙМАНОВ
Акиф Шамил оглу — доктор технических наук, профессор, ректор Азербайджанского технологического университета, inf@atu.edu.az

СУМКИН
Владимир Радомирович — старший преподаватель кафедры фотоники и линий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, sumkinv@mail.ru

СУРМИНА
Мария Сергеевна — магистрант кафедры защищенных систем связи Санкт-Петербургского государственного университета им. проф. М. А. Бонч-Бруевича, positifit@mail.ru

ТАРЛЫКОВ
Алексей Владимирович — начальник научно-образовательного центра «Лаборатория программирования» Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, atarlykov@gmail.com

ТРИФАНОВ
Данил Андреевич — студент Уральского федерального университета им. первого Президента России Б. Н. Ельцина, d.a.letavin@urfu.ru

ТУРКОВ
Никита Евгеньевич — оператор научной роты Военной академии связи им. Маршала Советского Союза С.М. Будённого, stipler95@mail.ru

УДАЛЬЦОВ
Александр Владимирович — капитан, помощник начальника учебно-методического отдела Военной академии связи им. Маршала Советского Союза С.М. Буденного, axil2003@yandex.ru

УДАЛЬЦОВ
Николай Петрович — кандидат военных наук, профессор Военной академия связи им. маршала Советского Союза С. М. Буденного, n-p-ud@mail.ru

УКРАИНЦЕВ
Юрий Дмитриевич — кандидат технических наук, доцент кафедры телекоммуникационных технологий и сети Ульяновского государственного технического университета, 9019471930@mail.ru

УШАКОВ
Игорь Александрович — старший преподаватель кафедры защищенных сетей связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ushakovia@gmail.com

ФЕДОСЕЕВ
Денис Олегович — кандидат технических наук, доцент, заместитель начальника НИЦ Военной академии связи им. Маршала Советского Союза С. М. Будённого, stipler95@mail.ru

ФЕРАПОНТОВА
Светлана Сергеевна — студентка Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, s.ferapontova@list.ru

ФИЛИМОНОВА
Мария Игоревна — студентка Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, filimonova_sar@mail.ru

ФИЛИППОВ
Алексей Александрович — кандидат технических наук, доцент кафедры «Информационные системы» Ульяновского государственного технического университета al.filippov@ulstu.ru

ФИЦОВ
Вадим Владленович — старший преподаватель кафедры инфокоммуникационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, noldi@iks.sut.ru

ФОСТАЧ
Елена Сергеевна — студентка Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, elena.fostach@gmail.com

ФРИК
Павел Александрович — студент Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, frik.pavel@mail.ru

ФРОЛОВА
Юлия Аркадьевна — студентка Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, fr95juli@mail.ru

ХАЛИЛОВ
Михаил Николаевич — студент группы ИКТФ-76м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, 1trspb571833@gmail.com

ХОЛОДЕНКО Валерий Юрьевич — студент Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, valera-holodenko@inbox.ru

ХОМИН Илья Игоревич — студент Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, angelok432@gmail.com

ХУДАЙНАЗАРОВ Юрий Кахрамонович — кандидат технических наук, старший преподаватель кафедры Военной академии связи им. Маршала Советского Союза С. М. Буденного, yu-78@yandexl.ru

ХУССЕЙН Мустапха Роблех — магистрант кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, Mustafa.djib@gmail.com

ХУССЕЙН Ошди Абдулкарим — аспирант кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, hussein.oah@spbgut.ru

ЦВЕТКОВ Александр Юрьевич — аспирант кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, alexander.tsvetkov89@gmail.com

ЧЕРНОБОРОДОВ Иван Сергеевич — магистрант кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, skich1984@gmail.com

ЧЕХУТСКИЙ Вячеслав Сергеевич — магистрант кафедры защищенных сетей связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, vyacheslav.chekhutsky@yandex.ru

ЧЕЧУЛИН Андрей Алексеевич — кандидат технических наук, доцент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, andreych@bk.ru

ЧМУТОВ Михаил Валериевич — студент Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, frost32.ru@yandex.ru

ЧУМАК Евгений Александрович — магистрант Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптики, eugenich@ya.ru

ШАРИКОВ
Павел Иванович — студент Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, sharikov.pavel@ro.ru

ШЕВЧЕНКО
Александр Александрович — младший научный сотрудник научно-исследовательского центра Военной академии связи им. Маршала Советского Союза С.М. Буденного, alex_pavel1991@mail.ru

ШЕСТАКОВА
Анастасия Алексеевна — студентка Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, nastya28011995@rambler.ru

ШИРОКОВ
Геннадий Александрович — старший преподаватель кафедры теории электрических цепей и связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, dashazab10@gmail.com

ШКЛЯЕВА
Алина Владимировна — магистрант кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, shkljaevaalina@rambler.ru

ШОСТАК
Роман Константинович — адъюнкт Военной академии связи им. Маршала Советского Союза С. М. Буденного, Novikov.p.ark@yandex.ru

ШТАНЕНКО
Василий Иванович — кандидат военных наук, доцент кафедры Военной академии связи им. Маршала Советского Союза С. М. Буденного, ivanmartin88@yandex.ru

ШТЕРЕНБЕРГ
Игорь Григорьевич — кандидат педагогических наук, заместитель директора Института Военного Образования Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, shterenberg@yandex.ru

ШТЕРЕНБЕРГ
Станислав Игоревич — ассистент кафедры защищенных систем связи, Санкт-Петербургского государственного университета им. проф. М. А. Бонч-Бруевича, stas.shterenberg.89@mail.ru

ШУМАКОВ
Павел Петрович — кандидат технических наук, профессор, заведующий кафедрой теории электрических цепей и связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, shumackov_pp@sut.ru

ЮШКЕВИЧ
Андрей Дмитриевич — оператор научной роты Военной академии связи им. Маршала Советского Союза С. М. Буденного, anton0430@mail.ru

ЯГУДИН
Ильдар Рашидович — магистрант кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, Ildardag@gmail.com

ЯКОВЛЕВ
Виктор Алексеевич — доктор технических наук, профессор кафедры защищенных систем связи Санкт-Петербургского государственного университета им. проф. М.А. Бонч-Бруевича, viyak@bk.ru

АВТОРСКИЙ УКАЗАТЕЛЬ