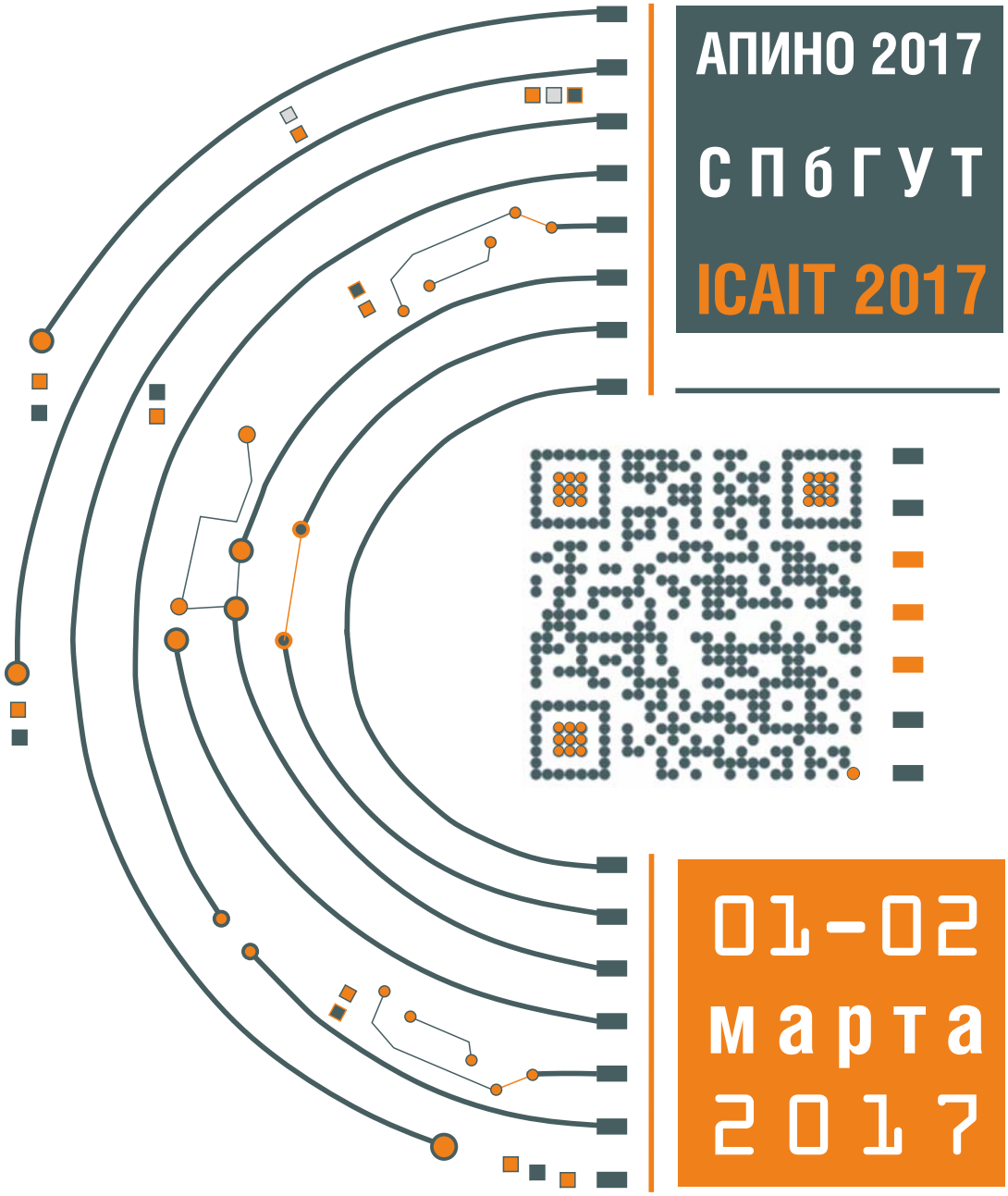
VI МЕЖДУНАРОДНАЯ НАУЧНО-ТЕХНИЧЕСКАЯ И НАУЧНО-МЕТОДИЧЕСКАЯ КОНФЕРЕНЦИЯ

«АКТУАЛЬНЫЕ ПРОБЛЕМЫ ИНФОТЕЛЕКОММУНИКАЦИЙ В НАУКЕ И ОБРАЗОВАНИИ»

6th INTERNATIONAL CONFERENCE ON ADVANCED INFOTELECOMMUNICATION (ICAIT 2017)



COLLECTION OF SCIENTIFIC PAPERS

СБОРНИК НАУЧНЫХ СТАТЕЙ

УДК 001:061.3(082)
ББК 72 А43

Актуальные проблемы инфотелекоммуникаций в науке и образовании. VI 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, 2017. Т. 2. 594 с.

ГЕНЕРАЛЬНЫЙ СПОНСОР

технологии бесконечности ®
КОМПАНИЯ «Т8»

СПОНСОРЫ КОНФЕРЕНЦИИ

АРГУС
НАУЧНО-ТЕХНИЧЕСКИЙ ЦЕНТР

UZTELECOM

bcc ИНФРАСТРУКТУРНОЕ СТРОИТЕЛЬСТВО И ИННОВАЦИИ

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 978-5-89160-149-9

Научное издание
Литературное редактирование,
корректура Е. А. Аникевич
Оформление Л. М. Минаков
Верстка Е. М. Аникевич
Подписано в печать 01.08.2017.
Вышло в свет 31.08.2017. Формат 60x90 1/8.
Уст. печ. л. 37,125. Заказ № 032-ИТТ-2017.
пр. Большевиков, д. 22, корп. 1.
Россия, Санкт-Петербург, 193232

СОДЕРЖАНИЕ

ИНФОКОММУНИКАЦИОННЫЕ СЕТИ И СИСТЕМЫ

УДК 004.056.5

СПОСОБ ПОСТОЯННОЙ АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ НА ОСНОВЕ ИНФОРМАЦИОННОГО ПОЧЕРКА

В. С. Авраменко

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

Одним из проблемных вопросов управления доступом к информации в автоматизированных системах различного назначения является обеспечение постоянного контроля подлинности пользователей на протяжении всего сеанса работы. В статье рассматривается способ постоянной аутентификации на основе информационного почерка пользователя, характеризующего индивидуальные особенности его работы на средствах автоматизации.

автоматизированные системы, пользователь, аутентификация, информационный почерк, сенсомоторный компонент, признак.

Проблема аутентификации пользователей в автоматизированных системах (АС) различного назначения относится к классу постоянных. Несмотря на многообразие современных средств и способов аутентификации угроза «подмены» пользователя является актуальной. Отсутствие готовых эффективных решений по реализации постоянного контроля подлинности пользователей (тем более – удаленных и мобильных) на протяжении всего сеанса работы обуславливает актуальность проблемы постоянной аутентификации пользователей (АП).

В первую очередь данная проблема актуальна для автоматизированных систем, нарушение безопасности информации в которых может привести к критическому ущербу. К числу таких систем относятся автоматизированные системы специального назначения, банковские инфокомму-

никационные системы, автоматизированные системы управления производством и т. д.). Также данная проблема актуальна и для автоматизированных систем, применяемых в сфере образовательной деятельности. В частности, существует потенциальная возможность «подмены» удалённого обучающегося более подготовленным пользователем на различных этапах «электронного» обучения, в том числе при прохождении процедуры удаленного автоматизированного контроля (тестирования) уровня знаний [1].

Основными требованиями к АП являются высокая защищенность аутентификатора (невозможность использования аутентификаторов другими лицами) и непрерывность на протяжении всего сеанса работы.

Наиболее распространенные способы аутентификации, основанные на применении паролей и токенов (электронные карты, жетоны и т. д.) не обеспечивают требуемого уровня защищенности и непрерывности АП. А на основе известных технологий биометрической АП (проверка отпечатков пальцев пользователя встроенными в средства ввода информации датчиками, сканирование изображения лица, рисунка сетчатки глаза и др.) реализовать постоянную аутентификацию на практике сложно, в том числе и по причине неудобства для пользователя.

Одним из путей решения проблемы постоянной аутентификации пользователей в АС является применение способа аутентификации пользователей по информационному почерку [2].

Информационный почерк пользователя (ИПП) представляет собой совокупность формализованных признаков пользователя, характеризующих индивидуальный стиль его работы на средствах автоматизации.

АП по информационному почерку пользователя относится к поведенческим методам биометрической аутентификации. Сущность АП по информационному почерку заключается в сравнении текущих значений признаков с эталонными на основе выбранного критерия (решающего правила). Эталонные значения признаков формируются после начальной регистрации пользователя на основе процедуры обучения. Текущие значения признаков формируются в процессе работы пользователя. Решение об истинности пользователя принимается в случае соответствия текущих значений признаков эталонным значениям.

ИПП в общем случае может включать сенсомоторный и психомоторный компоненты. Сенсомоторный компонент (СК) ИПП – это совокупность формализованных признаков пользователя, характеризующих его индивидуальные психофизиологические особенности работы на средствах ручного ввода информации (СРВИ).

Типовыми средствами ввода информации являются клавиатура и манипулятор типа «мышь». Соответственно, базовый ИПП включает призна-

ки работы пользователя с манипулятором типа «мышь» и признаки клавиатурного почерка.

В качестве признаков СК при работе с «мышью» могут использоваться следующие: форма траектории движений «мышью»; средняя скорость перемещения «мыши»; ускорение на начальном отрезке траектории; ускорение (замедление) на конечном отрезке траектории; точность размещения (позиционирования) указателя «мыши» на стандартных объектах графического интерфейса (пиктограммах, кнопках меню и т. д.). Исходными данными для формирования значений признаков СК при работе с «мышью» является множество пространственно-временных координат траекторий движения указателя «мыши», которые определяются с помощью драйвера «мыши» и таймера операционной системы.

Клавиатурный почерк пользователя может включать следующие признаки: время удержания клавиш; интервал времени между последовательными нажатиями двух и более клавиш; разность интервалов времени между набором символов в слове или команде и др. Исходными данными для формирования признаков клавиатурного почерка является множество пар моментов времени нажатия и отжатия используемых в процессе работы клавиш.

Решение об истинности пользователя при аутентификации по СК принимается на основе классической процедуры статистической проверки гипотез о равенстве эмпирических средних эталонных и текущих выборок значений признаков. На этапе обучения на основе обучающей выборки определяется оценка эмпирического среднего для каждого признака. Эта оценка является эталонным значением признака. В процессе работы пользователя по текущей выборке определяется текущее значение признака. Далее проверяется гипотеза об истинности пользователя, то есть о принадлежности текущего и эталонного значений признаков одному пользователю. Альтернативной является гипотеза о ложности пользователя, то есть о принадлежности эталонного и текущего значения разным пользователям. При проверке гипотезы возможны ошибки двух типов: вероятность ошибочного отказа и вероятность ошибочного доступа. В контексте задач защиты информации от несанкционированного доступа вероятность ошибочного доступа следует позиционировать в качестве основного показателя.

При АП по СК производится процедура проверки статистических гипотез для всех признаков почерка при работе с «мышью» и клавиатурного почерка. В случае несоответствия текущих признаков эталонным принимается решение о ложности почерка пользователя.

При выполнении пользователем стандартных работ (операций) на компьютере требуется некоторое время для получения выборок необходимого объема (для АП с требуемой точностью). Следовательно, в течение

времени формирования статистической выборки не обеспечивается непрерывность аутентификации. Для АП в условиях неполноты или неопределенности исходных данных (в том числе и при ограниченных выборках значений признаков) может использоваться подход, основанный на применении нечетких треугольных примитивов (НТП) [2], представляющих собой разновидность нечеткого числа [3]. Функция принадлежности НТП может быть уникальной для каждого признака СК. Значения элементов НТП для каждого признака сенсомоторного компонента определяются по выборкам ограниченного объема. Решение об истинности пользователя в условиях неопределенности исходных данных производится на основе проверки нечеткого равенства, эталонного и текущего НТП каждого признака.

Таким образом, для АП по СК статистический подход является основным, а для промежуточных этапов аутентификации и нештатных ситуаций может использоваться подход на основе НТП. В отличие от известных подходов предлагаемый способ постоянной аутентификации, основанный на совместном применении аппарата теории вероятностей, математической статистики и теории нечетких множеств, позволяет обеспечить непрерывность АП, по своей сути представляет собой новый интеллектуальный сервис защиты информации [4].

Психомоторный компонент (ПК) ИПП представляет собой совокупность формализованных признаков пользователя, характеризующих его индивидуальные особенности взаимодействия с программными средствами (ПС) и информационными ресурсами при выполнении работ (задач) на средствах автоматизации. В общем случае в ПК декомпозируется на операционный стиль работы пользователя и профиль типичных ошибок.

Операционный стиль работы пользователя отражает содержание и привычный порядок выполнения работы пользователем на средствах автоматизации. К признакам операционного стиля работы пользователя следует отнести следующие: множество программных средств и информационных ресурсов, используемых при выполнении работ (задач) на средствах автоматизации, перечень приемов (последовательностей элементарных действий с интерфейсом ПС) выполнения отдельных задач при работе с отдельным программным средством, с набором программных средств и др.

Профиль типичных ошибок пользователя отражает индивидуальные особенности памяти пользователя и таких психических процессов, как внимание и мышление. Профиль ошибок пользователя включает следующие признаки: множество типичных ошибок, совершаемых при выполнении операций с ПС (операционные ошибки); набор типичных ошибок, совершаемых при наборе команд и текста (наборные ошибки); приемы исправления ошибок и др.

Значения признаков ПК определяются на основе данных, получаемых от соответствующих компонентов операционной системы. Также могут использоваться дополнительные средства измерения. Например, для анализа наборных ошибок пользователя в некоторых приложениях может потребоваться программный модуль для анализа правописания. Правила аутентификации пользователей по ПК также основаны на совместном применении статистического подхода и подхода на основе НТП.

Эталонные значения признаков ИПП формируются в ходе процедуры обучения. Для ускорения процесса обучения могут использоваться специальные обучающие программы, предлагающие пользователю выполнить определенный набор задач и манипуляций, позволяющий за минимальное время получить эталонные значения признаков ИПП.

Алгоритмы и программные средства, реализующие способ АП по информационному почерку, должны учитывать возможные изменения состава программных средств и средств ввода информации (должна быть предусмотрена возможность оперативного автоматического изменения набора используемых признаков ИПП в зависимости от ситуации). Также алгоритмы аутентификации должны обеспечивать возможность корректировки эталонных значений признаков ИПП при изменении стиля работы пользователя на СРВИ и с ПС.

Таким образом, совместное применение традиционных методов аутентификации и ИПП позволит существенно повысить защищенность и обеспечить непрерывность аутентификации в АС. Также достоинством способа АП по информационному почерку является отсутствие необходимости использования дополнительных устройств, возможность реализации скрытого от пользователя контроля подлинности, низкая стоимость реализации.

Также следует отметить, что получаемые в ходе аутентификации по ИПП результаты измерения, обработки и анализа признаков действий пользователя на средствах автоматизации могут использоваться и для решения других задач защиты информации. В частности, в рамках контроля защищённости информации от несанкционированного доступа и компьютерных атак в автоматизированных системах [5] данные подсистемы аутентификации по ИПП могут использоваться для распознавания личности нарушителя, обнаружения известных атак, выявления аномальных действий пользователей, диагностирования инцидентов компьютерной безопасности.

Список используемых источников

1. Авраменко В. С., Купчиненко О. П., Пантюхин О. И. Адаптивное тестирование при автоматизации контроля знаний // Актуальные проблемы инфотелекоммуникаций в науке и образовании. V Международная научно-техническая и научно-методическая

конференция: сб. научных статей в 3 т.; Т. 2 / Под. ред. С. В. Бачевского. СПб.: СПбГУТ, 2016. С. 213–217.

2. Авраменко В. С. Бушуев С. Н. Распознавание пользователей на основе нечетких треугольных примитивов // Известия ВУЗов. Приборостроение. 1999. Т. 42. № 1. С. 13–19.

3. Кофман А., Алуха Х. Хил. Введение теории нечетких множеств в управлении предприятиями: пер. с исп. Минск: Вышэйшая школа, 1992. 224 с.

4. Котенко И. В., Саенко И. Б. Архитектура системы интеллектуальных сервисов защиты информации в критически важных инфраструктурах // Труды СПИИРАН. 2013. № 1 (24). С. 21–40.

5. Авраменко В. С. Адаптивный контроль защищенности информации от несанкционированного доступа на основе информационных образов // Проблемы информационной безопасности. Компьютерные системы. 2010. № 2. С. 45–49.

УДК 004.056.5

АНАЛИЗ ПРОБЛЕМЫ ОБНАРУЖЕНИЯ КОМПЬЮТЕРНЫХ АТАК, РЕАЛИЗУЕМЫХ С ИСПОЛЬЗОВАНИЕМ ЭКСПЛОЙТОВ

В. С. Авраменко, Д. И. Бобрешов-Шишов

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

Одной из острых проблем в современных инфокоммуникационных системах является проблема защиты от компьютерных атак, реализуемых с помощью эксплойтов. В статье представлен анализ типовых атак с использованием эксплойтов, предложен оригинальный подход к защите от подобных атак.

инфокоммуникационная система, угроза безопасности, эксплойт, уязвимость.

Под эксплойтом принято понимать компьютерную программу, фрагмент программного кода или последовательность команд, использующие уязвимости в программном обеспечении и применяемые для проведения атаки на вычислительную систему. Эксплойт после запуска повышает привилегии или загружает дополнительные вредоносные программы с сервера нарушителя.

В мире ежедневно создаются десятки эксплойтов. Такое же количество ежедневно устаревает. Такая тенденция обусловлена тем, что большинство эксплойтов ориентировано на уязвимости нулевого дня. По этой причине сигнатурные методы и методы эмуляции не используются в качестве основной защиты от эксплойтов.

В настоящее время использование одиночного эксплойта стало достаточно редким явлением. Большой популярностью у взломщиков сетей пользуются связки эксплойтов, так называемые эксплойт-пакеты (эксплойт-паки). Такие связки представляют собой набор эксплойтов, готовых к применению. В случае обнаружения соответствующей уязвимости один из эксплойтов «выдается» пользователю [1]. При этом вместе с эксплойт-пакетом должен находится плагин-детект, способный определить версию программного обеспечения (ПО) пользователя и подобрать рабочий эксплойт. Для выявления закономерностей в атаках, связанных с применением эксплойтов, был изучен эксплойт-пак, скрытый на веб-странице. Рассматриваемый пакет был «спрятан» в Flash-файл. Пользователь по ссылке попадает на страницу с упакованным Flash-объектом, который является эксплойт-паком в виде картинки. Такой подход позволяет взломщику скрыть наличие эксплойта от анализаторов трафика во время загрузки страницы.

Путь и имя загруженного файла похожи на адрес и имя стандартных библиотек Windows. Это позволяет, применив стандартную технику dll hijacking, не использовать функции run, start, open и т. д. и таким образом скрыть от антивируса запуск файла с расширением .dll. Эксплойт меняет переменную окружения sysdir и пытается подгрузить System.ShellApplication, инициируя запуск файла с расширением .dll.

В свою очередь, запущенная .dll загружает на компьютер жертвы и запускает скрипт “p.js”. Этот скрипт и является загрузчиком целевого вредоносного файла.

Следует отметить, что любой файл (в том числе и загружаемая с известных сайтов картинка) может хранить в зашифрованном виде набор эксплойтов. Кроме того, при настройке средств обнаружения атак необходимо учитывать, что наличие нескольких однотипных исполняемых файлов небольшого размера, в одном документе, так же может являться признаком эксплойта.

Эксплойты являются серьезной угрозой безопасности информации в компьютерных системах. Согласно статистическим отчетам лаборатории Касперского за 2015 г. 37 % компьютерных атак были реализованы с применением эксплойтов [2].

Согласно исследованиям, проведенным компанией PANDASEC [3], за 2014 г. в отношении «Банка Англии» было произведено 2340 атак с применением эксплойтов. Из них порядка 800 нанесли ущерб различного масштаба. Наиболее популярными способами внедрения эксплойта стали: зараженные флэш-носители, подменные Wi-Fi сети и фишинговые ссылки, распространяемые по электронной почте. Таким образом, можно сделать вывод, что более 30 % реализованных атак с применением эксплойтов наносят ущерб закрытой системе.

Анализ программного обеспечения, используемого в автоматизированных системах специального назначения (АССН), приводит к выводу, что данные системы также могут быть подвержены атакам с применением эксплойтов. Эксплойты могут распространяться с помощью съемных носителей информации, через систему электронной почты, электронного документооборота, сервера гипертекстовой обработки данных и геоинформационных систем.

Например, в 2016 г. на сайте Wikiliks [4] появилась информация об использовании ЦРУ не опубликованной уязвимости в протоколе Pluggable Authentication Modules (PAM). Следует отметить, что именно протокол PAM используется как основное средство аутентификации в операционная система (ОС) Linux с ядром Generic, к которым относится и ОС AstraLinux, используемая в силовых структурах, объектах энергетики, и в других критически важных информационных системах.

Для оценки возможности реализации атаки, связанной с применением эксплойта в отношении ОС с ядром Generic, было проведено следующее исследование: скомпилированный при помощи Metasploit эксплойт cve_2016_0728_exploit, размещенный в базе “git-hab” в 2016 г., был передан по протоколу ftp на ЭВМ, работающую под управлением ОС с ядром Generic. После чего данный эксплойт был помещен в каталог /tmp и оттуда был произведен его запуск. Эксплойт полностью отработал в ядре Generic, а порожденный им процесс просуществовал в течении 25 минут, после чего был уничтожен. Но можно предположить, что наиболее эффективные эксплойты, составляющие основу кибероружия иностранных разведок, не публикуются в открытом доступе.

Анализ атак показал, что эксплойт может быть спрятан в графическом файле, электронном письме и в других внешне безопасных объектах [5]. Эксплойт, внедренный в сеть передачи данных специального назначения, при условии применения унифицированного программного обеспечения способен в короткие сроки (несколько суток) компрометировать автоматизированные системы в глобальных масштабах. Очевидно, что подобное развитие ситуации может привести к значительному ущербу. Существующее положение обуславливает необходимость повышения эффективности существующих средств защиты от эксплойтов.

Одним из лидеров в этой области является продукт лаборатории Касперского Automatic Exploit Prevention (автоматическая защита от эксплойтов). Данный продукт предназначен для защиты от вредоносного ПО, использующего уязвимости в прикладных программах и операционной системе. В ее основе лежит анализ поведения существующих эксплойтов и сведения о приложениях, которые чаще других подвергаются атакам злоумышленников. За такими программами устанавливается особый контроль – как только одна из них пытается запустить подозрительный про-

граммный код, процедура прерывается и начинается проверка. Запуск исполняемого кода может быть вполне легитимным, например, программа может запросить обновление с сайта разработчика. Чтобы различить обычную деятельность и попытку заражения, новая технология «Лаборатории Касперского» использует информацию о наиболее типичном поведении известных эксплойтов. Характерное поведение таких вредоносных программ позволяет предотвратить заражение, даже если речь идет о неизвестном ранее эксплойте, либо при использовании уязвимости «нулевого дня». Довольно часто эксплойты перед непосредственным заражением системы осуществляют предварительную загрузку файлов. Модуль «Автоматическая защита от эксплойтов» отслеживает обращение программ к сети и анализирует источник файлов.

Технология может также различать файлы, созданные как при участии пользователя, так и новые, неавторизованные. Соответственно, попытка запустить файл, загруженный из подозрительного источника и без ведома пользователя, также будет заблокирована. Метод основан на технологии Address Space Layout Randomization (ASLR). Поддержка подобной технологии встроена в операционную систему Windows (начиная с Vista), и обеспечивает случайное расположение ключевых данных (например, системных библиотек) в адресном пространстве, что значительно усложняет использование некоторых уязвимостей. Технология «Лаборатории Касперского» предлагает пользователю функцию Forced Address Space Layout Randomization, которая выполняет те же операции и способна работать в тех случаях, когда аналогичная система в Windows бессильна. В частности, Forced ASLR может работать и в Windows XP.

Технология «Автоматическая защита от эксплойтов» доступна в новых версиях продукта Kaspersky Internet Security и Антивирус Касперского. Она по умолчанию блокирует запуск любого подозрительного кода, имеющего признаки использования уязвимости в ПО, причем новые методы практически исключают возможность ложного срабатывания.

В сочетании с другими инструментами, в частности – проверкой вебстраниц и писем на предмет вредоносного кода, «Автоматическая защита от эксплойтов» обеспечивает надежную комплексную защиту от компьютерных угроз, в том числе новых и ранее неизвестных [1].

Однако, несмотря на все достоинства описываемого продукта, его использование в целях защиты в некоторых автоматизированных системах, в том числе и специального назначения, не представляется возможным. В первую очередь это связанно с техническими требованиями к продукту. В описании [2] указано, что для работы требуется операционная система Windows, в то время как в инфокоммуникационных системах специального назначения используются и операционные системы семейства Unix.

Кроме того, все данные необходимые для работы системы, хранятся на серверах разработчика, доступ к ним осуществляется через Интернет. Такой подход в закрытых системах специального назначения.

Общий недостаток системы – отсутствие механизмов передачи информации администратору об уязвимости, ставшей причиной реализации эксплойта. Другими словами, несмотря на высокую эффективность выполнения задачи по блокированию эксплойта, данная программа не способна предупреждать дальнейшие атаки. Блокирование уязвимых приложений не производится, «дыры» не перекрываются.

Таким образом, проблема обнаружения компьютерных атак, реализуемых с использованием эксплойтов, является актуальной, в том числе и для инфокоммуникационных специального назначения.

Одним из путей решения данной проблемы является разработка технологии обнаружения уязвимостей на основе анализа процесса, порождённого запущенным нарушителем шелл-кодом. Такие процессы работают с переменными, адреса которых в оперативной памяти позволяют выявить файлы, возможно содержащие эксплойты. Для обнаружения процесса реализации атаки с использованием эксплойтов может использоваться подход на основе информационных образов [6, 7]. Для непосредственного обнаружения файлов с эксплойтами может использоваться технология анализа содержимого файла, предложенная в [8]. На заключительном этапе изучение обнаруженного эксплойта позволит идентифицировать использованные для атаки на инфокоммуникационную систему уязвимости.

Список использованных источников

1. Ежегодный статистический отчет Лаборатории Касперского за 2014 г. [Электронный ресурс]. URL: http://kaspersky-cyberstat.com/rus/st14/html (дата обращения 19.02.2017).

2. Ежегодный статистический отчет Лаборатории Касперского за 2016 г. [Электронный ресурс] URL: http://kaspersky-cyberstat.com/rus/st14/html (дата обращения 19.02.2017).

3. Результаты исследований компании PANDASEC [Электронный ресурс]. URL: http://www.pandasecurity.com/mediacenter/panda-security/edr-technology-much-more-than-just-standard-protection/ (дата обращения 19.02.2017).

4. Интернет ресурс «Wikiliks»[Электроный ресур]. URL: https://wikileaks.org (дата обращения 19.02.2017).

5. Милосердов А., Гриднев Д. Тестирование на проникновение с Kali linux [Электронный ресурс] URL: http://ed-lifehack.ru/wp-content/uploads/E%D1%88%D0%B0%D1%8F-%D0%BA%D0%BD%D0%B8% D0%B3% D0%B0Kali-Linux-.pdf 2012 (дата обращения 19.02.2017).

6. Авраменко В. С. Адаптивный контроль защищенности информации от несанкционированного доступа на основе информационных образов // Проблемы информационной безопасности. Компьютерные системы. 2010. № 2. С. 45–49.

7. Авраменко В. С. Адаптивный контроль защищенности информации от несанкционированного доступа // Информация и космос. 2010. № 3. С. 116–119.

8. Авраменко В. С., Баранов В. А., Бочков М. В. Метод контроля безопасности содержимого файлов // Телекоммуникации. 2004. № 11. С. 41–45.

УДК 528.7

ОПРЕДЕЛЕНИЕ КООРДИНАТ МОРСКИХ ОБЪЕКТОВ, ТЕРПЯЩИХ БЕДСТВИЕ, С ИСПОЛЬЗОВАНИЕМ БЕСПИЛОТНОГО ЛЕТАТЕЛЬНОГО АППАРАТА

С. Н. Агиевич[1], С. В. Дворников[1], В. В. Севидов[1], В. П. Эконом[2]

[1]Военная академия связи имени Маршала Советского союза С. М. Буденного
[2]Военный учебно-научный центр Военно-Морского Флота «Военно-морская академия им. Адмирала Флота Советского Союза Н. Г. Кузнецова»

Вопросы определения местоположения морских объектов, терпящих бедствие, имеют приоритетное значение для службы спасения, в связи с чем, все суда оборудуются навигационной аппаратурой. Между тем, нередко возникают ситуации, когда указанная аппаратура выходит из строя, поэтому решение задачи определения местоположения объектов в таких условиях имеет особое значение. В частности, предлагается методика определения координат терпящих бедствие судов с использованием беспилотных летательных аппаратов службы спасения.

морской объект, определение местоположения, беспилотный летательный аппарат, терпящие бедствие судно.

Указанная методика базируется на разностно-дальномерный способ (РДС) определения координат удаленного объекта [1], исходя из следующих соображений. Терпящее бедствие судно (ТБС) подает сигналы в службу спасения посредством спутниковой системы связи. Следовательно, если эти же сигналы ретранслировать посредством аппаратуры, установленной на беспилотных летательных аппаратах (БПЛА), то зная его координаты, по вычисленной разности прихода относительно сигналов спутника ретранслятора (СР) на входе аппаратуры контроля и радиомониторинга (КРМ) [2], открывается возможность вычисления координат источника сигналов.

На рис. 1 представлена геометрическая интерпретация реализации предлагаемого подхода.

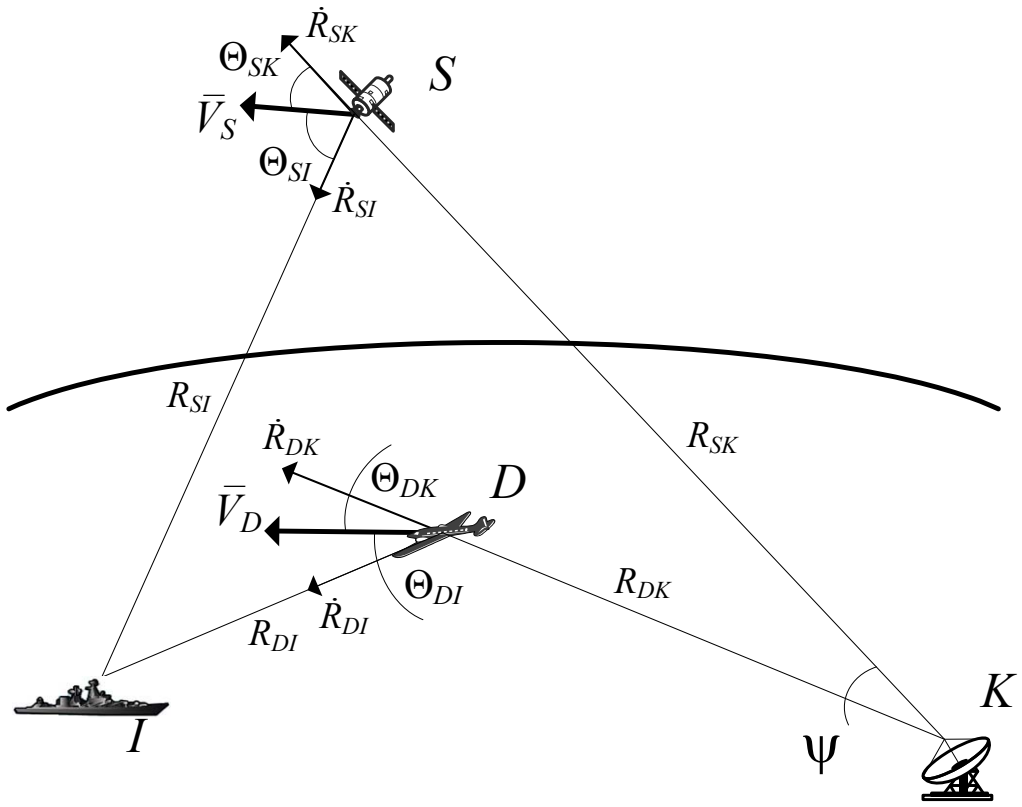


Рис. 1. Геометрическая основа определения координат ТБС с использованием БПЛА

Здесь: R_{SI} – расстояние от СР (на рис. 1 обозначен как *S*) до ТБС; R_{SK} – расстояние от СР до КРМ (на рис. 1 обозначен как *K*); R_{DI} – расстояние от БПЛА до ТБС (на рис. 1 обозначен как *I*); R_{DK} – расстояние от БПЛА до КРМ; $\bar{V}_S$ – вектор скорости СР в пространстве; $\bar{V}_D$ – вектор скорости БПЛА в пространстве; Θ_{SI} – угол между вектором $\bar{V}_S$ и осью *SI*; Θ_{SK} – угол между вектором $\bar{V}_S$ и осью *SK*; Θ_{DI} – угол между вектором $\bar{V}_D$ и осью *DI*; Θ_{DK} – угол между вектором $\bar{V}_D$ и осью *DK*; R_{SI} – радиальная скорость СР относительно ТБС (проекция вектора $\bar{V}_S$ на ось *SI*); R_{SK} – радиальная скорость СН относительно КРМ (проекция вектора $\bar{V}_S$ на ось *SK*); $\dot{R}_{DI}$ – радиальная скорость БПЛА относительно ТБС (проекция вектора $\bar{V}_D$ на ось *DI*); $\dot{R}_{DK}$ – радиальная скорость СР относительно КРМ (проекция вектора $\bar{V}_D$ на ось *DK*).

Радиоканалы ISK и IDK прохождения одной и той же реализации радиосигнала $S_I(t)$, излучаемого ТБС на средней частоте f_I в момент времени t_I будут различными. Следовательно, в КРМ будут приняты реализации сигнала $S_I(t)$: от СР – $S_{\text{ISK}}(t)$ на средней частоте f_{ISK} в момент времени t_{ISK}, от БПЛА – $S_{\text{IDK}}(t)$ на средней частоте f_{IDK} в момент времени t_{IDK}.

Схематически временные задержки и частотные сдвиги сигналов системы определения местоположения отображены на рис. 2. В КРМ нет информации о f_I и t_I, следовательно, в качестве координатно-информативных параметров могут выступать лишь разностные параметры, а именно временная задержка $t_{ЗД}$ и частотный сдвиг $f_{СД}$, которые могут быть определены на основе корреляционной обработки, при решении функции взаимной неоднозначности [3, 4]:

$$A(t_{ЗД}, f_{СД}) = \int_0^T S_{IDK}(t) S_{ISK}(t + t_{ЗД}) \exp(-2\pi f_{СД})\,\mathrm{d}t.$$

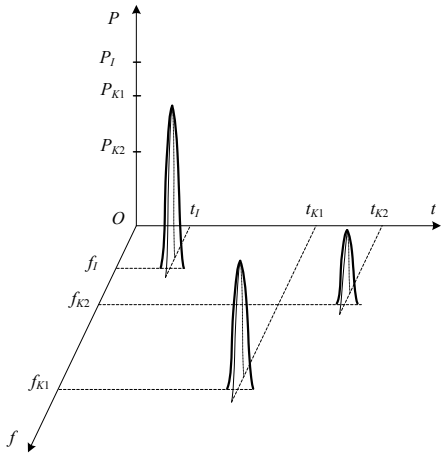


Рис. 2. Временные задержки и частотные сдвиги сигналов системы ОМП

В результате, неизвестные координаты ТБС x_I, y_I, z_I будут связаны между собой следующим уравнением [1]:

$$\begin{aligned}&\sqrt{(x_S - x_I)^2 + (y_S - y_I)^2 + (z_S - z_I)^2} - \\ &-\sqrt{(x_D - x_I)^2 + (y_D - y_I)^2 + (z_D - z_I)^2} = R_{SD};\end{aligned} \quad (1)$$

где $R_{SD} = ct'_{ЗД}$ – разность расстояний от СР и БПЛА до ТБС; $t'_{ЗД} = t_{ЗД} - \dfrac{R_{SK} - R_{DK}}{c} - t_S + t_D$ – временная задержка одной и той же реализации радиосигнала, принятого в СР и в БПЛА; t_S, t_D – временные задержки радиосигналов в СР и БЛА соответственно.

Задержки t_S и t_D могут быть определены с помощью тестовых сигналов, излученных КРМ и принятых им же от СР и БПЛА. В результате, известные координаты S, D и K позволяют рассчитать расстояния R_{SK} и R_{DK} в момент измерения временной задержки $t_{ЗД}$, используя выражения:

$$R_{SK} = \sqrt{(x_S - x_K)^2 + (y_S - y_K)^2 + (z_S - z_K)^2};$$

$$R_{DK} = \sqrt{(x_D - x_K)^2 + (y_D - y_K)^2 + (z_D - z_K)^2},$$

где x_K, y_K, z_K – координаты КРМ K; x_S, y_S, z_S –координаты СР S; x_D, y_D, z_D – координаты БПЛА D.

Частотный сдвиг $f_{СД}$ может быть выражен посредством частот f_{ISK} и f_{IDK}, представляющих реализации радиосигнала после прохождения им радиоканалов ISK и IDK, и принимаемых в КРМ следующим образом:

$$f_{СД} = f_{ISK} - f_{IDK}. \quad (2)$$

В свою очередь f_{ISK} и f_{IDK} равны:

$$f_{\text{ISK}} = f_I + f_{\text{Д}_{SI}} + f_S + f_{\text{Д}_{SK}}; \tag{3}$$

$$f_{\text{IDK}} = f_I + f_{\text{Д}_{DI}} + f_D + f_{\text{Д}_{DK}}, \tag{4}$$

где f_I – частота, излучаемая ТБС, $f_{ДSI}$ – составляющая доплеровского сдвига частоты за счет удаления (сближения) СР от (с) ТБС, $f_{ДSK}$ – составляющая доплеровского сдвига частоты за счет удаления (сближения) СР от (с) КРМ, $f_{ДDI}$ – составляющая доплеровского сдвига частоты за счет удаления (сближения) БПЛА от (с) СтСС, $f_{ДDK}$ – составляющая доплеровского сдвига частоты за счет удаления (сближения) БПЛА от (с) КРМ, f_S и f_D – частоты конвертирования (частоты «подставки») СР и БПЛА соответственно.

Частоты f_S и f_D определяют с помощью тестовых сигналов, излученных КРМ и принятых им же от СР и БПЛА.

Доплеровские сдвиги частот, фигурирующие в формулах (3) и (4) рассчитывают на основе следующих выражений:

$$f_{\text{Д}_{SI}} = f_I \frac{\dot{R}_{SI}}{c}, \qquad f_{\text{Д}_{SK}} = (f_I + f_{\text{Д}_{SI}} + f_S)\frac{\dot{R}_{SK}}{c}, \tag{5}$$

$$f_{\text{Д}_{DI}} = f_I \frac{\dot{R}_{DI}}{c}, \qquad f_{\text{Д}_{DK}} = (f_I + f_{\text{Д}_{DI}} + f_D)\frac{\dot{R}_{DK}}{c}. \tag{6}$$

Поскольку справедливы неравенства $f_I >> f_{\text{Д}_{SI}}$ и $f_I >> f_{\text{Д}_{SK}}$, то выражения (5) и (6) с учетом (3) и (4) преобразуют к следующему виду:

$$f_{\text{Д}_{SI}} = (f_{\text{ISK}} - f_S)\frac{\dot{R}_{SI}}{c}, \qquad f_{\text{Д}_{SK}} = f_{\text{ISK}}\frac{\dot{R}_{SK}}{c}, \tag{7}$$

$$f_{\text{Д}_{DI}} = (f_{\text{ISK}} - f_S)\frac{\dot{R}_{DI}}{c}, \qquad f_{\text{Д}_{DK}} = f_{\text{IDK}}\frac{\dot{R}_{DK}}{c}. \tag{8}$$

Радиальная скорость СР относительно ТБС равна:

$$\dot{R}_{SI} = |\bar{V}_S| \cos\Theta_{SI}. \tag{9}$$

Согласно теореме о скалярном произведении векторов [4], имеем:

$$\cos\Theta_{SI} = \frac{(x_I - x_S)\dot{x}_S + (y_I - y_S)\dot{y}_S + (z_I - z_S)\dot{z}_S}{\sqrt{(x_I - x_S)^2 + (y_I - y_S)^2 + (z_I - z_S)^2}\,|\bar{V}_I|}, \tag{10}$$

где $\dot{x}_S$, $\dot{y}_S$, $\dot{z}_S$ – компоненты вектора скорости СР $\bar{V}_S$.

Подставляя выражение (10) в (9), получают:

$$\dot{R}_{SI} = \frac{(x_I - x_S)\dot{x}_S + (y_I - y_S)\dot{y}_S + (z_I - z_S)\dot{z}_S}{\sqrt{(x_I - x_S)^2 + (y_I - y_S)^2 + (z_I - z_S)^2}}. \tag{11}$$

Также выводят аналитические выражения для расчета радиальных скоростей $\dot{R}_{SK}$, $\dot{R}_{DI}$ и $\dot{R}_{DK}$:

$$\dot{R}_{SK} = \frac{(x_K - x_S)\dot{x}_S + (y_K - y_S)\dot{y}_S + (z_K - z_S)\dot{z}_S}{\sqrt{(x_K - x_S)^2 + (y_K - y_S)^2 + (z_K - z_S)^2}}. \quad (12)$$

$$\dot{R}_{DI} = \frac{(x_I - x_D)\dot{x}_D + (y_I - y_D)\dot{y}_D + (z_I - z_D)\dot{z}_D}{\sqrt{(x_I - x_D)^2 + (y_I - y_D)^2 + (z_I - z_D)^2}}. \quad (13)$$

$$\dot{R}_{DK} = \frac{(x_K - x_D)\dot{x}_D + (y_K - y_D)\dot{y}_D + (z_K - z_D)\dot{z}_D}{\sqrt{(x_K - x_D)^2 + (y_K - y_D)^2 + (z_K - z_D)^2}}. \quad (14)$$

где $\dot{x}_D$, $\dot{y}_D$, $\dot{z}_D$ – компоненты вектора скорости БПЛА $\bar{V}_D$.

Возможно составление системы из трех уравнений с тремя неизвестными x_I, y_I, z_I (координаты ТБС):

$$\begin{cases} \sqrt{(x_S - x_I)^2 + (y_S - y_I)^2 + (z_S - z_I)^2} - \\ \sqrt{(x_D - x_I)^2 + (y_D - y_I)^2 + (z_D - z_I)^2} = R_{SD}; \\ \dfrac{(x_I - x_S)\dot{x}_S + (y_I - y_S)\dot{y}_S + (z_I - z_S)\dot{z}_S}{\sqrt{(x_I - x_S)^2 + (y_I - y_S)^2 + (z_I - z_S)^2}} - \\ - \dfrac{(x_I - x_D)\dot{x}_D + (y_I - y_D)\dot{y}_D + (z_I - z_D)\dot{z}_D}{\sqrt{(x_I - x_D)^2 + (y_I - y_D)^2 + (z_I - z_D)^2}} = V, \\ \sqrt{x_I^2 + y_I^2 + z_I^2} = R_З, \end{cases} \quad (15)$$

где $R_З$ – радиус Земли, $V = \dfrac{(f_{СД} - f_S - f_{Д_{SK}} + f_D + f_{Д_{DK}})c}{(f_{ISK} - f_S)}$.

Первое уравнение системы (15) это выражение (1), второе получают подстановкой (3) и (4) в (2) с учетом (7), (8), (11...14), третье составляют в предположении того, что ТБС расположена на поверхности Земли (на поверхности океана).

Решение системы уравнений (15) возможно численным методом Ньютона-Рафсона с помощью итерационного алгоритма [4].

В интересах оценки разработанной методики воспользуемся результатами [5], где обосновано выражение, характеризующее среднюю квадратическую ошибку (СКО) линии положения (ЛП) для РДС:

$$\sigma_{l_{рдс}} = \frac{\sigma_{\Delta R}}{2\sin(\psi/2)}, \quad (16)$$

где $\sigma_{\Delta R}$ – СКО измерения разности расстояний, в данном случае от ТБС до КРМ; ψ – угол обзора базы, под которым видны БПЛА и СР.

Анализ представленных результатов показывает, что предложенный подход физически реализуем. Причем точность значений ОМП зависит от точности измерения собственных координат СР, КРМ и БПЛА, а также угла обзора базы РДС, образованного СР и БПЛА. Так при $\psi = 180^\circ$ обеспечивается наименьшее значение СКО ЛП, равное половиной величине $\sigma_{\Delta R}$. Согласно результатам на рис. 3*б*, на практике не допустимо снижение $\psi < 60^\circ$. Дальнейшие исследования связаны с разработкой подхода ОМП с использованием двух и более БПЛА, а также внедрение в предложенный подход методов обнаружения сигналов, представленных в [6, 7, 8, 9, 10], для расширения зона контроля БПЛА.

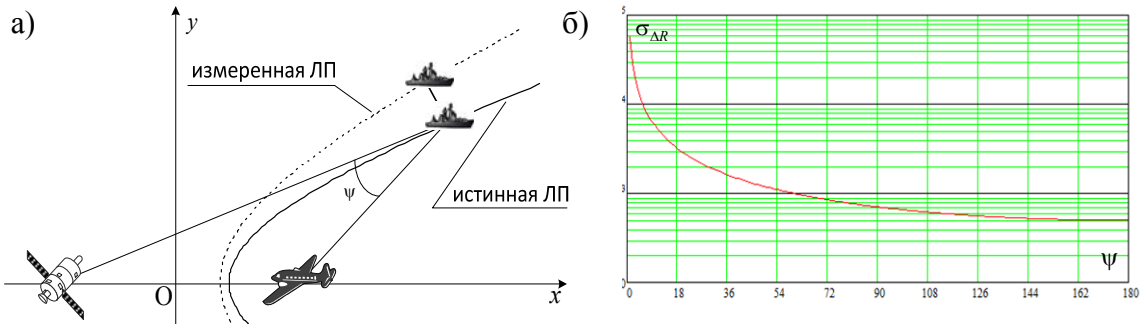


Рис. 3. Ошибка линии положения при РДС:
а) геометрическое представление, б) зависимость от величины угла обзора базы

Список используемых источников

1. Волков Р. В., Дворников С. В., Саяпин В. Н., Симонов А. Н. Основы построения и функционирования разностно-дальномерных систем координатометрии источников радиоизлучений. СПб.: ВАС, 2013. 116 с.

2. Дворников С. В. Проблема поиска сигналов источников информации при радиомониторинге // Мобильные системы. 2007. № 4. С. 33–35.

3. Дворников С. В., Яхеев А. Ф. Метод измерения параметров кратковременных сигналов на основе распределения Алексеева // Информация и космос. 2011. № 1. С. 66–74.

4. Корн Г., Корн Т. Справочник по математике для научных работников и инженеров. М.: Наука, 1984. 820 с.

5. Дворников С. В., Саяпин В. Н., Симонов А. Н. Теоретические основы координатометрии источников радиоизлучений: учебн. пособие. СПб.: ВАС, 2007. 80 с.

6. Дворников С. В. Метод обнаружения на основе посимвольного перемножения реализаций спектра наблюдаемого процесса с автоматическим расчетом порога принятия решения // Научное приборостроение. 2004. Т. 14. № 4. С. 92–97.

7. Дворников С. В. Метод обнаружения сигналов диапазона ВЧ на основе двухэтапного алгоритма принятия решения // Научное приборостроение. 2005. Т. 15. № 3. С. 114–119.

8. Дворников С. В., Сауков А. М. Модификация частотно-временных описаний нестационарных процессов на основе показательных и степенных функций // Научное приборостроение. 2004. Т. 14. № 3. С. 76–85.

9. Дворников С. В., Кудрявцев А. М. Теоретические основы частотно-временного анализа кратковременных сигналов : монография / С. В. Дворников, А. М. Кудрявцев; Воен. акад. связи. Санкт-Петербург, 2010. 239 с.

10. Дворников С. В., Алексеева Т. Е., Клепиков В. П., Шавула А. Б. Трехэтапный алгоритм принятия решения при обнаружении сигналов с различной динамикой амплитуд // Информация и космос. 2008. № 4. С. 14–17.

УДК 65.011.56

КЛИЕНТСКИЙ ОПЫТ В КОГНИТИВНОЙ МОДЕЛИ УПРАВЛЕНИЯ СЕТЬЮ ОПЕРАТОРА СВЯЗИ

В. А. Акишин

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

Клиентский опыт – понятие, включающее в себя совокупность впечатлений, которые клиент получает от взаимодействия с компанией-оператором связи. Однако, на сегодняшний день нет формальной модели, описывающей, как формируется клиентский опыт в специфике деятельности оператора связи, в частности, как на него влияют характеристики сети, качество предоставляемого сервиса, уровень развития OSS ландшафта и прочие аспекты телекоммуникационной среды. В работе рассматривается вариант функциональной модели, положенной в основу формирования когнитивной карты зависимости клиентского опыта от операционных процессов и сетевых характеристик оператора связи. Функциональная модель строится на основе рекомендаций TM Forum.

клиентский опыт, CEM, когнитивные карты, TM Forum.

Реалии современного рынка телекоммуникационных услуг заставляют компании работать в ситуации, когда большинство клиентов уже распределено по операторам связи, что, в свою очередь, увеличивает стоимость привлечения каждого нового клиента. В таком случае, реальным драйвером роста становится грамотная работа с существующими клиентами, в т. ч. персонализация взаимодействия, оптимизация регламентов общения с клиентом, анализ обратной связи о работе компании. Подобная ситуация заставляет операторов связи заниматься изучением и внедрением в процесс взаимодействия с клиентом концепции Customer Experience Management – управление клиентским опытом [1].

На текущий момент существует две явных проблемы на стыке концепции Customer Experience Management (CEM) и прикладной области телекоммуникаций. Во-первых, нет формальной модели, которая позволит

определить в количественном эквиваленте, как на клиентский опыт могут влиять невыполнение KPI в рамках операционных процессов, некачественный сервис и различные характеристики сети оператора связи. А во-вторых, само понятие «Клиентский опыт» является достаточно абстрактным, т. е. не формализованы факторы, влияющие на него.

Целью данного исследования является имплементация понятия клиентского опыта в различные аспекты управления сетью оператора связи: в частности, создание функциональной модели, описывающей формальную корреляцию клиентского опыта и факторов, характеризующих эксплуатационную деятельность оператора связи и количественные показатели сети. Развитием данной функциональной модели будет создание когнитивной карты, дающей количественную оценку взаимосвязям между управляющими и целевым фактором модели. Создание подобной когнитивной карты предоставляет возможность разработать научно обоснованные рекомендации управляющим звеньям оператора связи, которые позволят формировать клиенто-ориентированную стратегию развития оператора связи и решать прикладные вопросы при ежедневном взаимодействии с клиентом [2].

Процесс разработки когнитивной модели проблемы состоит из последовательности взаимосвязанных шагов: выделение предметной области, проведения SWOT и PEST анализа предметной области, выделение наиболее важных факторов, оказывающие различные по степени, характеру и периодичности влияния на исследуемую область. В результате анализа формируется проблемное поле в виде совокупности базисных факторов [3]. Когнитивное отображение проблемного поля осуществляется в виде когнитивной карты – взвешенного ориентированного графа:

$$G = <V, E>,$$

где V – множество вершин; $Vi \in V$, $i = 1, 2, \ldots, k$; E – множество дуг.

Дуга $eij \in E$, $i, j = 1, 2, \ldots, n$ соединяет вершины графа, которые соответствуют базисным факторам проблемного поля, наиболее значимым для управления проблемой. Влияние факторов может быть положительным, отрицательным или нулевым:

Исходя из обозначенной задачи, в рамках данной предложена функциональная модель для когнитивной карты управления клиентским опытом в сфере телекоммуникаций. Для данного исследования, в качестве управляющих факторов когнитивной модели были выбраны метрики TM Forum, стандартизированные данной организацией в 2015 году и характеризующие клиентский опыт на этапе жизненного цикла Manage [4].

Данные метрики были выбраны исходя из проведенных автором исследований наличия данных показателей в OSS/BSS комплексах нескольких отечественных операторов связи.

Выбранные метрики представлены ниже (оригинальное описание):

– Seconds Manage Profile Service (M-C-2a);
– First Contact Resolutions (M-C-5);
– Incidents Resolved (M-C-6a);
– Incidents Due Closure (M-C-6c);
– Minutes to Resolve Incident (M-C-9a);
– Unresolved Incidents – Smelly Fish (M-C-11);
– Repeat Contacts (M-C-12);
– Maintenance Notifications Violated (M-E-10);
– Customer Subjective Score – General Support (M-E-11);
– Support Hotline Subjective Score – Manage Service/Profile (M-F-3);
– Online Channel Subjective Score – Receive Help (M-F-8);
– % Service Configurations Failed (M-F-23);
– Minutes per Service Configuration (M-F-24) [4].

Далее необходимо оценить, как управляющие факторы коррелируются между собой и как влияют на целевой фактор. Как уже было отмечено в постановке задачи, влияние факторов может быть положительный, отрицательным и нулевым: положительное влияние (+)-данное значение характеризует наличие влияния фактора А на фактор Б, при условии, что изменение в большую сторону значения фактора А влечет за собой изменение в большую строну значения фактора Б, и наоборот, изменение в меньшую сторону значения фактора А влечет за собой изменение в меньшую сторону значение фактора Б; отрицательное влияние (–)-данное значение отражает влияние фактора А на фактор Б, при условии, что изменение в большую сторону значения фактора А повлечет за собой изменение в меньшую сторону фактора Б, и наоборот, изменение в меньшую сторону фактора А повлечет за собой увеличение значения фактора Б; нулевое влияние (0)-данное значение отражает отсутствие взаимовлияния (отношения причинности) фактора А на фактор Б.

Для наглядности связь факторов можно рассмотреть в виде матрицы взаимовлияния. В таблице представлена матрица взаимовлияния управляющих факторов этапа Manage жизненного цикла клиента.

Далее управляющие и целевые факторы, а также их корреляцию можно представить в виде когнитивной карты моделируемой области (рис.). На когнитивной карты визуализировано влияние управляющих факторов друг на друга, влияние управляющих факторов на значение показателя клиентского опыта в рамках этапа Manage, а также влияние на целевой фактор – композитный показатель клиентского опыта (*M*).

ТАБЛИЦА. Матрица взаимовлияния факторов когнитивной модели

Факторы	M-C-2a	M-C-5	M-C-6a	M-C-6c	M-C-9a	M-C-11	M-C-12	M-E-10	M-E-11	M-F-3	M-F-8	M-F-23	M-F-24	Целевой
M-C-2a		–	0	0	0	0	0	0	0	–	–	+	+	–
M-C-5	0		0	0	0	0	–	0	+	+	0	0	0	+
M-C-6a	0	+		0	0	–	–	0	+	+	+	0	0	+
M-C-6c	0	0	+		–	–	–	0	+	+	+	0	0	+
M-C-9a	0	0	0	–		+	+	0	–	–	0	0	0	–
M-C-11	0	–	–	–	+		+	+	–	–	–	+	0	–
M-C-12	0	+	0	0	0	0		0	–	–	–	0	0	–
M-E-10	0	0	0	0	0	0	+		–	–	–	0	0	–
M-E-11	0	+	0	0	0	0	0	0		0	0	0	0	+
M-F-3	0	+	0	0	0	0	0	0	+		0	0	0	+
M-F-8	0	0	0	0	0	0	0	0	+	+		0	0	+
M-F-23	+	–	0	0	0	0	0	0	–	–	–		0	–
M-F-24	+	–	0	0	0	0	0	0	–	–	–	+		–

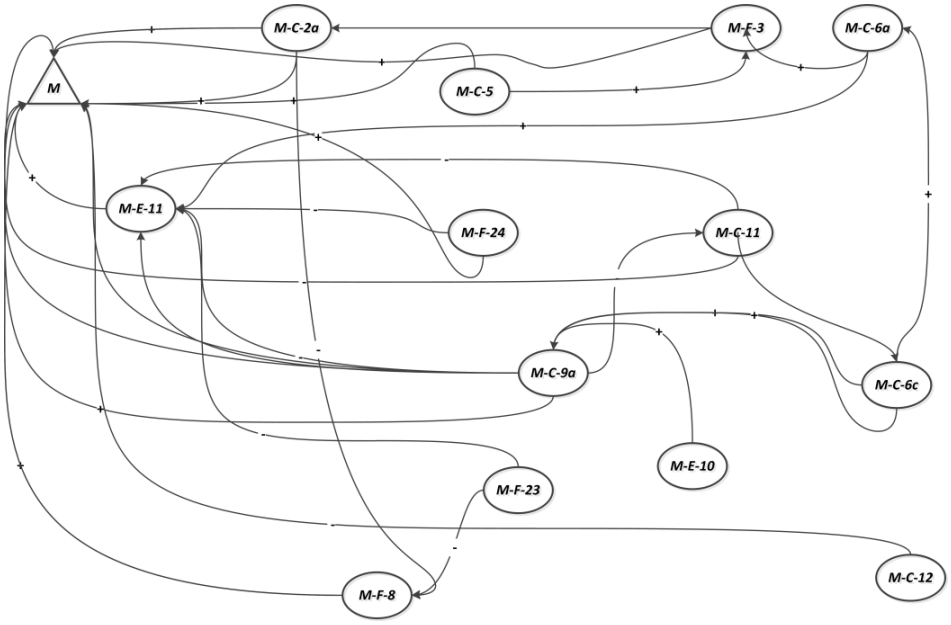


Рисунок. Функциональная карта моделируемой области

В рамках исследования описана формальная функциональная модель для когнитивной карты зависимости клиентского опыты от факторов эксплуатационных процессов оператора связи и различных характеристик сети. В качестве основных тезисов исследования были приняты утверждения о том, что клиентский опыт – это многомерный композитный параметр, формирующийся на различных этапах жизненного цикла клиента. В качестве управляющих факторов предложенной модели был использованы метрики – рекомендации TM Forum.

Развитием данной модели, автор видит два основных направления:

– интенсивное развитие, а именно статистическая оценка корреляции целевых и управляющих факторов модели, что позволит делать количественные заключения об изменении целевого фактора при подаче определенного возмущения на управляющие;

– экспансивным развитие, т. е. дальнейшая функциональная декомпозиция модели. В частности анализ клиентского опыта в рамках определенной сервисной платформы, технологии предоставления сервиса, сегмента клиентов, а также анализ клиентского опыта в проекции на различные каналы общения с клиентом.

Список используемых источников

1. Ланкевич К., Хабаев Н., Скоринов М. OSS комплекс как инструмент контроля лояльности пользователей оператора связи // T-Comm: Телекоммуникации и Транспорт. 2016. Т. 10. № 5. С. 36–40.

2. Пожарский Н. А., Лихачев Д. А., Кисляков С. В. Использование когнитивных карт и нечёткой логики в разработке OSS/BSS решений для операторов связи // T-Comm: телекоммуникации и транспорт. 2016. Т. 11. № 11. 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. DOI : 10.17150/1993-3541.2015.25(6).1014-1024.

4. TM FORUM. GB962A_Lifecycle_Metrics_R15.0.1. TM Forum; December 2015.

Статья представлена научным руководителем, кандидатом технических наук, доцентом С. В. Кисляковым.

УДК 004.056

РАЗРАБОТКА МОДЕЛИ НАРУШИТЕЛЯ В БЕСПРОВОДНЫХ СЕТЯХ СТАНДАРТА IEEE 802.11

Е. С. Александрова, М. М. Ковцур

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

Беспроводные сети нашли широкое применение как в современных корпоративных сетях, так и в сетях, предназначенных для персонального пользования. Беспроводные интерфейсы семейства стандартов IEEE 802.11 имеют большую популярность и устанавливаются в мобильных терминалах пользователей, портативных и стационарных компьютерах, медиаустройствах. В докладе рассматриваются основные угрозы, характерные для беспроводных сетей, а также возможные атаки на беспровод-

ные сети семейства стандартов IEEE 802.11 и комбинации атак, которые может реализовать активный нарушитель с учетом текущего уровня развития технических средств и доступного программного обеспечения. На основании возможных атак разрабатывается модель нарушителя в беспроводных сетях.

Wi-Fi, беспроводные сети, модель нарушителя, IEEE 802.11.

Обеспечение информационной безопасности играет важную роль, как при развертывании беспроводной сети, так и при ее эксплуатации. Важными факторами, которые необходимо учитывать при защите от атак сетей современных беспроводных стандартов, являются большая зона покрытия и высокая пропускная способность, что позволяет реализовать атаку, находясь в пределах радиодоступности сети.

Рост популярности рассматриваемых беспроводных сетей обусловлен положительной динамикой продаж беспроводных устройств (рис. 1) [1].

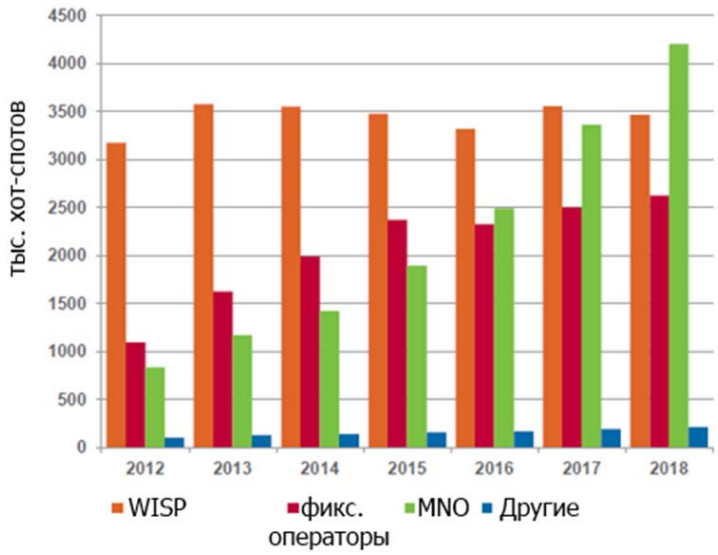


Рис. 1. Число точек доступа homespot-сетей в мире, тыс. шт.

Целью работы является построение актуальной модели нарушителя в беспроводных сетях. Основные задачи:

– обзор существующих атак в беспроводных сетях стандарта IEEE 802.11;

– разработка алгоритма возможных действий нарушителя при реализации атаки на беспроводные сети;

– обзор существующих методов защиты.

Данная модель отличается от существующих [2, 3, 4], представленных в таблице 1, наличием алгоритма возможных действий нарушителя, а также более широким охватом существующих атак, таких как DoS, взлом WPS PIN.

ТАБЛИЦА 1. Существующие модели нарушителя

Автор	Название	Недостатки
Белов Э. В.	Обзор безопасности беспроводных сетей семейства 802.11	Не упоминаются некоторые атаки, например, взлом WPS PIN, MITM
Бадамшин М. Р.	Проблемы безопасности беспроводных сетей	Не учитываются DoS атаки
Mohammed Farik	Recurrent Security Gaps in 802.11ac Routers	Не приведен алгоритм действий нарушителя

Модель может быть использована при оценке безопасности при проектировании защищенных беспроводных сетей, а также для анализа существующих решений.

Для получения несанкционированного доступа нарушитель может реализовать следующие атаки:

– Атака на контроль доступа (*War Driving, Rogue Access Point, MAC Spoofing, 802.1X RADIUS Cracking*);

– Нарушение целостности (*802.11 Frame Injection, 802.11 Data Replay, 802.1X EAP Replay, 802.1X RADIUS Replay*);

– Нарушение конфиденциальности (*Eavesdropping, WEP Key Cracking, Evil Twin AP, AP Phishing*);

– Нарушение доступности (*Queensland DoS, 802.11 Beacon Flood, 802.11 Associate/ Authenticate Flood, 802.11 TKIP MIC Exploit*);

– Похищение данных аутентификации (*Shared Key Guessing, 802.1X Identity Theft, 802.1X EAP Downgrade, взлом WPS PIN*) [5, 6].

Алгоритм возможных действий нарушителя представлен на рис. 2. Для достижения цели нарушителю необходимо реализовать совокупность атак.

1. Нарушитель может провести сетевую разведку – обнаружить беспроводную сеть, найти ее уязвимости путем отправки фреймов probe request, либо прослушивая beacon фреймы, тем самым создавая точку отправления для последующих атак.

2. Перехват конфиденциальной информации, передающейся по беспроводному каналу связи.

3. Rogue Access Point – установка нелегитимной точки доступа внутри атакуемой сети.

4. Восстановление RADIUS secret путём отправки запроса на подключение, для дальнейшего создания Evil Twin.

5. Атаки, нацеленные на нарушение доступности, препятствующие получению беспроводного доступа легитимным пользователям путём отказа к доступу к оборудованию.

7. Изменение MAC адреса нарушителя с целью обойти список контроля доступа к сети или с целью реализации Man In The Middle.

8. Отправка ложного ARP-ответа, предварительно перехватив ARP-запрос, объявляя себя искомым узлом.

9. Evil Twin – организация нелегитимной точки доступа с таким же SSID, что и у легитимной точки доступа, к которой подключаются пользователи.

10. Man In The Middle – использование классических средств для атаки MITM на ложной точке доступа с целью перехвата и изменения пользовательского трафика.

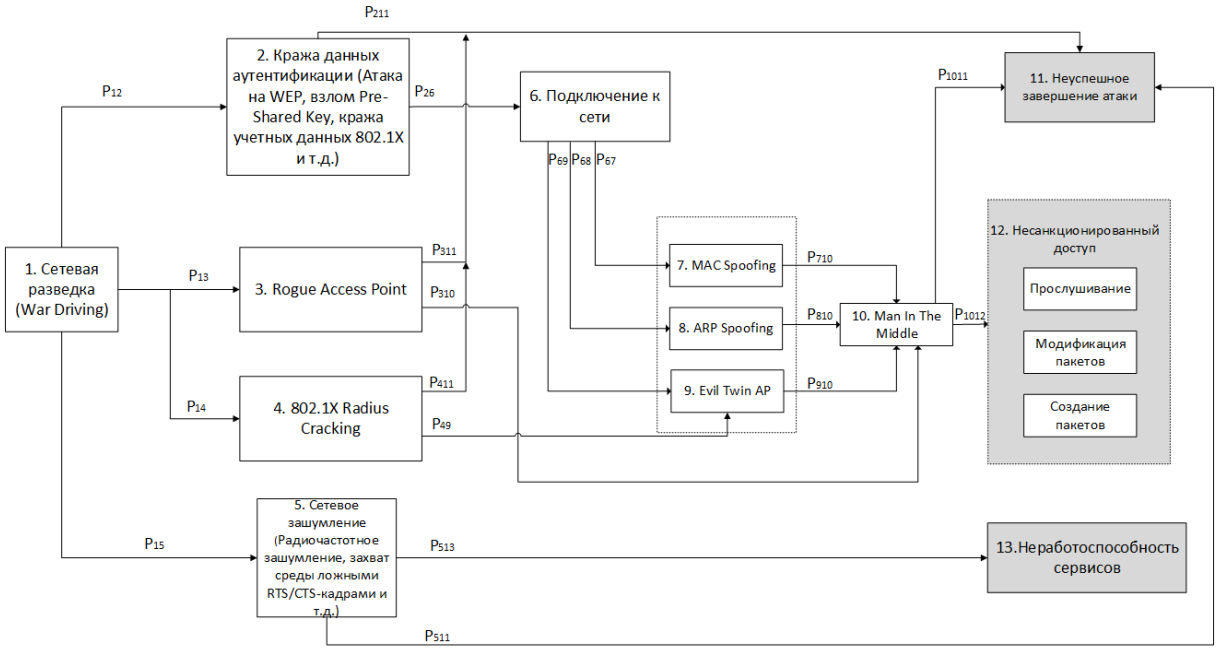


Рис. 2. Алгоритм возможных действий нарушителя

В случае успешной реализации атак нарушитель может просматривать, изменять, удалять и создавать сетевые пакеты, проходящие через атакуемую беспроводную сеть, либо влиять на работоспособность атакованной сети [7]. На исход атаки в большей степени влияет оборудование доступа к сети. Можно существенно повысить безопасность сети за счет внедрения дополнительных средств защиты, в том числе:

1. WIPS (Wireless Intrusion Prevention System) – предотвращают целый спектр атак, таких как «злой двойник», Man In The Middle, MAC Spoofing, DoS, Eavesdropping [8], ложная точка доступа [9].

2. DHCP Snooping, Option 82, Access Control List – функционал, позволяющий разделить трафик пользователей, подключенных к различным точкам доступа.

3. Изоляция беспроводных клиентов (Wireless Isolation) – функция, изолирующая друг от друга устройства, подключенные к сети. Предотвращает спуфинг.

4. Cisco Clean Air – технология, выявляющая радиопомехи и их источник, защищает от атак, направленных на сетевое зашумление.

Уровень безопасности сети во многом определяется оборудованием доступа и грамотностью его настройки. Одной из наиболее опасных атак является атака на сетевое зашумление, т. к. определение источника атаки требует значительных ресурсов и реализована лишь у нескольких вендоров.

Список используемых источников

1. Рынок публичных сетей Wi-Fi в Республике Беларусь и в сопредельных государствах. URL: http://json.tv/ict_telecom_analytics_view/rynok-publichnyh-setey-wi-fi-v-respublike-belarus-i-v-sopredelnyh-gosudarstvah-20141110114322 (дата обращения 15.02.2017).

2. Бадамшин М. Р. Проблемы безопасности беспроводных сетей // Международная молодежная научная конференция «XXII Туполевские чтения (школа молодых ученых)». Материалы конференции сборник докладов. Российский фонд фундаментальных исследований, Казанский национальный исследовательский технический университет им. А. Н. Туполева-КАИ (КНИТУ-КАИ). 2015. С. 178–182.

3. Белов Э. В. Обзор безопасности беспроводных сетей семейства 802.11 // Научно-технический вестник информационных технологий, механики и оптики. 2006. N 29. С. 205–208.

4. Mohammed Farik and ABM Shawkat Ali 2015. Recurrent Security Gaps In 802.11ac Routers. URL: http://www.ijstr.org/final-print/sep2015/Recurrent-Security-Gaps-In-80211ac-Routers.pdf (дата обращения 01.02.2017).

5. Ковалев Д., Ковцур М. Механизмы аутентификации и управления ключами стандарта IEEE 802.11 // Первая миля. 2014. № 3 (42). С. 72–77.

6. Меркулов А. Б., Никитин В. Н., Юркин Д. В. Криптографические протоколы безопасности сетей широкополосного радиодоступа стандартов IEEE 802.1x // Защита информации. Инсайд. 2009. № 5 (29). С. 38–45.

7. Емельянов А. А., Меркушев О. В. Передача данных в беспроводных сетях IEEE 802.11: угрозы безопасности и методы защиты // Приборостроение в XXI веке – 2015. Интеграция науки, образования и производства. Сборник материалов XI Международной научно-технической конференции. 2016. С. 411–419.

8. Чечулин А. А., Котенко И. В. Комбинирование механизмов защиты от сканирования в компьютерных сетях // Информационно-управляющие системы. 2010. № 6. С. 21–27.

9. Юркин Д. В., Никитин В. Н. Системы обнаружения вторжения в сетях широкополосного радиодоступа стандарта IEEE 802.11 // Информационно-управляющие системы. 2014. № 2 (69). С. 44–49.

УДК 004.732

ТЕСТИРОВАНИЕ SDN ПОДХОДОВ ДЛЯ СЕТЕЙ WLAN НА БАЗЕ МОДЕЛЬНОЙ СЕТИ

А. В. Амелянович, А. С. Мутханна

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

В данной статье представлены методы тестирования программно-конфигурируемой беспроводной локальной сети на базе модельной сети Санкт-Петербургского государственного университета телекоммуникаций им. М. А. Бонч-Бруевича. В ходе практического эксперимента рассматривается взаимодействие точек доступа с контроллером SDN. При использовании контроллера OpenDaylight, топологию сети можно контролировать через пользовательский графический интерфейс SDN. В результате была измерена производительность точки доступа в тестовой среде беспроводной локальной сети.

контроллер SDN, точка доступа (AP), беспроводная локальная сеть.

Введение

В последнее время развитие беспроводных локальных сетей (WLAN) резко возросло в связи с ростом спроса на беспроводной доступ. Для того чтобы гарантировать пользователям WLAN всегда лучшее качество обслуживания (QoS), современные системы WLAN всегда состоят из сотен точек доступа (AP), контроллеров беспроводной локальной сети, системы управления и различных услуг в масштабируемой сети. Эти услуги включают в себя контроль доступа, управление мобильностью, балансировка нагрузки, динамической реконфигурации канала и так далее. Есть много WLAN решений, предлагаемых различными производителями. Но большинство этих решений с закрытым исходным кодом и дорогим оборудованием, что ограничивает гибкость и расширяемость сети. Предлагается новый подход к построению WLAN сетей – SDWN (*Software defined Wireless Access Network*), открытая платформа WLAN [1], на основе подхода Software Defined Networking (SDN) [2], заключающегося в разделении плоскости данных и плоскости управления. Архитектура SDWN содержит логический централизованный контроллер, множество точек доступа, агентов, работающих на верхнем уровне точек доступа, а также набор приложений SDWN. Контроллер имеет глобальный обзор всей сети (общую топологию), и позволяет производить связь операций с помощью API. Приложения, работающие на верхнем уровне SDWN -контроллера используют API для реализации разновидности сетевого управления. Пользова-

тельский протокол, называемый протоколом SDWN, используется контроллером для вызова команд к агентам точек и сбор статистических данных из них.

На рис. 1 представлены частные случаи построения сети SDN в плотных WLAN сетях: напрямую и через маршрутизаторы. В первом подходе каждая точка доступа должна поддерживать OpenFlow протокол [3, 4], что позволяет управлять точками доступа и потоками трафика. При построении через маршрутизаторы поддержка протокола точками доступа не обязательна, но остается возможность управления трафиком.

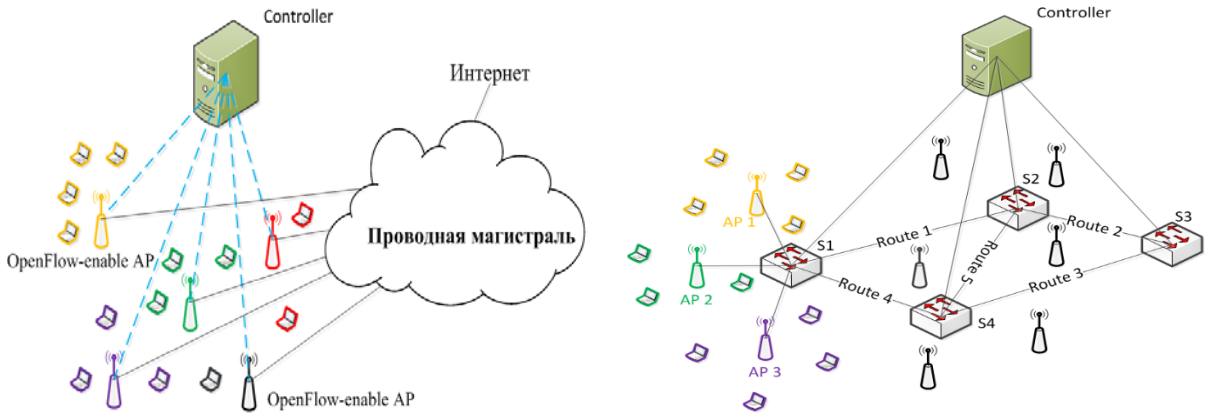


Рис. 1. Возможные реализации SDN в плотных WLAN сетях

Структурная схема натурного эксперимента

На рис. 2 представлена топология беспроводной локальной сети на базе SDN котроллера. В качестве точек доступа(AP) использовались Raspberry Pi 3 Model B на OpenWRT [5] платформе.

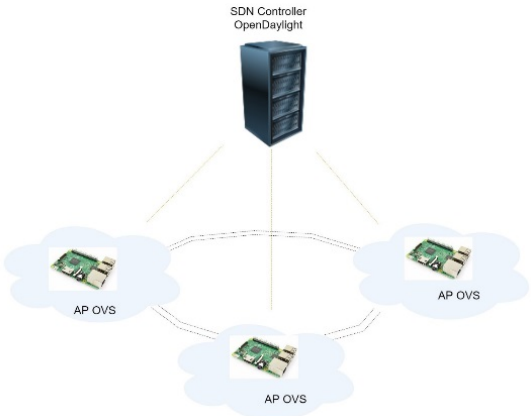


Рис. 2. Схема сети

Топология ключает:

– аппаратная платформа Raspberry Pi;
– контроллер SDN;

– WiFi адаптеры.

Используемое программное обеспечение:

– SDN платформа OpenDaylight;
– Платформа OpenWRT.

Результаты исследования

В таблице представлены результаты исследования задержек и потерь пакетов.

Как видно из таблицы, задержки при передаче пакетов позволяли бы воспроизводить потоковое видео при подключении к любой из точек доступа. Однако потери у третьей точки доступа превышают рекомендуемые [5]. Это обуславливается тем, что AP3 не имеет прямого соединения со шлюзом.

ТАБЛИЦА. Результаты исследования

Параметры	Задержка (ms)	Потеря пакетов (%)
AP1	51,96	0,25
AP2	70,04	1,25
AP3	84,65	9,50

Заключение

В ходе исследования был разработан стенд для управления потоками трафика в беспроводной локальной сети на основе SDN контроллера. Данное решение позволило уменьшить количество одновременно работающих беспроводных устройств, а также повысился приоритет трафика чувствительных к задержкам приложений в сравнении с остальными.

Благодаря данному подходу становится легко применять новые политики QoS, а также динамично их обеспечивать через программные приложения.

Список используемых источников

1. Honglin Hu, Hsiao-Hwa Chen, Peter Mueller, “Software defined wireless networks (SDWN)”, IEEE Communications Magazine, Nov. 2015. Vol. 53. No. 11. pp. 108–109.

2. Vladyko A., Muthanna A., Kirichek R. Comprehensive SDN testing based on model network // Lecture notes in computer science. 2016. pp. 539–549.

3. Yong LI and Min Chen,” Software-Defined Network Function Virtualization: A Survey,” IEEE Access, Dec. 2015. Vol. 3. pp. 2542–2553.

4. Sakir, Sezer, et al,” Are we ready for SDN? Implementation challenges for software-defined networks,” IEEE Communications Magazine. July 2013. Vol. 51. No. 7. pp. 36–43.

5. Palazzi C. E., Brunati M., and Roccetti M. ”An OpenWRT solution for future wireless homes,” IEEE Multimedia and Expo (ICME). July 2010. pp. 1701–1706.

6. G.1010 : End-user multimedia QoS categoriesб, ITU-T. Nov 2001. pp. 14.

УДК 621.391.63; 681.7.068

МЕТОД РАСЧЕТА ПАРАМЕТРОВ СХЕМЫ ПРЕЦИЗИОННОГО ПРОСТРАНСТВЕННОГО ПОЗИЦИОНИРОВАНИЯ КАНАЛОВ СИСТЕМЫ MDM НА ТОРЦЕ СЕРДЦЕВИНЫ ВОЛОКОННОГО СВЕТОВОДА ЛИНИИ ПЕРЕДАЧИ

В. А. Андреев, А. В. Бурдин, В. А. Бурдин

Поволжский государственный университет телекоммуникаций и информатики

В работе предложен метод расчета параметров схемы пространственного прецизионного позиционирования каналов мультиплексора, реализующего технологию модового уплотнения, на торце возбуждаемого маломодового оптического волокна линии передачи. Представлены результаты расчета параметров ввода 5 мод системы MDM в торец маломодового оптического волокна с диаметром сердцевины 42 мкм и уменьшенной дифференциальной модовой задержкой. Показано, что при соответствующем сочетании значений радиуса пятна моды канала MDM и радиального рассогласования на вводе удается добиться передачи практически всей мощности вводимой моды MDM отдельной направляемой моде оптического волокна этого же азимутального порядка.

модовое мультиплексирование, маломодовые оптические волокна, маломодовый режим передачи оптического сигнала, пространственное позиционирование поля моды, дифференциальная модовая задержка, прецизионное радиальное рассогласование, диаметр пятна моды, коэффициенты связи мод

На сегодняшний день нелинейный предел Шеннона является ключевым фактором, ограничивающим реализацию сверхвысокоскоростных транспортных сетей связи нового поколения, ориентированных на передачу данных со скоростью сотни Тбит/с и более [1]. Очевидным способом подавления нелинейных эффектов в оптическом тракте является уменьшение нелинейности самого волоконного световода непосредственно за счет существенного увеличения площади эффективного сечения оптического волокна (ОВ). Неслучайно переход на маломодовые световоды (FMF – *Few Mode Fibers*) с экстремально увеличенным, по сравнению с традиционными телекоммуникационными коммерческими одномодовыми и маломодовыми ОВ, диаметром сердцевины, обеспечивающим практически полное устранение нелинейности ОВ, в сочетании с технологией модового мультиплексирования (MDM – *Mode Division Multiplexing*) и MIMO (*Multiple Input Multiple Output* – множественные входы/множественные выходы),

считается в настоящее время одним из перспективных подходов для решения данной задачи [1, 2, 3].

Очевидно, что существенное увеличение диаметра сердцевины FMF, необходимое для практически полного устранения нелинейности ОВ, неизбежно приводит к появлению еще большего числа новых модовых составляющих высших порядков, удовлетворяющих условию отсечки рассматриваемого световода. Это требует проведения дополнительных мероприятий по уменьшению дифференциальной модовой задержкой (ДМЗ), которая, в общем случае, является основным негативным линейным фактором искажения оптического сигнала при распространении по ОВ в маломодовом режиме [4]. И в этом смысле при разработке конструкций FMF ключевой проблемой является поиск компромисса между эффективной площадью сечения ОВ, непосредственно связанной с диаметром сердцевины, который, в том числе, определяет модовый состав волоконного световода, и минимизацией ДМЗ на заданной оптической несущей или в определенном выделенном диапазоне длин волн [2, 3].

Известны работы [5, 6], в которых было экспериментально продемонстрировано, что если изначально подобрать условия ввода сигнала с выхода лазера в торец волокна таким образом, чтобы практически вся мощность поступаемого излучения передавалась непосредственно одной определенной моде заданного порядка, то и амплитуды новых компонентов, возбуждаемых в процессе распространения по ОВ, обусловленных его нерегулярной структурой, а также наличием микро-/макро изгибов и механических напряжений, будут пренебрежимо малы, по сравнению с ней. Таким образом, можно предположить, что использование данного подхода для «размещения» каналов системы MDM с выхода мультиплексора на торце FMF линии с некоторым заданным пространственным смещением относительно центра сердцевины ОВ при одновременном согласовании радиусов пятна мод (MFR – *Mode Field Radius*) искомых порядков, позволит реализовать селективное возбуждение заданных направляемых мод, характеризующихся минимальным разбросом задержки из всего модового состава данного ОВ и, тем самым, исключить сильное проявление ДМЗ.

Для проверки данной гипотезы на первом этапе был разработан метод расчета параметров схемы пространственного прецизионного позиционирования каналов мультиплексора MDM на торце возбуждаемого ОВ. Предлагаемое решение базируется на сочетании известного метода интеграла перекрытия полей (ИПП) [7] и ранее разработанной модификации приближения Гаусса, обобщенной на случай расчета параметров передачи направляемых мод произвольного порядка, распространяющихся в слабонаправляющем ОВ с произвольным осесимметричным профилем показателя преломления (ОМПГ) [8]. ОМПГ базируется на совместном применении модификации приближения Гаусса [7] и методе стратификации [9],

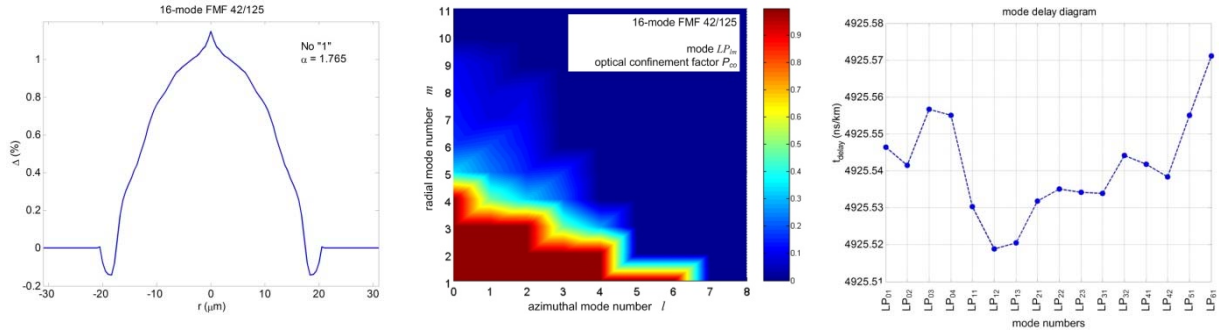
характеризуется малой погрешностью [8], низкими требованиями к вычислительным ресурсам и при этом позволяет учесть конструктивные особенности профиля показателя преломления реальных градиентных ОВ. Последующая подстановка в ИПП радиального распределения полей мод соединяемых ОВ, описываемых в рамках ОМПГ простыми функциями Лагерра-Гаусса, обеспечивает возможность перехода к аналитическим выражениям для оценки коэффициентов связи мод (КСМ) произвольного порядка.

В частности, для случая радиального рассогласования, ИПП предварительно был записан в Декартовой системе координат с учетом введенного осевого смещения d. Далее для перехода к модам высших азимутальных порядков потребовалось совместное применение известных формул разложения $\cos(lx)$ относительно $\cos(x)$, представления алгебраической функции $(a+z)^n$ в виде конечного степенного ряда, а также умножения конечных степенных рядов неодинаковой степени [10] и ранее выведенных формул произведения полиномов Лагерра разной степени, порядка и аргумента [8], что в итоге позволило разделить переменные интеграла числителя ИПП и перейти к табличным интегралам по dy и dx [10]. Громоздкие аналитические выражения для оценки КСМ с учетом введенного прецизионного радиального рассогласования, записанные в виде конечных вложенных сумм, приведены в ранее опубликованной работе [11].

Для апробации разработанного метода предлагается рассмотреть кварцевое слабонаправляющее FMF с диаметром сердцевины 42 мкм и оболочки 125 мкм, ранее полученная в результате оптимизации [12] специальная градиентная форма профиля показателя преломления которого обеспечивает снижение ДМЗ в центральной области «С»-диапазона длин волн до 30 пс/км и менее. Данное ОВ поддерживает во всем «С»-диапазоне длин волн распространение 16 направляемых мод LP_{lm} – до 6го азимутального l = 0…6 и 4-го радиального m = 1…4 порядков включительно (рис. 1).

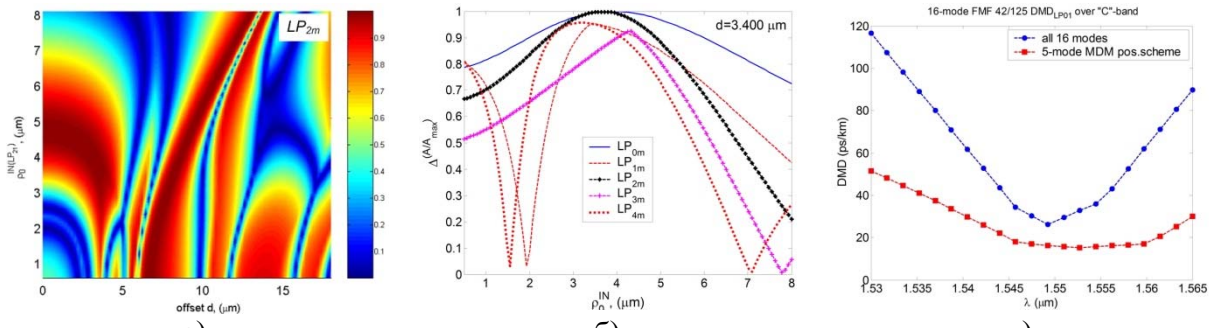
На первом этапе для длины волны $\lambda = 1550$ нм был проведен расчет КСМ возбуждаемых мод FMF и, соответственно, вводимых мод каналов системы MDM в зависимости от MFR последних и их положения относительно центра сердцевины возбуждаемого ОВ на заданном расстоянии d. Рассматривались следующие диапазоны значений: MFR $\rho_0^{IN} = 0{,}5…8{,}0$ мкм; радиальное смещение d = 0,0…18,0 мкм. Полученные результаты расчетов коэффициентов связи позволили перейти далее к построению 3D-диаграмм зависимости минимального разброса нормированных амплитуд возбуждаемых мод FMF соответствующих азимутальных порядков, в зависимости от перечисленных выше параметров (рис. 2*а*). Последующий анализ построенных диаграмм позволил выделить опти-

мальные значения MFR и локации торца сердцевины FMF, как в центральной, так и периферийной части, при которых для всех 5-ти перечисленных модовых групп $LP_{0m}...LP_{4m}$ минимальное отклонение нормированных амплитуд внутри одной группы идентичного азимутального порядка $l = 0…4$ составило не менее 0,95 (рис. 2*б*). При этом передача практически всей мощности вводимых каналов MDM осуществляется искомым направляемым модам FMF LP_{01}, LP_{11}, LP_{21}, LP_{32}, LP_{42}, отличающимся минимальным разбросом задержки относительно основной моды LP_{01} (рис. 1*в*). При этом если мода LP_{11} MDM вводится центрированно, то остальные каналы позиционируются на расстоянии 3,4…4,8 мкм относительно центра сердцевины FMF. В таблице представлены результаты расчета параметров несимметричной схемы прецизионного позиционирования 5 каналов MDM на торце сердцевины FMF в ближнем поле (длина волны λ = 1550 нм).



а) б) в)

Рис. 1. 16-модовое FMF 42/125 с уменьшенной ДМЗ:
а) профиль показателя преломления; б) оптический фактор ограничения (λ = 1550 нм);
в) диаграмма ДМЗ (λ = 1550 нм)



а) б) в)

Рис. 2. К расчету параметров схемы прецизионного позиционирования:
а) 3D-диаграммы зависимости минимального разброса нормированных амплитуд возбуждаемых мод FMF в зависимости от MFR вводимой моды LP_{21} MDM и ее смещения d (λ = 1550 нм); б) кривые зависимости этого же параметра от MFR моды LP_{21} при фиксированном смещении d = 3,400 мкм (λ = 1550 нм);
в) спектральные зависимости ДМЗ по основной моде FMF 42/125 «С»-диапазоне длин волн без и с подбором параметров схемы позиционирования мод каналов MDM

ТАБЛИЦА. Параметры схемы прецизионного позиционирования мод системы MDM

№ канала	MDM (λ = 1550 нм)		FMF (λ = 1550 нм)		*d*, мкм
	мода	*MFR*, мкм	мода	*MFR*, мкм	
1	LP_{01}	3,250	LP_{01}	4,6367	4,600
2	LP_{11}	4,680	LP_{11}	4,7636	0,000
3	LP_{21}	3,840	LP_{21}	4,7462	3,400
4	LP_{31}	1,710	LP_{32}	4,6228	4,800
5	LP_{41}	2,300	LP_{42}	4,6378	4,200

Сопоставление спектральных характеристик ДМЗ без и, напротив, с выбором параметров схемы прецизионного позиционирования, представленных на рис. 2, показывает, что подбор сочетания MFR вводимых мод и их положения на торце FMF на заданном расстоянии от центра сердцевины позволяет еще уменьшить ДМЗ более чем в 1,8 раз относительно исходного значения не только в области длины волны λ = 1550 нм, но и во всем «С»-диапазоне длин волн (рис. 2*в*).

Работа подготовлена при финансовой поддержке РФФИ в рамках научного проекта № 16-37-6001515 мол_а_дк.

Список используемых источников

1. Richardson D. J., Fini J. M., Nelson L. E. Space-division multiplexing in optical fibers // Nature Photonics. 2013. V. 7, No 5. PP. 354–362.

2. Mizuno T., Takara H., Sano A., Miyamoto Yu. Dense space-division multiplexed transmission systems using multi-core and multi-mode fiber // IEEE Journal of Lightwave Technologies. 2016. Vol. 34 (2). PP. 582–592.

3. Sillard P., Molin D., Bigot-Astruc M., Amezcua-Correa A., de Jongh K., Achten F. 50 μm multimode fibers for mode division multiplexing // IEEE Journal of Lightwave Technologies. 2016. Vol. 34 (8). PP. 1672–1677.

4. Bottacchi S. Multi-Gigabit transmission over multimode optical fibre. Theory and design methods for 10GbE systems. West Sussex: John Wiley & Sons Ltd., 2006. 654 p.

5. Bunge C.-A., Choi S., Oh K. Analysis of ring launching scheme using hollow optical fibre mode converter for 10 Gps multimode fibre communication // Optical Fiber Technology. 2006. Vol. 12. PP. 48–58.

6. Sim D. H., Takushima Y., Chung Y. C. High-speed multimode fiber transmission by using mode-field matched center-launching technique // IEEE Journal of Lightwave Technology. 2009. Vol. 27 (8). P. 1018–1026.

7. Снайдер А., Лав Дж. Теория оптических волноводов: пер. с англ. М.: Радио и связь, 1987. 656 с.

8. Bourdine A. Modeling and simulation of piecewise regular multimode fiber links operating in a few-mode regime // Advances in Optical Technologies. 2013. Vol. 2013. PP. 469389-1–469389-18.

9. Adams M. J. An introduction to optical waveguides. New York: John Wiley and Sons, 1981. 401 p.

10. Градштейн И. С., Рыжик И. М. Таблицы интегралов. М.: Физматгиз, 1962. 1100 с.

11. Bourdine A. V., Zhukov A. E. Fast approximate method for VCSEL-MMF transverse mode coupling analysis // Telecommunications and Radio Engineering. 2016. Vol. 7 (11). PP. 979–999.

12. Андреев В. А., Бурдин А. В., Бурдин В. А., Дмитриев Е. В., Евтушенко А. С., Севрук Н. Л., Халиков Р. Х. Моделирование градиентного профиля показателя преломления кварцевых оптических волокон с диаметром сердцевины 42 мкм и уменьшенной дифференциальной модовой задержкой // Инфокоммуникационные технологии. 2016. № 3. С. 235–246.

УДК 35.082

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ДЕЯТЕЛЬНОСТИ ОРГАНОВ ГОСУДАРСТВЕННОЙ ВЛАСТИ

Я. В. Андреянов[1], В. И. Андрианов[1], Л. А. Виткова[1], И. Ю. Потехин[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 (Роскомнадзор) по Северо-Западному федеральному округу

Всё большее количество жителей планеты, стало собираться в социальных сетях и прочих разнообразных проектах, объединяющих людей в сети Интернет. Число таких проектов растёт год от года, а это значит, что проблема выявления информационно-психологического воздействия в информационной инфраструктуре становится все более актуальной для государства.

мониторинг, социальные сети, BigData, SERM, ORM, информационно-психологическое воздействие, информационная война.

Во все времена безопасность была острой проблемой, начиная от древнего мира до наших дней. И сегодня информационная безопасность стала частью системы обеспечения национальной безопасности каждой страны. В Дохе в 2015 г. прошел 13-ый Конгресс по предупреждению преступности и уголовному правосудию, он был посвящен вопросам киберпреступности. В своем докладе Ян Элиассон, заместитель Генерального секретаря Организации Объединенных Наций отметил, что «Киберпреступность является новой – и одной из быстроразвивающихся – формой транснациональной преступности… Киберпреступность принимает самые

различные формы, чаще всего – преступлений, связанных с персональными данными. Кроме того, через Интернет все чаще совершаются преступления, связанные с нарушением авторских прав и прав интеллектуальной собственности, а также распространением материалов с детской порнографией и сценами насилия» [1].

Отметим, что сегодня с развитием технологий совершать киберпреступления стало проще, и сейчас даже не имеющие глубоких знаний или специальных навыков злоумышленники могут представлять реальную угрозу. В сети можно без труда приобрести программы, позволяющие пользователю находить открытые порты или проникать в системы, обходя парольную защиту. Но, к сожалению, выявлять такие нарушения проще не стало. В условиях анонимности киберпространства правоохранительным органам сложно устанавливать личность и местонахождение преступников. При этом известно, что более чем три четверти киберпреступлений в настоящее время связаны с организованной преступностью.

В октябре 2016 г. на Саммите ООН было официально заявлено, что отныне театром военных действий является инфокоммуникационное пространство. Отмечено, что киберпреступность и кибертерроризм развиваются стремительно, и превратились в промышленную индустрию. Известно, что отсутствие надлежащего регулирования и ресурсов во многих странах делает противодействие киберпреступность и кибертерроризм крайне непростой задачей. Для укрепления защиты и повышения эффективности регулирования в данной сфере требуются глобальные усилия, поскольку сейчас законодательные пробелы в странах с менее развитым режимом регулирования служат преступникам удобным прикрытием [2].

В данной работе авторы исследуют вопросы сохранности информационных ресурсов и защищённости, в инфокоммуникационных системах государственных органов власти. Авторы в своей работе отталкиваются от того, что информационная безопасность – это сохранность информационных ресурсов и защищённости, законных прав личности и общества в информационной сфере, это процесс обеспечения: конфиденциальности, целостности и доступности.

Анализ

Информация всегда играла важную роль в функционировании и развитии общества. Человек в принципе не может жить без информации, которая поступает к нему из различных источников.

Общественный и государственный интерес состоит в обеспечении возможности распространения информации, обеспечивающей конституционный порядок и законность, создании благоприятных условий для всестороннего развития человека.

Информационные технологии, проникая во все сферы общественной жизни, с одной стороны, создают условия для их нормального функционирования в современных условиях, обеспечивают высокую скорость обмена информацией и принятия решений, с другой стороны, порождают новые проблемы и угрозы, которых не было прежде.

Информационные технологии привели к появлению новых видов информационного поведения людей и организаций. Они позволяют получать и сохранять информацию, содержащую огромное количество детализированных сведений о людях, сообществах, организациях.

К изменениям в масштабе сбора и видах информации, которые регистрируются при помощи современных компьютерных технологий, добавилась еще легкость копирования и распространения информации в электронном виде. Теперь, когда используются телекоммуникационные каналы связи, степень обмена информацией стала практически безграничной.

Однако развитие современных компьютерных технологий обострило эту проблему как никогда. Особую актуальность сохранность информации имеет в органах государственной власти. С одной стороны они аккумулируют огромное количество персональной информации граждан, а с другой – их деятельность связана с безопасностью страны и поэтому далеко не вся информация может выходить за их пределы. Информация, которая циркулирует в сетях министерств и ведомств, чаще всего имеет закрытый характер. Поэтому обеспечение защиты информации, ее целостности является чрезвычайно важной задачей для эффективного функционирования органов государственной власти на всех уровнях.

В России существуют огромные базы данных, в которых хранятся сведения об избирателях (ГАС «Выборы»), пенсионерах (АИС Пенсионного фонда РФ), налогоплательщиках (АИС Федеральной налоговой службы), застрахованных лицах (АИС Фонда обязательного медицинского страхования). Сейчас ведется работа над созданием Государственного регистра населения РФ, который позволит получать доступ к персональным данным конкретного человека, размещаемым в различных ведомственных и региональных информационных системах учета населения.

Естественно, что утечка информации из этих или других баз крайне нежелательна и может привести к непредсказуемым последствиям.

С теоретической точки зрения, кажется, что сильной стороной государственных информационных систем в России является то, что они имеют закрытый, автономный характер. Конечно, в первую очередь, это касается таких систем, в которых содержится информация, имеющая отношение к государственным информационным системам (ГИС). Такие системы практически полностью изолированы от глобальных информационных сетей, поэтому специалистам, кажется, что защита информации в них несколько упрощается.

Практика же показывает, что трансграничная передача информации осуществляется по каналам связи крупнейших операторов в стране. Если проанализировать сайт zakupki.gov.ru, то мы видим, что услуги связи предоставляются в СЗФО чаще всего операторами Ростелеком или Мегафон [3].

Именно эти операторы связи являются наиболее частыми победителями в контрактах на поставку связи банкам России, и при этом в 2016 г. было зафиксировано более 52 млн атак на отказ в обслуживании на банковские сети. Официальной статистки по подобным атакам на органы исполнительной власти нет, но это не значит, что таких атак не было и не будет [4].

Одновременно с этим, еще один существенный пробел в российской системе информационной безопасности заключается в неспособности защитить конфиденциальную информацию. Об этом, в том числе свидетельствует наличие в свободной продаже баз данных ГИБДД, операторов связи, банков, которые содержат не только номер телефона, но и паспортные данные, место регистрации владельца, место работы и т. д.

С точки зрения регламентирующих правовых и нормативно-методических документов, исключающий какую-либо инициативу со стороны специалистов, на предприятиях действуют аттестованные ИСПДн, ГИС. Но при анализе только сайта zakupki.gov.ru мы видим, что одна организация аттестует в год (особенно если она указана в списке плановых проверок ФСТЭК) не более 1/4, а то и 1/10 всех машин из ИСПДн или ГИС. Формализм и необходимость сокращать расходы оказывают, в конечном счете, негативное влияние на качество защищенности государственных информационных ресурсов.

Выводы

Таким образом, решение проблем обеспечения информационной безопасности в органах государственной власти пока находится не на должном уровне; требуют существенного улучшения и обновления методы и технические средства, используемые в работе на этом направлении.

Первоочередной задачей является, необходимость обеспечения безопасности информации в соответствии с ее значимостью. Обязательное построение модели нарушителя, модели угроз и ежегодное обновление документов по ИБ, в связи с быстрым темпом обновления способов и типов угроз для различных ИС [5]. Одновременно с этим, важно помнить, что безопасность информации определяется отсутствием недопустимого риска, связанного с утечкой информации по техническим каналам, несанкционированными и непреднамеренными воздействиями на данные

и на другие ресурсы автоматизированной информационной системы, используемые в автоматизированной системе. Необходимо внедрять концепции управления рисками ИБ в органах государственной власти.

Список используемых источников

1. Компьютерная преступность и информационная безопасность // Под ред. Леонова А. П. Минск: АРИЛ, 2000. 552 с.

2. Мирошников Б. Н. Борьба с киберпреступлениями – одна из составляющих информационной безопасности Российской Федерации [Электронный ресурс] / Доступно из URL: http://www.crime-reeearch.ru/articles/Miroehl (дата обращения 20.03.2017).

3. Официальный сайт единой информационной системы в сфере закупок [Электронный ресурс]. URL:http://www. zakupki.gov.ru (дата обращения 20.03.2017).

4. Официальный сайт газеты Ведомости [Электронный ресурс]. URL: http://www. vedomosti.ru (дата обращения 21.03.2017).

5. Донской Д. М., Рябова О. Н., Сахаров Д. В., Виткова Л. А. Некоторые аспекты модели нарушителя информационной безопасности в интернете вещей // В сборнике: Интернет вещей и 5G. 2016. С. 47–50.

УДК 4.056

ИССЛЕДОВАНИЕ ВОЗМОЖНОСТЕЙ СЕТИ БОТНЕТ И МЕТОДОЛОГИЯ ЗАЩИТЫ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

В. И. Андрианов, А. А. Чекалов

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

В статье рассматривается: что такое ботнет, процесс его формирования, какими возможностями обладают ботнеты. Описаны основные методы обнаружения и отражения атак с использованием ботнетов.

ботнет, эксплойты, кликеры, грабберы, фреймеры.

28 сентября 2016 года был опубликован отчет Европола «Оценка угроз 2016 г., связанных с организованной преступностью в интернете» [1]. В отчете указано, что сетевые атаки с использованием ботнетов (DDoS-атаки в частности) признаются правоохранительными органами членов Евросоюза основной угрозой для любой структуры, использующей доступ в интернет. А объемы трафика при подобных атаках стано-

вятся беспрецедентными. В сентябре были зафиксированы объемы трафика свыше 620 Гбит/сек, и даже около 1 Тбит/сек [2, 3].

Рассмотреть процесс создания и возможности ботнета, а также методы борьбы с ним.

Ботнет (от англ. “*robot*” и “*network*”) – это сеть компьютеров, состоящая из *n* рабочих станций с запущенными бот-программами (далее просто бот). Боты предоставляют злоумышленнику удаленный доступ к рабочим станциям (рис. 1).

Бот – это программа, работающая на компьютере и выполняющая команды, полученные от сервера управления. Сервер управления (*Command&Control Centre*), как правило, не привязывается к одному компьютеру, а перемещается между компьютерами, входящими в ботнет, что сильно затрудняет его обнаружение.

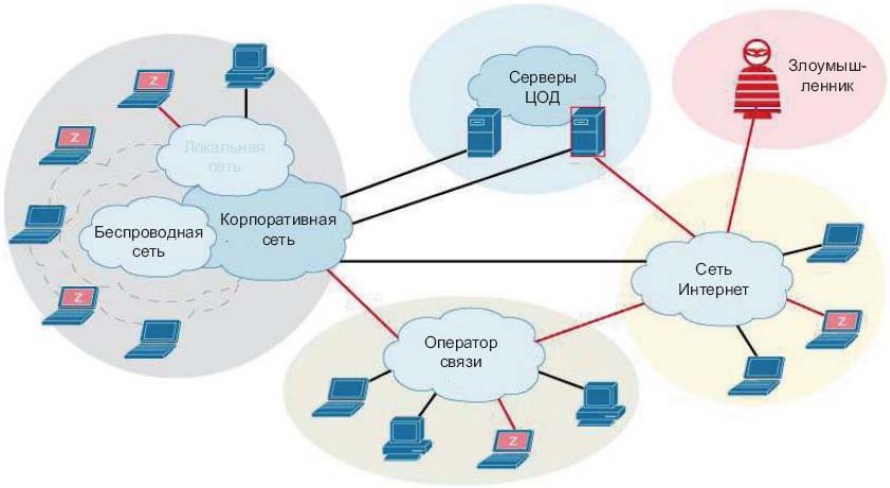


Рис. 1. Схема типичного ботнета

Бот на зараженном компьютере может:

– загружать других ботов;

– имитировать действия человека на сайтах («накручивание» кликов на рекламных площадках и групп в социальных сетях);

– рассылать почтовый и прочий спам;

– размещать сообщения на сайтах;

– собирать пароли с компьютера пользователя (т. е. кража персональных данных);

– вести лог действий пользователя;

– менять стартовые и поисковые страницы;

– подменять поисковую выдачу, когда пользователь что-то ищет (фишинг).

Отдельно стоит упомянуть про распределенные атаки типа «отказ в обслуживании» (DDoS-атаки). Ботнет осуществляет скоординированную

атаку на целевую систему с целью превышения её вычислительных мощностей и полосы пропускания каналов передачи (объем трафика постоянно растет), что приводит к отказу данной системы. Целью подобной атаки чаще всего является вымогательство денег у жертвы в обмен на её прекращение или получение доступа к атакуемой системе.

Для работы и пополнения своего ботнета злоумышленник(и) использует большой набор программ и сервисов.

Первая необходимая для работы ботнета программа – это *лоадер* (от англ. "*loader*"). Ее задача – попасть на компьютер пользователя, и скачать другие бот-программы.

Лоадер состоит из веб-панели администратора, в которой злоумышленник может указать различные параметры, и исполнимого файла, запускаемого на компьютере жертвы и получающего команды от сервера управления. Если сигнатура лоадера есть в базе антивирусов, то они его называют, как правило, "Trojan.downloader".

Для загрузки лоадера используется exploit pack (от англ. "*exploit pack*" – связка эксплойтов). Эксплойт – это несколько строк вредоносного кода на странице web-сайта. Эксплойты используют уязвимости браузера или же его плагинов для того, чтобы выполнить на компьютере жертвы свой код, т.е. осуществить загрузку лоадера.

Для стабильной работы связки эксплойтов злоумышленник систематически ее «чистит». «Чистка» связки – это модификация кода данной связки так, чтобы антивирусы не смогли её идентифицировать по сигнатуре, которая уже есть в их базе. Чем больше трафика проходит через связку, тем быстрее ее сигнатура попадет в базы антивирусов и процент успешных заражений упадет.

Также злоумышленнику необходим особый трафик, чтобы направлять пользователей на свою связку. Трафик в данном контексте – это количество посещений за сутки определенной web-страницы. Измеряется трафик в единицах уникальных посещений. Заражается не каждый компьютер, а от 1 до 20 % в зависимости от источника трафика и качества связки эксплойтов и лоадера [4].

Для получения подобного рода трафика злоумышленник широко использует почтовый и прочий спам, в котором содержится ссылка на web-страницу с лоадером. Кроме того лоадеры часто встраиваются в активаторы и генераторы ключей к взломанному программному обеспечению. Как итог пользователь сам запускает у себя лоадер и становится еще одним ботом ботнета.

Для монетизации ботнета (рис. 2) злоумышленник использует такие программы как:

– *Грабберы.* Собирают пароли на сайтах, ftp-серверах, почтовых сервисах, социальных сетях, ISQ и т. д.

– *Фреймеры*. Собранные пароли к ftp-серверам используется для установки на web-сайтах фреймов, ведущих на связку эксплойтов.

– *SOCKS proxy*. Через них работают программы, занимающиеся рассылкой спама, парсингом, «накрутками» и т. п.

– *Спам программы*. Рассылают спам с рекламой злоумышленника.

– *CEO спам программы*. Расставляют по форумам и комментариям на них ссылки на web-сайты злоумышленника.

– *Чатботы в социальных сетях*. Имитируя пользователя, разговаривают с жертвой, чтобы убедить ту перейти по ссылке на web-сайт злоумышленника.

– *«Автозалив»*. Ворует деньги, если у пользователя есть средства в онлайн платежных системах или обычных банках.

– *Кликеры*. Накручивают посещения на сайтах злоумышленника; кликают по рекламе, где платят за клики.

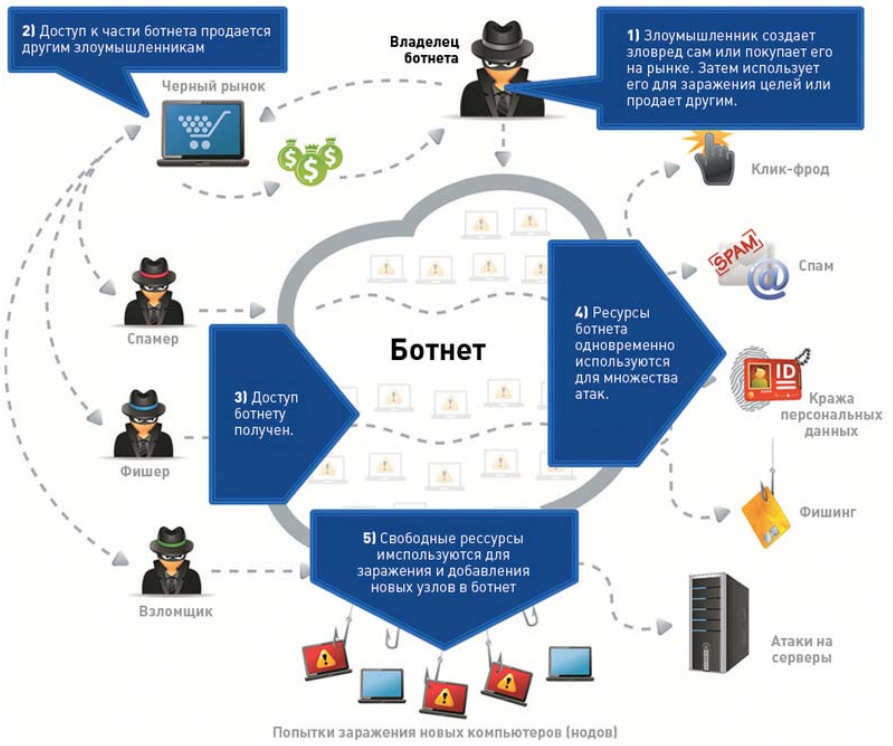


Рис. 2. Возможности ботнета

Обнаружение и борьба с ботнетами

Такие методы как анализ трафика на основе используемых портов, фильтрация трафика и проверки с использованием сигнатур не могут эффективно бороться с атаками ботнетов, так как ботнеты способны быстро и динамично менять свой код и систему управления [5]. Для обнаружения

ботнета и защиты от него следует использовать средства, которые используют такие методы как:

Анализ телеметрии. Метод заключается в использовании сводной информации сетевого и транспортного уровня от сетевых устройств. Благодаря анализу телеметрии можно обнаружить трафик DDoS-атак, всплески трафика SMTP, характерного для массовой рассылки спама и управляющего трафика сервера управления ботнета.

Обнаружение аномалий. В отличие от метода сравнения атаки с уже накопленной базой данных сигнатур, этот подход описывает характеристики стандартного трафика, а затем производится поиск отклонений от заданной нормы. Таким образом, обеспечивается эффективное обнаружение и блокировка DDoS-атак и попыток массового сканирования, которые предпринимают ботнеты. Данный метод может применяться как на сетевых устройствах (маршрутизаторы ядра сети), так и на оконечных узлах (серверы и рабочие станции). При использовании на оконечных узлах этот метод позволяет обнаруживать подозрительные действия и нарушения политик безопасности и предотвращать заражение компьютера.

Анализ журнала сервера DNS. Часто ботнеты используют бесплатные службы DNS для размещения адреса поддомена серверов IRC, захваченных ботнетом и содержащих программы с вредоносным кодом. Как правило, бот-программы содержат в своем коде жестко заданные ссылки на DNS-сервер. Эти ссылки способно обнаружить любое средство анализа журнала DNS-запросов. При обнаружении подобного рода служб администратор DNS-сервера может нейтрализовать ботнет, переадресовав поддомены, нарушающие действующую политику, на несуществующий IP-адрес (т. е. «маршрутизация в никуда»).

Выводы

В статье рассмотрен механизм пополнения ботнета новыми ботами. Показано, что ботнеты используют множество векторов заражения и атак. Рассмотрено как именно злоумышленники монетизируют возможности ботнетов. Показано, что данная проблема на сегодняшний день является актуальной как для крупных провайдеров и хостингов (DDoS-атаки), так и для рядовых пользователей.

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. С. 28–34.

2. Штеренберг С. И., Виткова Л. А., Просихин В. П. Методика применения концепции адаптивной саморазвивающейся системы // Информационные технологии и телекоммуникации. 2014. № 4 (8). С. 126–133.

3. 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.

4. 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.

5. Андрианов В. И., Романов Г. Г., Штеренберг С. И. Экспертные системы в области информационной безопасности // Актуальные проблемы инфотелекоммуникаций в науке и образовании. IV Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 2 томах. 2015. С. 193–197.

УДК 004.056.53

ПРЕДОТВРАЩЕНИЕ УТЕЧЕК КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

Е. А. Аникевич, Л. А. Виткова, Е. Н. Сацук, И. Ю. Сергеева

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

Управление и контроль за событиями и инцидентами все чаще становятся приоритетными в информационной безопасности. Все большее количество организаций несут убытки из-за хищения информации. Неосторожность, неосмотрительность рядового сотрудника, отсутствие квалификации и знаний в области информационной безопасности повышают риски и становятся основными источниками угроз в информационных системах. В данной статье авторы рассматривают некоторые популярные способы обеспечения безопасности.

угроза, уязвимость, вредоносное ПО, хакер, ущерб, атака, BYoD, DLP-системы, SIEM.

Введение

Современный мир уже невозможно представить без информационных систем. Появление и повсеместное использование баз данных открывают новые способы хищения личной информации.

Количество угроз, которые могут нанести вред информационной системе, с каждым годом приумножается. Количество утечек данных постоянно растет, а объемы скомпрометированной информации увеличиваются по мере того, как возрастает ценность электронной информации. Такая динамика роста обусловлена новыми возможностями, связанными с использованием и представлением информации в цифровом виде (пере-

вод услуг в электронный вид, e-commerce, электронные деньги, интеллектуальная собственность). Несомненно, чем больше таких возможностей в глобальном масштабе, тем выше интерес злоумышленников к цифровым данным [1].

Анализ

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. Задачи информационной безопасности сводятся к уменьшению ущерба, а также к прогнозированию и предотвращению негативных воздействий.

На сегодняшний день в Банке данных угроз ФСТЭК России представлена информация об 194 угрозах и 15176 уязвимостях программного средства или информационной системы в целом [2].

Обзор статистики и динамики утечек данных позволяет понять, какой канал коммутации наиболее уязвим и по какой причине, и что же опаснее: внешняя атака или деструктивные действия сотрудников компании. Каналов, по которым может произойти утечка, множество – они включают в себя внешние устройства, сетевое хранилище или буфер обмена, электронные письма, IP-телефонию, SSL-трафик, весь веб-трафик, облачные хранилища данных, печать и отправка факса, IM и т. д. Имеется достаточное количество автоматизированных средств анализа, которые выявляют среди легитимного потока информации подозрительную передачу конфиденциальных данных. Проанализировав частоту утечек по тому или иному каналу, можно разработать модель угроз и выяснить каким каналам следует уделить повышенное внимание, а затем и внедрить средства защиты. Можно заметить, что сетевой канал ежегодно находится на первом месте по количеству утечек и по объему скомпрометированных данных [3].

Одной из важнейших проблем, имеющихся в организации, которая должна быть решена в рамках обеспечения ее безопасности, является проблема управления «заплатками» и обновлениями ПО. Пренебрежение этой задачей создает серьезную уязвимость для бизнеса и способно парализовать работу всей организации [4].

Злоумышленники хорошо осознают, что наиболее действенный способ удара по цели – это атака на ее основание. Хакеры выбирают простейший доступный путь при определении, каким образом и где их эксплойты смогут добиться успеха. Обычно такие возможности появляются при использовании неисправного или старого программного обеспечения (ПО). Таким образом, чтобы обеспечить должную защиту от уязвимостей необ-

ходимо обновлять ПО до последней версии, в которой уже устранены данные ошибки. Неизвестное вредоносное ПО, как правило, не распознается антивирусным средством. Каждый новый вариант вредоносного ПО, даже если он незначительно отличается от предыдущего, потенциально способен обойти наиболее современный антивирус и другую защиту. Без распознавания сигнатуры вредоносного файла средства предотвращения не могут делать свою работу [5].

Один из наиболее действенных способов усилить и ускорить распространение вредоносного ПО – это зараженный троянской программой или вирусом компьютер; данный факт позволяет третьей стороне полностью или частично управлять работой машины. Таким образом, формируются ботнеты – сети, состоящие из зараженных ботами или «зомбированных» компьютеров под управлением злоумышленника или организации, использующих их для направления спама, атаки на другие компьютеры или запуска DDoS атак, еще известных как «распределенный отказ в обслуживании».

Если говорить о ботах, то можно назвать такие виды возможного ущерба, как кража банковских учетных записей и другой представляющей ценность информации, отключение системы безопасности, установка вредоносного ПО, выполнение задач «кликфрода» (обманные переходы по рекламным блокам), получение удаленного доступа.

Большой рост использования мобильных и личных устройств на работе BYoD (*Bring Your own Device*) ставит задачу обеспечения доступа сотрудников к корпоративным ресурсам независимо от места и способа входа в сеть. С самого начала можно было предсказать, что появление и распространение концепции BYoD может послужить источником проблем мобильной безопасности. В качестве вектора атаки мобильные устройства дают более легкий и прямой доступ к ценным корпоративным ресурсам, нежели любая другая точка вторжения в сеть, становясь, таким образом, слабейшим звеном в цепи безопасности. Если мобильная безопасность находится на низком уровне, то это позволит атакующим обойти все средства защиты и заполучить ценную информацию, такую как персональные данные, пароли, частная и деловая переписка, корпоративные документы, доступ к сетям и приложениям компании, то есть то, что принято называть коммерческой тайной. В деловом контексте эти опасения могут быть даже сильнее. Фактически 87 % профессионалов IT сферы констатировали, что беспечные сотрудники представляют собой более серьезную угрозу, нежели киберпреступники. Внешние нарушители могут быть нацелены на предприятие и извлечение ценной информации из мобильных устройств сотрудников, могут получить контроль над различными датчиками для осуществления записи ввода с клавиатуры, кражи сообщений, включения видеокамер и многого другого. Изначально внешние

угрозы считались более опасными, но необходимость защиты и от внутренних угроз была очевидна на всех этапах развития средств информационной безопасности [6].

Информационная система становится более уязвимой, когда администраторы пренебрегают базовыми средствами защиты или используют устаревшие средства, которые оказываются недостаточными для противодействия современным изменяющимся угрозам. В последние годы большое внимание стали уделять внутренним угрозам, и популярность на такие средства, как DLP-системы и SIEM, возросла.

Технология предотвращения утечек конфиденциальной информации за пределы корпоративной сети (*Data Loss Prevention*) строится на анализе потоков данных, пересекающих периметр защищаемой информационной системы [7]. При выявлении в потоке конфиденциальной информации срабатывает защита, и передача сообщения (пакета, потока, сессии) блокируется или отслеживается. Такая технология обеспечивает контроль и защиту генерируемой информации. Как показала практика, большая часть утечек происходит из-за невнимательности сотрудников компании и халатного отношения к данным, составляющим коммерческую тайну.

SIEM (*Security Information and Event Management*) – такие системы сами по себе не способны что-либо предотвращать или защищать. Задача этих систем состоит в другом, а именно – автоматизация мониторинга и анализа всех событий, которые происходят в многочисленных системах защиты, таких как антивирусы, DLP, IDS, маршрутизаторы, межсетевые экраны, операционные системы серверов и пользовательских ПК, и при этом детектирование отклонения от норм по неким критериям. Если такое отклонение выявлено, то система генерирует инцидент. Немаловажно, что с ее помощью можно выявить действия, которые внешне выглядят вполне безобидными, но в совокупности представляют угрозу. Например, если доверенный пользователь отправляет конфиденциальные данные на e-mail адрес, который лежит вне обычного круга адресатов, то DLP-система не всегда отслеживает такие действия, однако SIEM сгенерирует инцидент на базе накопленной статистики.

С помощью SIEM можно добиться почти абсолютной автоматизации процесса выявления угроз и рисков информационной безопасности на будущий период. SIEM позволяет акцентировать внимание только на важных и действительно критических угрозах, работать не с событиями, а с инцидентами, своевременно выявлять аномалии и риски, предотвращать финансовые потери и т. п. [8].

Выводы

Задача обеспечения информационной безопасности должна решаться системно. Это означает, что различные средства защиты (аппаратные, программные, физические, организационные и т. д.) должны применяться одновременно и под централизованным управлением.

Для того чтобы обезопасить рабочие станции, необходимо начать с базовых действий: убедиться в том, что на компьютерах работают персональные межсетевые экраны, установлены обновленные версии ПО, а также последние версии антивирусных продуктов.

На сегодняшний день имеется широкий арсенал способов обеспечения информационной безопасности:

1. Средства идентификации и аутентификации пользователей.
2. Средства шифрования информации, хранящейся на компьютерах и передаваемой по сетям.
3. Межсетевые экраны.
4. Виртуальные частные сети.
5. Средства контентной фильтрации.
6. Инструменты проверки целостности содержимого дисков.
7. Средства антивирусной защиты.
8. Системы обнаружения уязвимостей сетей и анализаторы сетевых атак.

Каждое из перечисленных средств может быть использовано как самостоятельно, так и в интеграции с другими. Это делает возможным создание систем информационной защиты для сетей любой сложности и конфигурации, не зависящих от используемых платформ.

Таким образом, для того, чтобы система могла противостоять угрозам, необходимо проводить оценку состояния и модернизировать ее. Необходимо обеспечивать защиту, как от внешних атак, так и внутренних. Любая, даже самая незначительная утечка информации может нанести серьезный урон организации и повлечь за собой финансовые убытки.

Подводя итоги, можно сказать, что проблему проще предотвратить, чем искать пути ее решения.

Список используемых источников

1. Глобальное исследование утечек конфиденциальной информации в I полугодии 2016 года [Электронный ресурс] // Аналитический центр InfoWatch. URL: http://itzashita.ru/analitics/globalnoe-issledovanie-utechek-konfidentsialnoy-informatsii-v-i-polugodii-2016-goda.html (дата обращения 26.12.2016).

2. Банк данных угроз безопасности информации [Электронный ресурс] // ФАУ «ГНИИИ ПТЗИ ФСТЭК России». URL: http://bdu.fstec.ru/threat (дата обращения 11.01.2017).

3. Аношин М. С. DLP – зачем нам это нужно [Электронный ресурс] // Jet Info. 2015. № 9. URL: http://www.jetinfo.ru/jetinfo_arhiv/dlp-so-znakom/dlp-zachem-nam-eto-nuzhno/2015 (дата обращения 26.12.2016)/

4. 2016_SecurityReport_PrintProduction_RUSv3 [Электронный ресурс] // Check Point – Отчет по безопасности 2016. URL: http://rrc.ru/upload/checkpoint/analytic_reports/2016_SecurityReport_PrintProduction_RUSv3_SCREEN.pdf (дата обращения 26.12.2016).

5. Панасенко А. Сравнение систем защиты от утечек (DLP) – часть 1 [Электронный ресурс] // Anti-Malware.ru. URL: http://www.anti-malware.ru/comparisons/data_leak_protection_2011_part1# (дата обращения 26.12.2016).

6. Системы предотвращения утечек конфиденциальной информации (DLP-системы) [Электронный ресурс] // Life-prog.ru. URL: http://life-prog.ru/1_1230_sistemi-predotvrashcheniya-utechek-konfidentsialnoy-informatsii-DLP-sistemi.html (дата обращения 30.12.2016)/

7. SIEM системы: найти иголку в стогу сена [Электронный ресурс] // Инфобезпека, 2013. URL: http://www.infobezpeka.com/publications/?id=589 (дата обращения 30.12.2016).

8. SIEM Security Information and Event Management [Электронный ресурс] // WAF NEMESIDA, 2016. URL: http://auditib.ru/siem-security-information-and-event-management/ (дата обращения 30.12.2016).

УДК 654.027

ИМИТАЦИОННАЯ МОДЕЛЬ РАСПРЕДЕЛЕНИЯ ТРАФИКА НА УЧАСТКЕ ТРАНСПОРТНОЙ СЕТИ

А. В. Ануфренко[1], С. Ф. Буцев[1], А. К. Канаев[2], А. Н. Копытин[1]

[1]Военная академия связи имени Маршала Советского Союза С. М. Буденного
[2]Петербургский государственный университет путей сообщения Императора Александра I

Развитие технологий транспортной сети связи, повышение требований к её функционированию вызывают необходимость детального понимания процессов, происходящих в транспортной сети связи. Хорошим средством для этого является имитационное моделирование. В работе изложена суть разработанной имитационной модели транспортной сети связи.

транспортная сеть связи, имитационное моделирование, GPSS World.

Ввиду широкого разнообразия технологий, протоколов, аппаратных средств, с помощью которых осуществляется процесс передачи информации, зачастую оказывается крайне сложно оценить и провести анализ распределения трафика на участке транспортной сети не говоря уже о его прогнозировании. Аналитические модели, применяемые для описания распределения трафика, либо очень сложны, либо недостаточно детализируют

описываемый процесс. Имитационное моделирование помогает создать достаточно детализированную модель, избегая сложного аналитического описания. Поэтому с помощью имитационного моделирования на основе программы GPSS STUDIO создана модель распределения трафика на участке транспортной сети. Разработанная модель позволяет проводить исследование характера распределения трафика на участке транспортной сети.

Моделируемая транспортная сеть связи представляет из себя набор последовательно соединенных узлов транспортной сети связи, которые работают на основе технологии оптических сетей OTN-OTH. Трафик в транспортную сеть связи поступает из узла агрегации и представляет собой сочетание речевого трафика, трафика данных и видео трафика [1, 2]. Из транспортной сети связи трафик попадает на другой узел агрегации. Транспортная сеть представлена как объект, имеющий многослойную (многоуровневую) функциональную структуру. Каждый слой многослойной сети интерпретируется как своего рода сеть слоя – «layer network», то есть сеть в пределах одного слоя [1]. В моделируемой сети рассматриваются два уровня эталонной модели взаимодействия открытых систем (физический и канальный), функционал которых в большей степени отвечает задачам, возлагаемым на транспортную сеть связи. На канальном уровне рассматривается технология Ethernet, на физическом уровне технология, которая включает в себя стек протоколов (GFP/SDH/OTN/DWDM) [1].

Модельное описание транспортной сети связи производится путем ее декомпозиции на множество структур, каждая из которых отображает отдельные аспекты архитектуры сети и взаимосвязь определенной группы элементов, выделенных на некотором уровне рассмотрения сети. Имитационная модель транспортной сети связи учитывает параметры физической и функциональной структур архитектуры транспортной сети связи. Имитационная модель построена с использованием дискретно-событийного подхода.

Модель разрабатывалась в программе GPSS STUDIO, которая является существенно доработанной и улучшенной версией программы GPSS World. GPSS STUDIO обладает расширенным функционалом: с помощью «Графического редактора» позволяет строить структурные схемы, с помощью «Конструктора форм» позволяет автоматизировать процесс ввода большого количества исходных данных, усовершенствован текстовый редактор GPSS World. В сравнении с GPSS World GPSS STUDIO значительно облегчила процесс разработки имитационных моделей, сохранив при этом без изменения достаточно простой для изучения язык программирования GPSS World, с помощью которого за последние 50 лет созданы сотни тысяч имитационных моделей.

Разработанная в GPSS STUDIO модель транспортной сети связи представляет собой многофазную многоканальную систему массового обслуживания с ограниченными ёмкостями буферов (накопителей), то есть с отказами [3, 4].

Общий алгоритм функционирования имитационной модели состоит из трех этапов: подготовительный этап, в рамках которого происходит инициализация модели, определяется топология сети, осуществляется ввод исходных данных в сетевые окончания (узлы агрегации) и в каждый тип оборудования узлов транспортной сети; основной этап, в рамках которого происходит непосредственно функционирование модели и обработка событий; заключительный этап, в рамках которого происходит генерация отчетов и вычисление требуемых оценок, а также сбор данных статистики.

В модель транспортной сети сообщения поступают от одного источника (узла агрегации). Интервалы поступления сообщений распределяются по закону, который формирует модель узла агрегации в зависимости от ее нагрузочных параметров. Интервалы между отказами, а также время восстановления работоспособности узлов транспортной сети связи, распределяются по экспоненциальному закону. В модели учитываются задержки работы защитных механизмов транспортной сети связи, которые разделены на внутриузловые и сетевые. Сообщения проходят через все узлы транспортной сети и попадают к получателю (на другой узел агрегации).

Функционирование модели протекает по таймеру модельного времени. Изменение модельного времени происходит путем его продвижения до ближайшего события, связанного с изменением состояния моделируемой системы. При моделировании транспортной сети связи такими событиями является поступление кадров в транспортную сеть связи. Таким образом, процесс моделирования продвигается путем определения ближайшего момента наступления каждого события. Таймер модельного времени корректируется автоматически в соответствии с логикой, предписанной моделью.

В результате моделирования получены оценки основных показателей для агрегированного трафика, проходящего через транспортную сеть связи, а именно: величина задержки распространения трафика, джиттер, количество потерянных кадров трафика с учетом меняющейся нагрузки транспортной сети связи, а также выходом из строя узлов транспортной сети связи. Получены граничные значения допустимой нагрузки, поступающей в транспортную сеть связи, при пошаговом увеличении значений интенсивности агрегированного трафика. Модель позволяет исследовать динамику увеличения задержки и джиттера при различных видах нагрузки транспортной сети связи, что приводит к пониманию, какие требования к данной сети необходимо предъявлять для обеспечения заданного уровня качества обслуживания.

Разработанная модель распределения агрегированного трафика на участке транспортной сети может применяться при обосновании решений в задачах планирования и проектирования телекоммуникационной инфраструктуры.

Список используемых источников

1. Фокин В. Г. Оптические системы передачи и транспортные сети. М.: Эко–Трендз, 2008. 288 с.

2. Ануфренко А. В., Волков Д. В., Канаев А. К. Принцип организации узла агрегации мультисервисной сети связи // Актуальные проблемы инфотелекоммуникаций в науке и образовании. IV Международная научно-техническая и научно-методическая конференция: сборник научных статей в 2 томах. 2015. Т. 1. С. 203–206.

3. Алиев Т. И. Основы моделирования дискретных систем. СПб.: СПбГУ ИТМО, 2009. 363 с.

4. Ануфренко А. В., Баранцев А. В., Канаев А. К. Обеспечение отказоустойчивости сетей связи, функционирующих на базе пакетно-ориентированных технологий // Юбилейная 70-я всероссийская научно-техническая конференция, посвященная Дню радио. 2015. С. 304–306.

УДК 654.027

ИМИТАЦИОННЫЕ МОДЕЛИ УЗЛА АГРЕГАЦИИ В ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ

А. В. Ануфренко[1], Е. Л. Васильев[1], В. К. Гойденко[1], А. К. Канаев[2]

[1]Военная академия связи имени Маршала Советского Союза С. М. Буденного
[2]Петербургский государственный университет путей сообщения Императора Александра I

От функционирования узла агрегации сети связи зависит работа узлов транспортной сети и узлов сети доступа. Разработка имитационных моделей узла агрегации позволяет проанализировать их сложную структуру. В работе представлены модели узла агрегации, разработанные в программе «GPSS STUDIO».

узел агрегации сети связи, имитационное моделирование, GPSS STUDIO.

На сегодняшний день существует ряд подходов для анализа и оценки процессов функционирование узлов агрегации сети связи. В то же время изменение характеристик сетевых информационных потоков требует применения современного математического аппарата для анализа процессов протекающих в узлах агрегации. Разработанные имитационные модели узлов агрегации помимо классических пуассоновских моделей трафика ис-

пользуют модели самоподобного трафика, что способствует получению оценки параметров моделируемых узлов агрегации, близким к реальным значениям [1, 2]. Для наглядной интерпретации особенностей поведения трафика в узлах агрегации сети связи моделирование трафика производится с использованием модели типа ON/OFF [3, 4], которая может быть использована при описании пульсирующей структуры трафика. Длительности ON и OFF периодов меняются по экспоненциальному закону. Интенсивность трафика описывается законами Парето, Вейбула, Пуассона (для трафика данных, видеотрафика, речевого трафика соответственно) [1, 3]. При моделировании трафика учитывается процесс инкапсуляции трафика в соответствии со стеком протоколов RTP/UDP/IP/Ethernet (для речевого трафика и видео трафика) и в соответствии со стеком протоколов TCP/IP/Ethernet (для трафика данных).

С точки зрения теории массового обслуживания структуры смоделированных узлов агрегации представляют из себя неприоритетную (как по параметрам поступающих заявок, так и по типу обслуживания), не экспоненциальную нелинейную разомкнутую сеть массового обслуживания [5]. В моделях узлов агрегации описана генерация трафика от различных источников, кодирования битов информации, процесс инкапсуляции, обработка пакетов в узле агрегации, задание длительности сеанса связи источника. Разработано шесть различных моделей узла агрегации сети связи. Количество узлов в сети массового обслуживания каждой модели узла агрегации соответствует структуре моделируемого узла агрегации. Количество обслуживающих приборов для всех узлов равно единице. Длительности обслуживания заявок в узлах сети массового обслуживания различны и зависят от параметров, рассматриваемых в моделях образцов сетевой аппаратуры и вида трафика. Часть узлов сети массового обслуживания имеют неограниченную емкость (генераторы трафика), емкость остальных узлов соответствует параметрам рассматриваемых в моделях образцов сетевой аппаратуры. Матрица вероятностей передачи заявок от узла к узлу сети массового обслуживания зависит от структуры моделируемого узла агрегации. Производительность узлов сети массового обслуживания зависит от параметров, рассматриваемых в моделях образцов сетевой аппаратуры.

Нагрузочные, структурные, функциональные параметры модели соотнесены с соответствующими параметрами рассматриваемого узла агрегации. Поступающие кадры данных имитируются транзактами. Модель включает в себя 17 взаимосвязанных функциональных элементов, отражающих структуру и логику узла агрегации.

Средой моделирования для разработки имитационных моделей узла агрегации была выбрана программа GPSS STUDIO, которая является общецелевой системой имитационного моделирования и представляет собой

мощную среду компьютерного моделирования общего назначения, разработанную для профессионалов в области моделирования. Данная программа обладает мощной дискретно-событийной частью, позволяет учитывать сотни тысяч элементов моделируемого объекта и обладает простым для понимания языком программирования. В сравнении с GPSS World GPSS STUDIO приобрела значительно расширенный функционал, позволяющий намного быстрее строить наглядные модели, а также намного проще проводить эксперименты с разработанными моделями.

В результате моделирования получены оценки основных параметров для агрегированного трафика с учетом различных по структуре узлов агрегации, а именно: величина задержки распространения трафика, джиттер, количество потерянных кадров трафика. Проведен анализ влияния интенсивности нагрузки от каждого генератора трафика, а также различных законов распределения трафика на параметры агрегированного трафика.

Разработанные модели узла агрегации в телекоммуникационной сети позволяют анализировать характер распределения агрегированного трафика в задачах анализа узлов агрегации и позволяют подобрать рациональную структуру узла агрегации для соответствующей нагрузки агрегированного трафика. Увеличение объемов информации, требование по балансированию нагрузки на сетях связи и эффективности работы сетевых элементов свидетельствует об востребованности разработанных имитационных моделей узла агрегации в телекоммуникационной сети.

Список используемых источников

1. Барбер Д., Дэвис Д., Прайс У., Соломонидес С. Вычислительные сети и сетевые протоколы. М. : Мир, 1982. 562с.

2. Ануфренко А. В., Баранцев А. В., Канаев А. К. Обеспечение отказоустойчивости сетей связи, функционирующих на базе пакетно-ориентированных технологий // Юбилейная 70-я всероссийская научно-техническая конференция, посвященная Дню радио. 2015. С. 304–306.

3. Шелухин О. И., Осин А. В., Тенякшев А. М. Фрактальные процессы в телекоммуникациях. М. : Радиотехника, 2003. 480 с.

4. Ануфренко А. В., Волков Д. В., Канаев А. К. Принцип организации узла агрегации мультисервисной сети связи // Актуальные проблемы инфотелекоммуникаций в науке и образовании. IV Международная научно-техническая и научно-методическая конференция: сборник научных статей в 2 томах. 2015. Т. 1. С. 203–206.

5. Алиев Т. И. Основы моделирования дискретных систем. СПб.: СПбГУ ИТМО, 2009. 363 с.

УДК 654.029

МУЛЬТИАГЕНТНЫЙ ПОДХОД К ФОРМИРОВАНИЮ СТРУКТУРЫ СИСТЕМЫ УПРАВЛЕНИЯ ТРАНСПОРТНОЙ СЕТЬЮ СВЯЗИ НА ОСНОВЕ ТЕХНОЛОГИИ CARRIER ETHERNET

А. В. Ануфренко[1], А. К. Канаев[2], Э. В. Логин[2]

[1]Военная академия связи имени Маршала Советского Союза С. М. Буденного
[2]Петербургский государственный университет путей сообщения Императора Александра I

Рост разнообразного цифрового оборудования, увеличение его контролируемых параметров требует от системы управления способности работать с распределенными объектами с большим набором изменяемых параметров. Ввиду этого используется мультиагентный подход к формированию структуры системы управления.

система управления транспортной сетью связи, мультиагентный подход, Carrier Ethernet.

Архитектура технологии Carrier Ethernet (CE) позволяет формировать фрагменты сети, как на базе порта, так и на базе виртуальных соединений, что в свою очередь позволяет выделить до восьми видов услуг, которые подробно рассмотрены в [1]. Важным преимуществом технологии CE является наличие механизмов управления OAM (управление, администрирование и поддержка). Сквозное управление отказами достигается путем взаимодействия механизмов стандартов IEEE 802.1ag, IEEE 802.3ah, ITU-T Y.1731 и MEF E-LMI. Стоит отметить, что возможности технологии и перечисленные стандарты накладывают ряд требований в отношении предполагаемой архитектуры системы управления транспортной сетью связи ОАО «РЖД». К таким требованиям в первую очередь относится обеспечение совместимости оборудования по применяемым технологиям и соответствию международным стандартам.

В связи с ростом разнообразия цифрового оборудования, количество контролируемых параметров элементов сети также заметно увеличивается. Таким образом, задача построения системы, позволяющей управлять распределенными объектами с большим набором изменяемых параметров, с учетом изменяющейся архитектуры сети связи, является актуальной. Подходом, позволяющим учесть динамику такого объекта управления, является мультиагентный подход [2, 3]. Физически агенты являются информационной реализацией элементов структуры сети связи, и их поведение

задано алгоритмически с целью совместного достижения целевой функции.

Перспективная структура системы управления транспортной сетью связи представлена на рисунке.

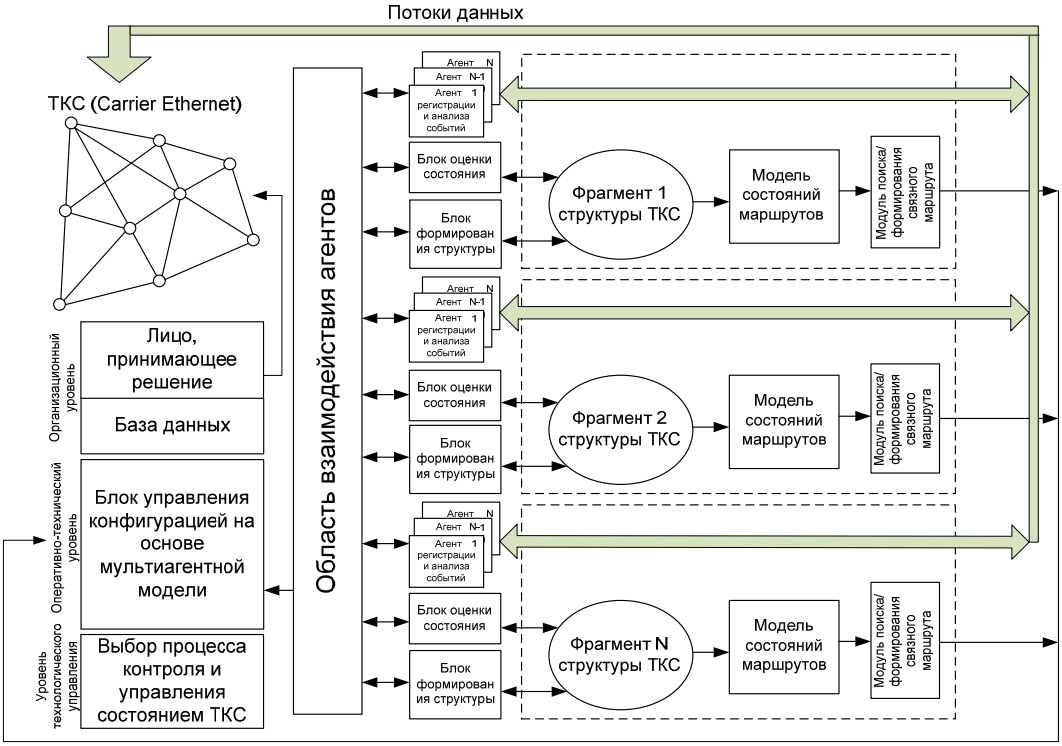


Рисунок. Структура перспективной мультиагентной СУ

Создание мультиагентных систем управления преследует повышение самостоятельности и адаптивности в процессе управления. Это достигается за счет двух ключевых показателей: параллельный процесс принятия решения на выделенных фрагментах и сокращение времени сбора данных управления. На основании этого в структуре перспективной СУ можно выделить следующие подсистемы:

– подсистема сбора и обработки данных выполняет функции контроля и управления состояниями элементов и их параметрами;

– подсистема оценки состояния выполняет функции анализа полученных данных;

– подсистема реконфигурации формирует новые структуры в виде предлагаемого набора решений, обеспечивая тем самым оптимальную фрагментацию ТКС.

Учитывая динамику распределенного объекта управления предпочтительно выделить два режима функционирования системы: основной (без изменений в структуре) и режим актуализации (с учетом изменения в структуре). Таким образом, предполагается, что в структуре системы

управления в роли распределенного объекта управления будет выступать транспортная сеть ОАО «РЖД» на основе технологии Carrier Ethernet. У каждого агента есть доступ к соответствующему фрагменту структуры. Процесс мониторинга структуры ТКС производится непрерывно и параллельно с периодичным анализом параметров состояний элементов.

Вся структура объекта управления делится на фрагменты, управление которыми делегируется узловым агентам верхнего уровня СУ. Для разделения ответственности и простоты управления каждый такой узел СУ содержит три блока управления (см. рис.):

1) Блок регистрации и анализа событий содержит некоторое множество агентов, каждый их которых запрашивает и получает необходимые данные о состоянии непосредственно тех элементов сети, которые входят в данный фрагмент структуры ТКС.

2) Блок оценки состояния на основе полученных данных агентов регистрации и анализа дает комплексную оценку состояния всего фрагмента структуры ТКС.

3) При выявлении отклонений от нормированных значений параметров элементов блок формирования структуры вырабатывает варианты решения для реструктуризации фрагмента ТКС.

Выбор того или иного решения осуществляется или автоматически, например, посредством изменения таблицы маршрутов, или лицом, принимающим решение посредством рабочего персонала. В первом случае, корректность выбора варианта управления будет зависеть от уровня автоматизации внедряемой системы управления и от поддерживаемого протокола резервирования.

Система управления, реализуемая по принципу представленной архитектуры, позволяет повысить оперативность функционирования СУ за счет выбранного объекта управления; упростить процесс реконфигурации за счет выбранного агентного подхода, а использование существующих модулей позволит развивать систему управления ОАО «РЖД» в рамках концепции.

Список используемых источников

1. Бенета Э. В., Канаев А. К. Перспективная телекоммуникационная сеть следующего поколения на основе технологии CARRIER ETHERNET // Бюллетень результатов научных исследований. 2014. № 4. С. 69-75.

2. Бенета Э. В., Канаев А. К., Сахарова М. А. Обоснование выбора типа системы управления телекоммуникационной сетью связи // Бюллетень результатов научных исследований. 2014. № 3 (12). С. 94-101.

3. Канаев А. К., Сахарова М. А., Бенета Э. В. Определение вероятностно-временных характеристик процесса функционирования системы управления сетью передачи данных при поддержании показателей QoS // Интеллектуальные технологии на транспорте. 2015. № 3. С. 30-35.

УДК 654.165

ИССЛЕДОВАНИЕ ПРОЕКТИРОВАНИЯ И СРЕДСТВ ПРОГРАММНО-КОНФИГУРИРУЕМЫХ СЕТЕЙ

Р. В. Арсаев, М. А. Гудков, Д. Д. Корякин, А. Р. Нигаматуллин

Военная академия связи имени Маршала Советского союза С. М. Буденного

Рассматривается технология и основные средства проектирования программно-конфигурируемых сетей на основе протокола OpenFlow.

Стремительное развитие вычислительной производительности, объемов памяти и возможностей высокоскоростной передачи данных привело к необходимости разработки новых технологий построения сетевых инфраструктур.

передача данных, защита информации, сети, Интернет.

В обычном маршрутизаторе Internet одновременно реализуются и управление, и передача данных (рис. 1).

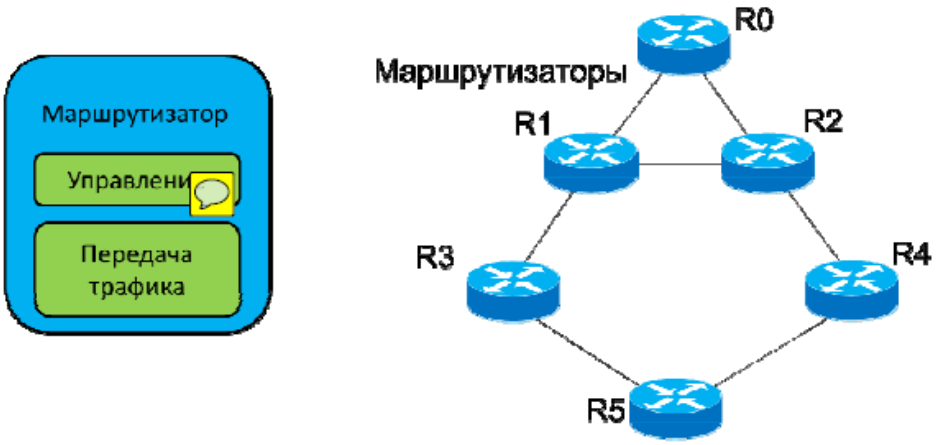


Рис. 1. Представление сети и функций классического маршрутизатора

Уровень управления представлен встроенным контроллером, уровень передачи данных – таблицей коммутации и коммутационной матрицей. Контроллер обладает интеллектуальными функциями, позволяющими ему самому принимать решения о передаче данных на основе информации о структуре сети. Но непосредственно управлять принятием решения нельзя – можно лишь конфигурировать контроллер, задавая определенные наборы правил и приоритетов.

Это значительно ограничивает функциональность коммутатора и всей сети. Проблему разделения уровня управления и передачей данных иссле-

дователи Стэнфорда и Беркли предложили решить в рамках подхода, получившего название программно-конфигурируемые сети (ПКС).

Программно-конфигурируемые сети (*Software Defined Networks*, SDN) – развивающаяся архитектура сети, где функция управления сетью разделена с функцией передачи данных и полностью программируема [1].

Основная идея ПКС состоит в том, чтобы, не изменяя существующего сетевого оборудования отделить управление этим оборудованием (маршрутизаторами и коммутаторами) за счет создания специального программного обеспечения, которое может работать на обычном отдельном компьютере и находится под контролем администратора сети (рис. 2).

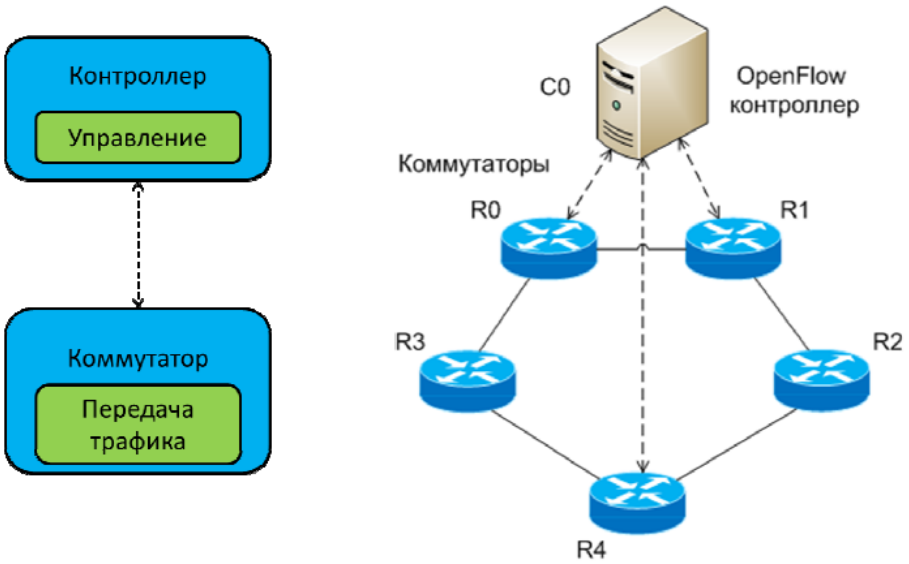


Рис. 2. Представление сети и функций коммутатора с использованием SDN

Теоретически ПКС дает возможность абсолютной гибкости в управлении трафиком, а так же обеспечивает легкую балансировку трафика без задействования отдельного специализированного оборудования. Самым используемым протоколом для поддержания обмена между контроллерами и коммутаторами ПКС является протокол OpenFlow.

Для проектирования и анализа инфраструктуры программноконфигурируемых сетей с поддержкой протокола OpenFlow наиболее часто используют эмулятор MiniNet. Он моделирует компьютерные сети, создавая виртуальные узлы, коммутаторы, контроллеры и каналы связи. Следовательно, топологии, построенные и работающие в MiniNet, могут быть применимы в реальных сетях, состоящих из реальных аппаратных устройств.

MiniNet предоставляет пользователям готовые решения для получения сведений о поведении и производительности ПКС архитектур, реализованных на различных экспериментальных сетевых топологиях. Появляется возможность комплексного тестирования сложных топологий без

запуска физической сети. Эмулятор поддерживает не только базовый набор встроенных топологий, но и произвольные пользовательские топологии. Их создание возможно с помощью сценариев, написанных на языке Python. Так же для программирования контроллеров OpenFlow сетей используют язык Frenetic [2].

Это новый, объектно-ориентированный язык, встроенный в Python, который включает в себя:

1) ограниченный, но высокоуровневый и декларативный язык сетевых запросов;

2) функциональную библиотеку политик управления сети. Frenetic предоставляет программисту интерфейс для классификации сетевого трафика, а так же набор правил фильтрации, группировки и передачи пакетов. Объединяя возможности Python и Frenetic, был создан язык Pyretic [3].

Pyretic одновременно является объектноориентированным языком программирования, встроенным в Python, и системой исполнения, которая реализует программы, написанные на языке Python на сетевых коммутаторах. Он позволяет сетевым программистам и операторам создавать емкие модульные сетевые приложения, предоставляя им мощные абстракции. За счет этого основное внимание уделяется способу задания сетевых политик. Например, с использованием Pyretic программисты могут задать правила передачи трафика в виде компактных абстрактных функций, которые на входе получают пакет, а на выходе возвращают набор новых пакетов.

Pyretic облегчает модульное проектирование за счет использования двух правил взаимодействия операторов: параллельного и последовательного, позволяющих программистам комбинировать множество правил без опасения возникновения конфликта между ними.

Разработчики приложений так же могут создавать динамические правила, которые меняют свое поведение в течение времени. Таким образом, Pyretic предоставляет ПКС-программистам краткий модуль сетевого приложения как абстракцию высокого уровня.

Список используемых источников

1. Software-defined networking: the new norm for Networks, ONF White Paper. April 13, 2012. 12 p. [Электронный ресурс]. URL: https://ru.scribd.com/document/104000608/Software-Defined-Networking-The-New-Norm-for-Networks (дата обращения 12.02.2017).

2. Foster N., Freedman M. J. et al. Languages for software-defined networks, IEEE Communications Magazine. 2013. Vol. 51, Issue 2. pp. 128-134.

3. Reich J., Monsanto C. et al. Modular SDN Programming with Pyretic, USENIX;login: Magazine. Vol. 38, Issue 5. 2013. pp. 128-134.

УДК 004.932.2

ГЕОМЕТРИЧЕСКИЕ ХЕШ-ФУНКЦИИ И ИХ ИСПОЛЬЗОВАНИЕ ДЛЯ ЗАЩИТЫ ИНФОРМАЦИИ

К. А. Ахрамеева, Б. А. Грузинский

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

В статье рассматривается возможность использования методов геометрического хеширования относительно решения задач обеспечения информационной безопасности. Приведены примеры практического применения геометрических хеш-функций в области защиты информации, такие как автоматическая фильтрация интернет-контента, обеспечение объектовой безопасности (анализ кадров видеопотока с целью идентификации объектов), аутентификация по биометрическим данным.

геометрическое хеширование, фильтрация контента, система оповещения, аутентификация.

Геометрическое хеширование изначально было разработано как эффективный метод распознавания объектов в сфере компьютерного зрения. Главной идеей метода является создание базы данных, в которой хранятся характеристики заранее известных объектов, для последующего обращения к этой базе с целью идентификации неопознанных объектов. Основным преимуществом геометрического хеширования является устойчивость к геометрическим изменениям объекта, то есть, возможность корректной идентификации объекта при его частичном скрытии на входном изображении, при различиях в масштабе и угле поворота между тренировочной моделью и входным объектом [1].

Данный метод состоит из двух этапов [2]. На первом этапе характеристики тренировочных объектов анализируются, кодируются при помощи некоторой функции, устойчивой к трансформациям, и сохраняются в базу данных (чаще всего используется хеш-таблица). На втором этапе неизвестный объект анализируется, после чего база данных проверяется на наличие моделей с совпадающими или похожими характеристиками. После этого путём голосования определяется наиболее подходящая из похожих модель.

Можно выделить три ключевых аспекта для работы алгоритма геометрического хеширования:

1. Представление характеристик объекта в виде, инвариантном к геометрическим трансформациям, для последующей идентификации объектов, подвергнутым этим трансформациям.

2. Хранение этих характеристик в хеш-таблице для последующего эффективного извлечения, которое практически не должно зависеть от сложности базы моделей.

3. Схема сравнения, гарантирующая надёжное распознавание даже при незначительном совпадении характеристик и при наличии значительных шумов.

Поскольку изначально эта техника разрабатывалась для нахождения частичных совпадений между кривыми на плоскости, подробнее принцип действия проще всего рассмотреть именно в этом контексте [3]. Подразумевается, что некий набор тренировочных кривых уже был обработан и сохранён в базе данных, и задача заключается в нахождении соответствий между сложной входной кривой и частями кривых, хранящимися в хеш-таблице.

На тренировочном этапе характеристики всех кривых извлекаются, кодируются и сохраняются в базу данных. Каждая кривая сканируется, и из неё извлекаются характеристики в равноудалённых точках кривой. Каждая характеристика получает порядковый номер в зависимости от расположения на кривой. Характеристику выбирают такой, чтобы она не изменялась при движении кривой. Чаще всего используется вторая производная от функции кривой, то есть изменение направления касательной к кривой в каждой точке. Каждая такая характеристика используется как ключ в хеш-таблице, в которую записывается кривая и номер точки на кривой, в которой была сгенерирована эта характеристика. Ожидаемое время выполнения тренировочного этапа линейно зависит от общего количества взятых точек. Поскольку анализ каждой кривой независим от других, процесс анализа можно проводить параллельно.

На этапе распознавания исследуемая кривая сканируется, вычисляются характеристики кривой с теми же параметрами дискретизации, что и тренировочном этапе. Для каждой характеристики находится подходящая запись в хеш-таблице и извлекаются все пары (кривая, порядковый номер), хранящиеся в этой записи. Каждая такая пара считается как один голос за модель соответствующей кривой и за относительный сдвиг между этой кривой и исследуемой. Сдвиг в данном случае является разностью между порядковыми номерами совпадающих точек. То есть, если характеристика i-ой точки в исследуемой кривой достаточно близка к характеристике j-ой точки на модели кривой c, то мы добавляем один голос кривой c с относительным сдвигом $j–i$. Для того, чтобы игнорировать небольшие различия в характеристиках, из хеш-таблицы берётся не только запись с совпадающей характеристикой, но также и соседние записи. Описывае-

мый механизм голосования опирается на предположение, что полные совпадения между длинными участками кривых результируют в большое количество схожестей по характеристикам у модели кривой и исследуемой кривой с одинаковыми сдвигами. Таким образом, к концу голосования определяются те пары (кривая, сдвиг), которые набрали наибольшее количество голосов, и для каждой из этих пар определяются примерные границы совпадающих отрезков на модели и на исследуемой кривой, учитывая при этом сдвиг.

У геометрического хеширования существует множество практических применений в различных сферах. Ключевым элементом для применения геометрического хеширования к любой задаче является подбор подходящей характеристики, наиболее точно выделяющей объект. Область информационной безопасности и смежные области также включают в себя ряд задач, для решения которых целесообразно использовать геометрическое хеширование.

Одной из таких задач является автоматическая фильтрация интернет-контента. В этом случае геометрическое хеширование может применяться для анализа содержимого страницы, поскольку анализа метаданных недостаточно для эффективного категоризирования страниц. Упрощённый алгоритм работы такой системы можно представить следующим образом:

1. На этапе подготовки системы создаётся база данных и заполняется тренировочными данными, полученными из большого набора типичных изображений, присущих веб-сайтам определённых категорий.

2. Для каждой категории настраиваются правила – от самых простых (фильтровать/пропускать) до более сложных, включающих несколько действий. Каждой категории также присваивается вес для этапа голосования – запрещённые категории имеют значительно больший вес, чем остальные.

3. На этапе работы системы исследуемая страница «парсится» программой, из неё извлекаются изображения.

4. Полученные изображения параллельно анализируются на совпадения с объектами тренировочной базы данных. Результатом каждой такой операции является категория, присвоенная конкретному изображению.

5. На основе полученных категорий (а также категорий, полученных на основе анализа текста страницы), осуществляется процесс голосования.

6. Решение записывается в базу данных решений, для страницы применяются заранее настроенные правила.

Основным преимуществом такой системы является невосприимчивость к геометрическим изменениям изображений и другим незначительным изменениям. Попытки «обмануть» алгоритм злоумышленниками не принесут никакого эффекта.

Также геометрическое хеширование находит применение в области объектовой безопасности. Всё большую актуальность приобретает автоматизация анализа данных с камер видеонаблюдения для последующего оповещения о внештатных ситуациях, предотвращения угроз и других целей [4]. В данном контексте геометрическое хеширование также может применяться для анализа кадров видеопотока с целью идентификации определённых объектов. Алгоритм работы с видеоданными можно обобщённо описать в следующем виде:

1. На этапе подготовки системы создаётся база данных и заполняется тренировочными данными, полученными из изображений объектов, которые требуется идентифицировать. Для разных видов объектов возможны различные правила оповещения или иных действий

2. Следует также определиться с частотой, с которой кадры будут анализироваться системой. Это определяется конкретным применением системы и параметрами камер. Например, если кадровая частота видеопотока 30 кадров в секунду, в большинстве случаев не имеет практического смысла анализировать каждый последовательный кадр, поскольку изменения между соседними кадрами незначительны.

3. На этапе работы системы индивидуальные кадры извлекаются из видеопотока с заранее указанной частотой. Изображение сравнивается с моделями объектов из хеш-таблицы, устанавливаются соответствия. Если время анализа индивидуального кадра в конкретной системе больше, чем время между отправкой кадров в систему, следует начать параллельную обработку следующего поступившего кадра для избежания появления очереди. Таким образом, удастся избежать накопления задержки.

4. При обнаружении того или иного объекта срабатывает заранее описанный набор действий (включается система оповещения, отправляется сигнал персоналу и т. д.).

Одно из главных требований к анализу видеоряда, наряду с быстродействием, – это возможность корректно идентифицировать объекты, находящиеся на различном расстоянии от камеры, объекты, повёрнутые к камере под другим углом, а также частично скрытые объекты, что обеспечивается при использовании геометрического хеширования.

Еще один пример применения геометрического хеширования связан с аутентификацией по биометрическим данным. Использование геометрического хеширование в данном случае позволяет значительно повысить качество распознавательного механизма без потерь с точки зрения безопасности. При использовании геометрического хеширования:

1. На этапе подготовки системы база данных заполняется заранее полученными биометрическими данными пользователей (отпечатки пальцев, геометрия руки, геометрия лица и др.) и устанавливаются соответствия между объектами биометрических данных и идентификаторами пользова-

телей в системе контроля и управления доступом или другой системе, для которой используется биометрическая аутентификация.

2. На рабочем этапе изображение, предоставляемое пользователем, сравнивается с объектами тренировочной базы данных, выявляются соответствия. Полученный в результате идентификатор пользователя передаётся в систему контроля и управления доступом или иную систему.

Геометрическое хеширование в биометрической аутентификации позволяет избежать проблемы выравнивания полученного от пользователя изображения перед сравнением с объектом, находящимся в базе данных, что уменьшает число false-negative результатов, не увеличивая число false-positive срабатываний. Кроме того, использование хеш-таблицы и хранение в ней характеристик объектов позволяет значительно сократить требования по объёму памяти для базы биометрических данных. Учитывая, что за последние годы биометрическая аутентификация стала более доступной для персонального использования (биометрические считыватели поставляются с последними моделями определённых смартфонов и ноутбуков, коммерческие сервисы предоставляют возможность биометрической аутентификации для пользователей), а также наличие экспериментальных примеров [5] использования геометрического хеширования в биометрической аутентификации, коммерческая имплементация такой системы крайне актуальна.

Таким образом, геометрическое хеширование – очень гибкий алгоритм, который при корректной адаптации и наличии подробной тренировочной базы можно применить к большому с пектру задач в различных областях информационных технологий, в том числе и к задачам информационной безопасности. Основные преимущества, предоставляемые геометрическим хешированием – это быстродействие, масштабируемость и низкая потребность к объёму хранилища, используемого для работы алгоритма.

Список используемых источников

1. Wolfson H. J., Rigoutsos I. Geometric hashing: An overview // IEEE Comput. Sci. Eng., Oct.-Dec. 1997. Vol. 4. PP. 10-21.

2. Lamdan Y., Wolfson H. J. Geometric Hashing: A General and Efficient Model-Based Recognition Scheme // IEEE Proc. Robotics and Automation. 1988. PP. 238-249.

3. Leondes C. Database and Data Communication Network Systems. Volume 1 // Academic Press, 2002. 952 p. ISBN: 0-12-443896-2.

4. URL: http://news.mit.edu/2012/auto-video-surveillance-algorithm-0605.

5. Lee S., Moon D., Chung Y. Inserting Chaff Minutiae for the Geometric Hashing-based Fuzzy Fingerprint Vault // Journal of Information Science and Engineering. July 2009. Vol. 25. No. 4. PP. 1177-1190.

УДК 654.173

STEGANRTP В IP-ТЕЛЕФОНИИ

К. А. Ахрамеева, С. А. Скородумов

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

В статье рассматривается использование метода цифровой стеганографии SteganRTP в IP-телефонии для просмотра входящего потока, или пересылки RTP пакетов на необходимое устройство, для дальнейшего погружения скрытой информации и ее извлечения. Предоставляется описание программы в нескольких режимах работы, что дает вариативность в использовании данного метода. Приведен анализ достоинств и недостатков метода, а также выявленные особенности и технические требования для использования программы.

цифровая стеганография, IP-телефония, РТП, SteganRTP.

SteganRTP – это метод выборочного вложения скрытых данных, разработанный на основе передачи RTP пакетов для создания скрытой выделенной линии [1]. Метод включает в себя не только правила вложения, но и определенные алгоритмы, включенные в программу, которая позволяет проводить анализ встраивания информации в RTP пакеты, избегая возможного обнаружения.

Программа предоставляет два режима работы. Первый режим (рис. 1) описывается как локально запущенная программа на узле в качестве конечной точки RTP. Второй режим (рис. 2) описывается как запущенная программа на промежуточном узле маршрута от одной RTP точки к другому устройству. Данная реализация позволяет выдать промежуточное устройство за идентичного оконечного пользователя, независимо от режима работа, путем накопления «пользовательского опыта». Вследствие чего путем взаимодействия непосредственно с сетевым стеком легитимной операционной системы будет происходить забор желаемых потоковых пакетов [2].

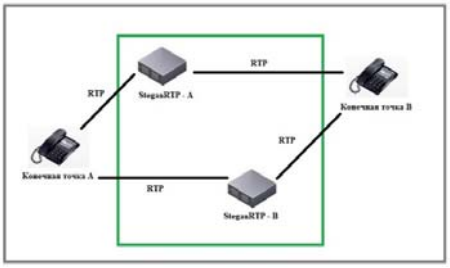


Рис. 1. Локальный режим работы программы

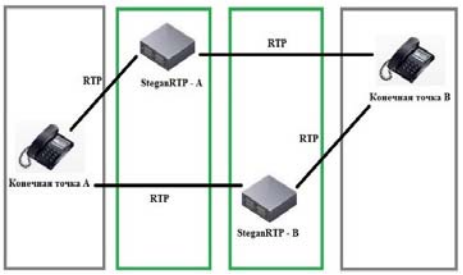


Рис. 2. Режим работы MITM (*Man-In-The-Middle*)

Сначала приложение начинает выполнять инициализацию (рис. 3), путем создания внутренних структур памяти и используя информацию о конфигурации из командной строки. Затем алгоритм переходит к просмотру сетевого трафика, пока не идентифицирует RTP сеанс, ограниченный командной строкой пользователя. Эти ограничения включают в себя контроль и выбор RTP сеансов между конкретными конечными точками пользователя. После идентификации RTP сеанса, приложение SteganRTP подстраивается в сетевой стек хоста, чтобы получить необходимые пакеты по их прибытию. Из сетевого потока приложение считывает и находит необходимые пакеты и перехватывает их. Является ли пакет входящим или исходящим, определяет дальнейший ход приложения. Это определение поступает из того, какой порт конечной RTP точки используется, «локальный» или «удаленный».

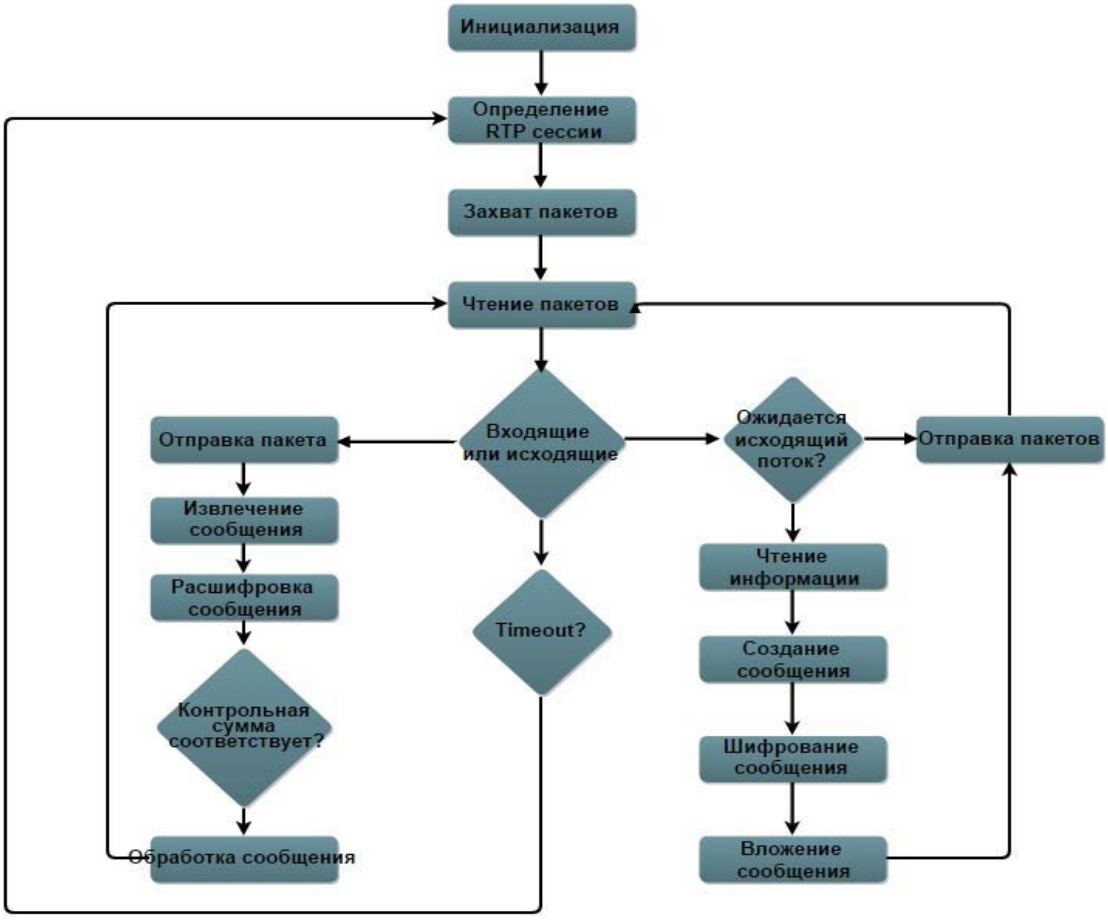


Рис. 3. Алгоритм работы SteganRTP

Когда исходящий RTP пакет считывается, приложение SteganRTP анализирует поток на сообщения, ожидающие немедленной отправки. Если нет такого сообщения, пакет сразу отправляется без изменений. Если такое сообщение есть, оно считывается из файлового дескриптора, упако-

вывается, шифруется, а затем при помощи стеганографии встраивается в поле полезной нагрузки RTP пакета. Измененный RTP пакет затем посылается вместо исходного.

При считывании входящего RTP пакета из потока, он копируется для использования приложением, а исходный пакет немедленно отправляется обратно в поток. Все полученные входящие пакеты считаются потенциально вложенными сообщениями, поэтому эти сообщения затем извлекаются из каждого входящего пакета на приемной стороне. Если контрольная сумма верна, то пакеты отправляются на дальнейшую обработку.

Следующий шаг включает в себя анализ потока на сообщения, ожидающие немедленной отправки. Если нет такого сообщения, пакет сразу отправляется без изменений. Если такое сообщение есть, оно считывается из файлового дескриптора, упаковывается, шифруется, а затем при помощи стеганографии встраивается в поле полезной нагрузки RTP пакета [3]. Измененный RTP пакет затем посылается вместо исходного.

При запуске, приложение SteganRTP сначала инициализирует различные структуры памяти, такие как кэш сообщения, настройки конфигурации и структуру RTP сессии. Наиболее примечательна задача, выполняемая на этапе инициализации – это вычисление ключа, используемого различными компонентами. Метод, выбранный для создания этого ключа, заключается в создании хэш-функции размером 20 байт типа SHA-1, которым пользователь обменивается секретной текстовой строкой. Эта операция нужна для использования ключа в различных компонентах системы SteganRTP, а также этот общий ключ должны получить оба устройства SteganRTP, которые хотят общаться между собой.

Список используемых источников

1. Melina Marcela Pontón Loaiza. Steganography using RTP packets [Электронный ресурс] // MSc. Ethical Hacking & Computer Security. 2013–2014. URL: http://repositorio.educacionsuperior.gob.ec/bitstream/28000/1677/1/T-SENESCYT-00795.pdf (дата обращения 05.03.2017).

2. Real-time Steganography with RTP [Электронный ресурс] / I)ruid, C2ISSP. 2007. URL: http://www.uninformed.org/?v=8&a=3&t=pdf(дата обращения 05.03.2017).

3. Небаева К. А., Скородумов С. А. Стеганография в IP-телефонии и сложности ее реализации // Актуальные проблемы инфотелекоммуникаций в науке и образовании. V Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 3-х т. / Под ред. С. В. Бачевского. СПб.: СПбГУТ, 2016. Т. 1. С. 494-498.

УДК 004.932.2

ИСПОЛЬЗОВАНИЕ ПЕРЦЕПТИВНЫХ ХЭШ–ФУНКЦИЙ ДЛЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

К. А. Ахрамеева, Н. Л. Трескин

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

В статье представлен результат исследования различных типов перцептивных хэш-функций, анализ их практического применения (способность к определению подлинности и схожести различных изображений), а также скорость работы алгоритмов по вычислению перцептивных хеш-функций. Рассмотрены варианты применения перцептивных хеш-функций для усовершенствования современной информационной безопасности, в частности для блокировки нежелательных изображений на сайтах в сети Интернет.

перцептивные хеш-функции, фильтрация контента, дискретно-косинусное преобразование.

Стремительное развитие инфокоммуникационных систем в XXI веке, привело к тому, что пользователи получили возможность обмениваться большим объёмом мультимедийной информации, такими как: видео, гиф-анимации, картинки, аудиофайлы и т. д. В связи с этим возникают следующие проблемы:

1) Размещение большого количества информации на серверах.

2) Контроль данных пользователями (изменение файлов, удаление, сортировка).

3) Безопасность и контроль подлинности.

4) Ограничение передачи информации (борьба со спамом).

Хэш-функция – это некоторый алгоритм, конвертирующий произвольную строку данных в битовую строку определённой длины. Такая строка называется хэшем и чаще всего используется в качестве контрольной суммы.

Отличие перцептивных хэш-функций от криптографических состоит в том, что в случае криптографического хэша можно сделать вывод только об идентичности двух хэшей. В то же время перцептивные хэши дают возможность сравнивать их между собой и делать выводы о схожести и различии данных [1].

В данной работе рассмотрены 3 типа функций:

– низкочастотное хэш преобразование и преобразование по среднему значению;

– хэш на основе гистограммы цветов;

– хэш на основе дискретного косинусного преобразования.

Рассмотрим данные алгоритмы подробнее. Первый – это метод низкочастотного преобразования. Для начала возьмём исходное изображение (рис. 1), уменьшаем его до размера 8×8 (рис. 2). После обесцвечиваем. Из-за этого размер хэша уменьшается втрое, благодаря удалению цветовой составляющей.

Рис. 1. Исходное изображение

Рис. 2. Уменьшенное до 8x8

Далее высчитываем среднее значение из полученных 64 пикселей по формуле:

$$Average = \frac{\sum_{i=1}^{n} v_i}{n}$$

и составляем хэш на основе среднего значения:

$$h_i = \begin{cases} 1, v_i > average; \\ 0, v_i < average. \end{cases}$$

Как видно данный метод очень простой и вследствие этого обладает высокой скоростью действия и устойчивостью к тональному изменению изображения. Для сравнения двух картинок, будет использоваться расстояние Хэмминга, то есть количество разных бит. Следовательно, чем больше количество различных бит, тем менее вероятно, что картинки одинаковы или схожи. Однако такой метод даёт сбои, если выполнялось пространственное изменение изображения, так как этот процесс меняет среднее цветовое значение.

Следующим будет рассмотрен метод построения гистограммы (рис. 3). В основе данного метода лежит создание гистограммы изоб-

ражения, которая представляет собой график статистических данных, по горизонтали которого отложены значения яркости, а по вертикали количество пикселей для данного уровня яркости.

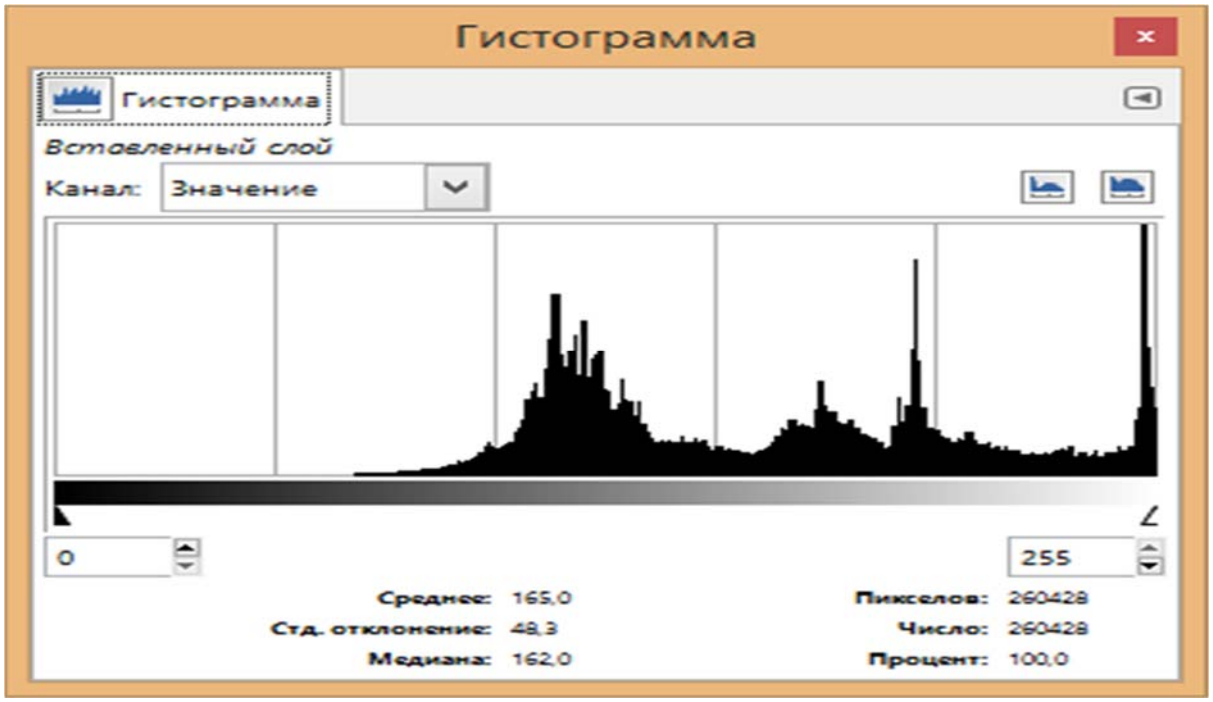


Рис. 3. Гистограмма изображения

Суть алгоритма состоит в сопоставлении гистограмм, чем больше элементов совпадают, тем больше шансов, что это одинаковые изображения, однако хоть данный метод и полностью устойчив к масштабированию, отражению и повороту, его эффективность сильно снижается при использовании изображений схожих цветовых гамм, в следствии чего даёт большое количество ошибочных результатов [2].

Последним рассмотренным будет метод дискретно-косинусного преобразования. Данный метод во многом схож с методом низкочастотной фильтрации и фильтром по среднему значению. Различие заключается в том, что исходное изображения сжимается до размера 32x32 и составляется матрица всех элементов изображения по формуле:

$$X[k] = \sum_{n=0}^{N-1} x[n] * \cos\left(\frac{(2n+1)*k\pi}{2N}\right), k = \overline{0, N-1}.$$

Далее из этой матрицы выбирается матрица 8x8, с которой так же будет проведено сравнение элементов со средним значением. Данный алгоритм является самым вычислительно-сложным из представленных, а также он будет обладать самой большим временем обработки алгоритма из представленных и будет иметь наибольшую устойчивость к различного рода искажениям.

Данные алгоритмы имеют широкий диапазон применения. Самым известным примером является сервис компании “GOOGLE” по поиску схожих изображений, в котором сравниваются перцептивные хэши многих изображений и выводятся наиболее похожие результаты. В плане информационной безопасности самым распространённым применением данных алгоритмов, являются спам фильтры. Спам фильтр работает по тому же принципу, что и сервис поиска картинок, только изображения со схожим хэшем не выводятся, а блокируются. Таким образом, сделав выборку из изображений нежелательного содержания, можно получить некий средний хэш данных изображений и блокировать все изображения, хэши которых в определённой степени с ним совпадают.

При выборе алгоритмов реализации перцептивных хеш-функций необходимо помнить, что:

– Низкочастотное преобразование устойчиво к изменению тонов и гаммы изображения, но очень сильно страдает при пространственных манипуляциях.

– Метод основанный на гистограммах же наоборот устойчив к подобного рода искажениям, но обладает высоким значением ложно подобности и теряет свою эффективность при изменении цветовой составляющей.

– Метод дискретно-косинусного преобразования является самым надёжным, но и одновременно самым вычислительно-ёмким из представленных алгоритмов и так же не способен работать с пространственными коллизиями.

Из этого можно сделать вывод, что ни один алгоритм сам по себе не является универсальным методом определения похожих изображений, вследствии чего следует применять комбинации этих алгоритмов для достижения оптимального уровня надёжности.

Список используемых источников

1. Datta R., Joshi D., Li J., Wang J.Z. Image Retrieval – Ideas, Influences and Trends of the New Age ACM Computing Surveys. 2008. Vol. 40, no. 2. PP. 1-60.

2. Zauner C. Implementation and Benchmarking of Perceptual Image Hash Functions: Ph.D. thesis. University of Applied Sciences, Hagenberg, 2010.

3. Рудаков И. В., Васютович И. М. Исследование перцептивных хеш-функций изображений [Электронный ресурс] // Наука и образование. МГТУ им. Н. Э. Баумана. Электрон. журн. 2015. № 8. С. 269–280.

УДК 517.958:52/59

ИСПОЛЬЗОВАНИЕ MATHCAD ДЛЯ МОДЕЛИРОВАНИЯ ФИЗИЧЕСКИХ ПРОЦЕССОВ В МОБИЛЬНЫХ СРЕДСТВАХ ИНФОРМИРОВАНИЯ И ОПОВЕЩЕНИЯ

Е. С. Бабынин, А. А. Задурова

Санкт-Петербургский университет государственной противопожарной службы МЧС России

Устройства громкоговорителей, установленных на крыше мобильных комплексов оповещения, с помощью которых осуществляется передача аудиоинформации населению, играют очень важную роль в чрезвычайных ситуациях. Моделирование физического процесса колебания металлической диафрагмы в рупорном громкоговорителе с помощью компьютерных систем и рассматривается в данной статье.

рупорный громкоговоритель, компьютерные системы, моделирование, MathCad, уравнение Бесселя, мембрана.

При возникновении чрезвычайной ситуации (ЧС) или угрозы террористических акций ключевую роль играет своевременное оповещение и оперативное информирование граждан, оказавшихся в опасности. Это явилось одной из целей создания «Общероссийской комплексной системы информирования и оповещения населения в местах массового пребывания людей (ОКСИОН)», которая представляет собой организационно-техническую совокупность аппаратно-программных средств обработки, передачи и отображения аудио и видеоинформации.

Существенное расширение функциональных возможностей ОКСИОН было достигнуто путём внедрения мобильных комплексов оповещения (МКО), который позволил решить ряд проблем, связанных с информированием и оповещением в местах, где массовое пребывание населения наблюдается нерегулярно (музыкальные фестивали под открытым небом, многолюдные шествия, спортивные соревнования и т. п.), а также в районах, где отсутствуют стационарные терминальные комплексы ОКСИОН [1, 2].

Фокус внимания сместим на устройство громкоговорителей, установленных на крыше МКО, с помощью которых осуществляется передача аудиоинформации населению.

Рупорный громкоговоритель является средством воспроизведения звукового акустического сигнала в допустимом частотном и динамическом диапазонах.

Характерными особенностями рупора являются обеспечение высокого акустического звукового давления и относительно узкого частотного диапазона.

Рупорный громкоговоритель представляет собой связующий элемент между драйвером (излучателем) и окружающей средой (рис. 1). Драйвер, жестко связанный с рупором, преобразует электрический сигнал в звуковую энергию, поступающую и усиливаемую в рупоре. Специальная геометрическая форма позволяет усилить звуковую энергию внутри рупора, обеспечивая её высокую концентрацию.

Рупор состоит из следующих частей (рис. 1):

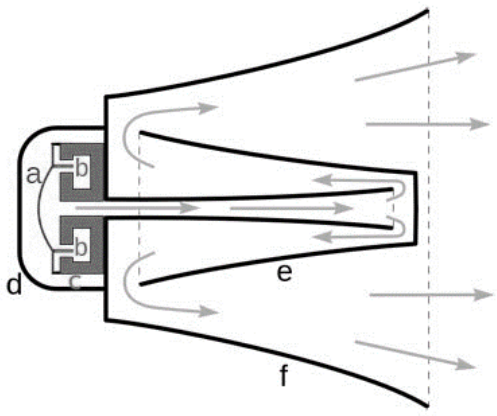


Рис. 1. Устройство рупорного громкоговорителя: a) металлическая диафрагма; b) звуковая катушка или кольцо; c) цилиндрический магнит; d) компрессионный драйвер; e) концентрический канал или выступ; f) рупор или горн

Рупорный громкоговоритель работает следующим образом: электрический звуковой сигнал поступает на вход компрессионного драйвера (d) преобразующего его в акустический сигнал на выходе. Драйвер (жестко) скреплен с горном (f) обеспечивающим высокое звуковое давление. Драйвер состоит из жесткой металлической диафрагмы (a) приводимой в движение (возбуждаемой) звуковой катушкой (витком или кольцом b) намотанной на цилиндрический магнит (c). Звук в данной системе распространяется от драйвера, проходя через концентрический канал (e), экспоненциально усиливается в рупоре (f), после чего поступает на выход.

Для исследования колебания металлической диафрагмы (a) целесообразно использовать компьютерную систему MathCad [3, 4].

Рассмотрим этапы компьютерного моделирования для построения функции, описывающей поверхность мембраны в произвольный момент времени t на платформе MathCad.

1-ый этап – построение функции Бесселя нулевого (J_0) и первого (J_1) порядков (рис. 2).

2-ой этап – нахождение для уравнения Бесселя нулевого порядка первых три корня.

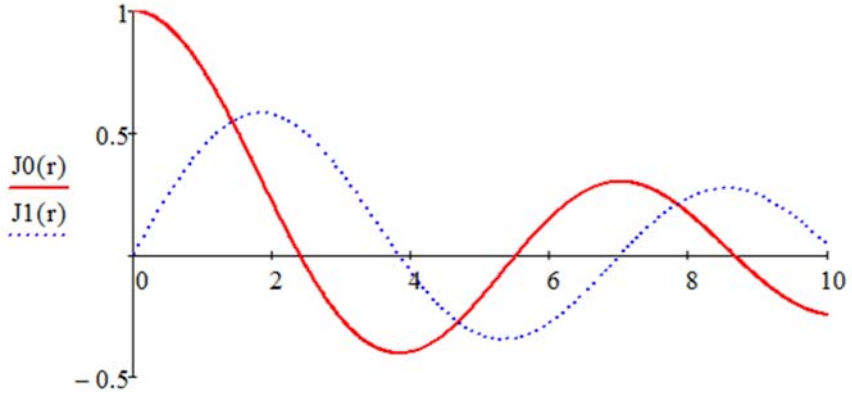


Рис. 2. График функций Бесселя

3-ий этап – нахождение первых трех коэффициентов A_k и B_k для ряда Фурье.

4-ый этап – построение графика поверхности мембраны (рис. 3).

5-ый этап – наблюдение за колебаниями мембраны.

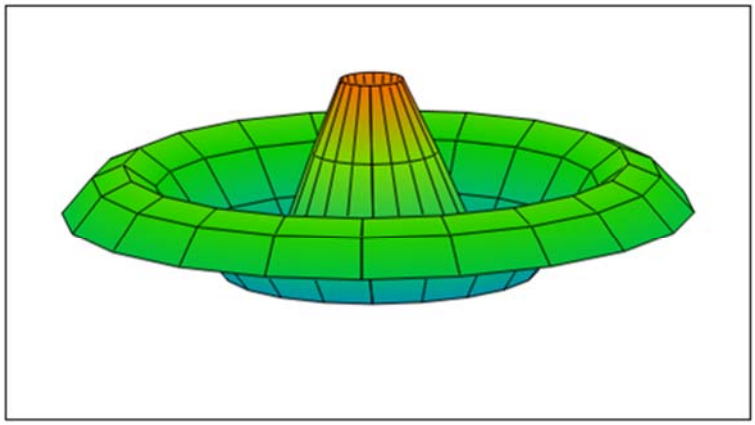


Рис. 3 График поверхности мембраны

Использование компьютерных систем при решении прикладных задач дает возможность наглядно проиллюстрировать протекание физических процессов, увидеть графическую зависимость различных величин, повысить точность получаемого результата, а главное – значительно сократить время его нахождения, что крайне важно в ходе оперативной деятельности МЧС России при возникновении чрезвычайных ситуаций.

Список используемых источников

1. Корольков А. П., Погребов С. А., Саратов Д. Н., Терехин С. Н. Общероссийская комплексная система информирования и оповещения населения в субъектах Россий-

ской Федерации и муниципальных образованиях (ОКСИОН) / Под общей ред. В. С. Артамонова. СПб.: Санкт-Петербургский университет Государственной противопожарной службы МЧС России, 2011. 72 с.

2. Каменецкая Н. В., Медведева О. М., Щётка В. Ф., Хитов С. Б. Применение метода последовательного анализа для моделирования процесса выработки решения в оперативной деятельности МЧС России // Проблемы управления рисками в техносфере. 2016. № 3 (39). С. 73–81.

3. Трофимец В. Я., Трофимец Е. Н. Оптимизация в Excel: учеб. пособие. Ярославль : Ярославский государственный технический университет, 2008. 104 с.

4. Трофимец Е. Н. Информационные технологии математического моделирования в экономических вузах // Образовательные технологии и общество. 2012. Т. 15. № 1. С. 414–423.

Статья представлена научным руководителем, кандидатом педагогических наук, доцентом Е. Н. Трофимец.

УДК 621.375

ИССЛЕДОВАНИЕ ВОЗМОЖНОСТИ ПРИМЕНЕНИЯ ОПТИЧЕСКОГО УСИЛИТЕЛЯ EDFA С УДАЛЕННОЙ НАКАЧКОЙ

М. Белаиди, М. С. Былина

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

В работе представлены результаты исследования возможностей использования оптических усилителей EDFA на основе волокон, легированных ионами эрбия, с удаленной накачкой. Исследование проводилось с помощью программы GainMaster, моделирующей работу EDFA.

оптический усилитель, волокно, легированное ионами эрбия, EDF, EDFA, коэффициент усиления.

Оптические усилители (ОУ), создаваемые на основе активного оптического волокна (АОВ), легированного ионами эрбия, (*Erbium Doped Fiber Amplifier* – EDFA) широко используются в современных волоконно-оптических системах передачи.

Принцип работы ОУ EDFA описывается двухуровневой квантовой системой, в соответствии с которой ион эрбия в АОВ в каждый момент времени может находиться на одном из двух энергетических уровней с энергиями $W_2 > W_1$. Концентрация N_i ионов, находящихся на i-ом уровне,

называется населенностью *i*-го уровня. Накачка ОУ EDFA осуществляется оптическим излучением. В результате поглощения фотонов накачки ионы эрбия переходят с основного уровня 1 на метастабильный уровень 2. При достаточной мощности накачки можно добиться инверсной населенности уровней ($N_2 > N_1$), создающей условия для усиления сигнала, фотоны которого могут вызывать вынужденные излучательные переходы ионов эрбия с уровня 2 на уровень 1 [1].

Находят применение ОУ EDFA с попутной, встречной и двунаправленной накачками (рис. 1) на длинах волн 980 и 1480 нм. Для объединения сигнала и накачки в АОВ используют мультиплексоры спектрального уплотнения (Wavelength Division Multiplexer – WDM).

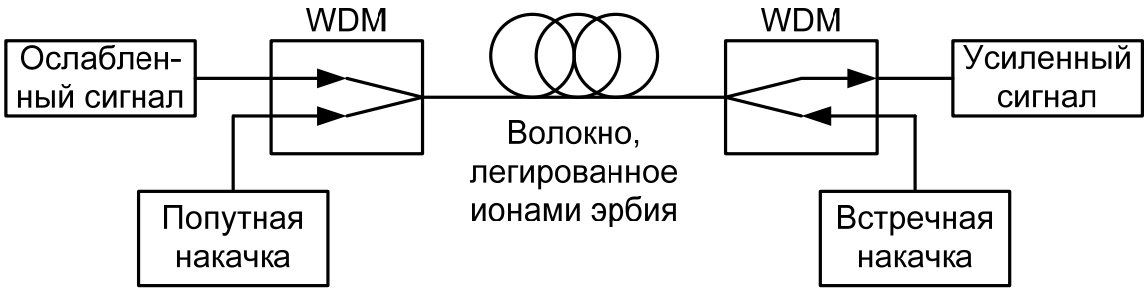


Рис. 1. Структурная схема ОУ EDFA

В протяженных ВОСС линейные ОУ могут устанавливаться в необслуживаемых усилительных пунктах, удаленных от источников энергии. Традиционный способ обеспечения ОУ электропитанием заключается в организации дистанционного питания по металлическим жилам, включаемым в конструкцию оптического кабеля. В [2] рассматривается альтернативный способ – применение ОУ с удаленной накачкой (ROPA – *Remote Optical Pumped Amplifier*). В ROPA источник накачки выносится за пределы конструкции усилителя и устанавливается в оконечном или промежуточном регенерационном пункте, имеющем источник энергии. Излучение источника накачки подводится к усилителю по одномодовому оптическому волокну. Основным достоинством данного способа является повышение надежности необслуживаемых ОУ, которые в этом случае содержат только пассивные компоненты, а недостатком – необходимость использования источников накачки существенно большей мощности.

Целью работы является исследование возможности создания и применения линейных ОУ EDFA с удаленной накачкой.

В первой части работы исследованы ОУ EDFA на основе АОВ IsoGain™, производства Fibercore. Параметры АОВ марок I-4, I-6 и I-25 семейства IsoGain™, отличающихся концентрацией ионов эрбия, представлены в таблице 1.

ТАБЛИЦА 1. Параметры волокон IsoGain™

Марка волокна	I-4	I-6	I-25
Коэффициент поглощения на длине волны 1532 нм, дБ/м	5,0–6,7	7,2–8,4	35–45
Диаметр модового поля на длине волны 1550 нм, мкм	5,4–6,6	5,5–6,3	5,2–6,3
Предназначено для усилителей, работающих в диапазоне	*C*	*C*	*C* и *L*

Исследование ОУ EDFA в работе осуществлялось с помощью моделирующего работу EDFA свободно распространяемого программного обеспечения GainMaster, разработанного компанией Fibercore [2]. На рис. 2 и 3 представлены результаты расчетов зависимости коэффициента усиления *G* ОУ EDFA от длины АОВ для разных схем накачки. Из рисунка видно, что для каждого значения мощности накачки существует эффективная длина АОВ l_{eff}, при которой коэффициент усиления *G* максимален. Видно также, что увеличение мощности источников накачки приводит к возрастанию *G* и l_{eff}. Расчеты показали, что максимальное достижимое значение коэффициента усиления для обеих марок волокна примерно одинаково, а эффективная длина АОВ I-25 с более высокой концентрацией ионов эрбия существенно меньше, чем I-6.

По графикам на рис. 2 и 3 можно определить необходимую мощность накачки на входе мультиплексора WDM в ОУ EDFA для получения заданного коэффициента усиления.

Во второй части работы исследовались процессы распространения излучения накачки по одномодовому кварцевому оптическому волокну (ОВ).

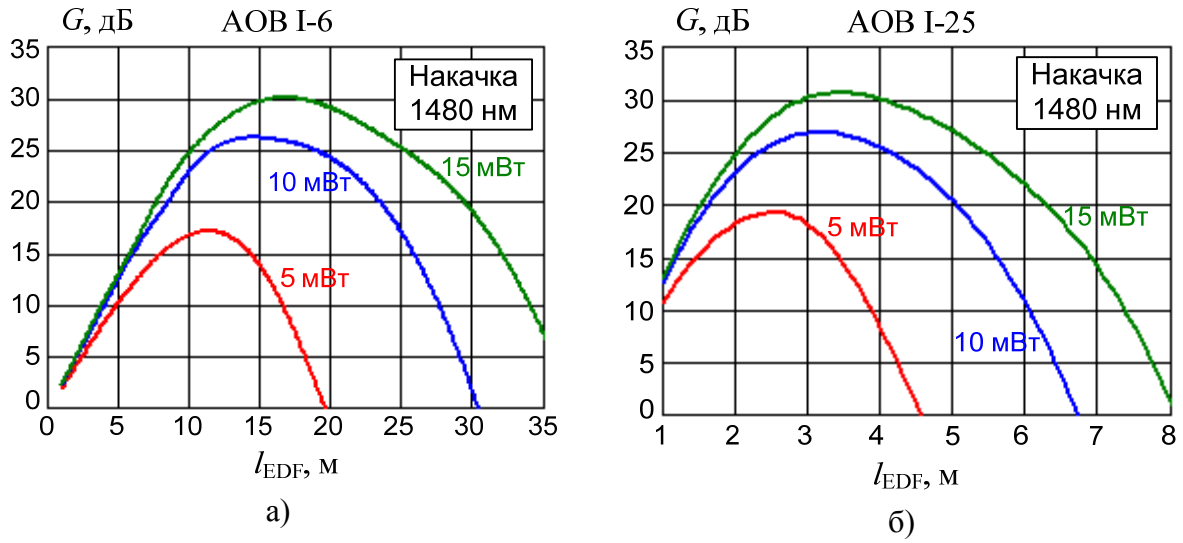


Рис. 2. Зависимости коэффициента усиления ОУ EDFA от длины АОВ I-6 (а) и I-25 (б) для схем с попутной или встречной накачкой мощностью 5, 10 и 15 мВт

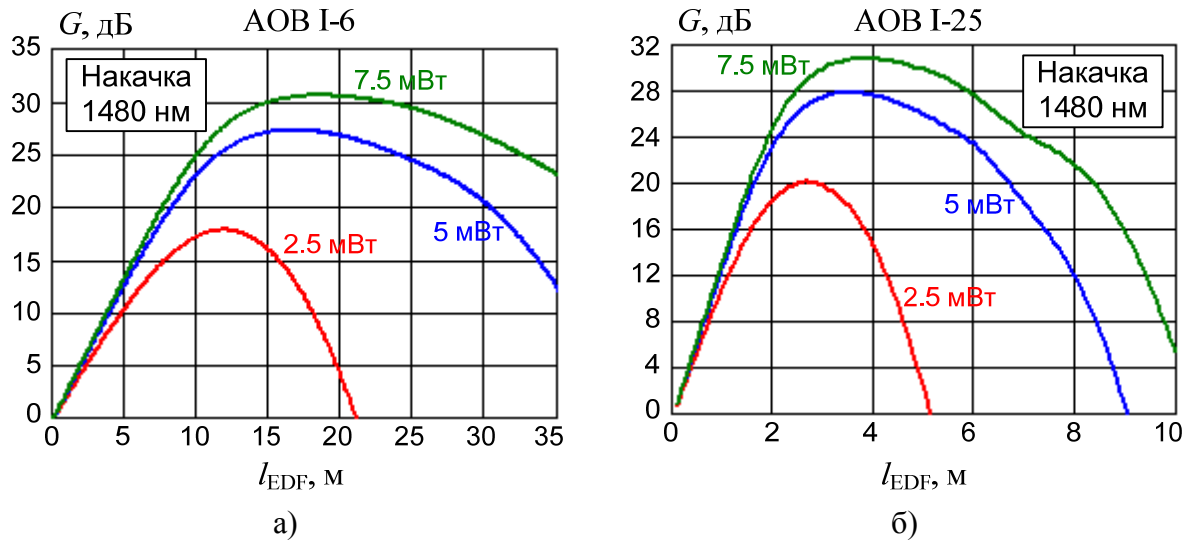


Рис. 3. Зависимости коэффициента усиления ОУ EDFA от длины AOB I-6 (а) и I-25 (б) для схемы с двунаправленной накачкой, полученные при одинаковых мощностях встречной и попутной накачек, равных 2,5, 5 и 7,5 мВт

Известно, что коэффициент затухания α в ОВ сложным образом зависит от длины волны λ, что обусловлено двумя протекающими в ОВ физическими процессами, которые приводят к потерям распространяющегося излучения – релеевским рассеянием и поглощением. Зависимости коэффициентов затухания, обусловленных рассеянием α_{rr} и поглощением α_a, от длины волны для стандартного ОВ может быть рассчитана по известным выражениям:

$$\alpha_{rr}(\lambda)=\chi\lambda^{-4},\ \alpha_a(\lambda)=\sum_{i=1}^{N}\alpha_{ai}(\lambda)\ \ \alpha_{ai}(\lambda)=\frac{\Delta\lambda_i\cdot g_i}{2\pi\left[(\lambda-\lambda_{0i})^2+(\Delta\lambda_i/2)^2\right]},$$

где χ – коэффициент рассеяния, равный 0,85 дБ·мкм^4/км [4]; N – число пиков поглощения, принятое равным 3; α_{ai} – коэффициент затухания, обусловленный i-ым пиком поглощения; λ_{0i}, g_i, $\Delta\lambda_i$ – длина волны, амплитуда и ширина i-го пика поглощения. Параметры пиков поглощения представлены в таблице 2.

ТАБЛИЦА 2. Параметры пиков поглощения в стандартном ОВ

Параметр \ Пик поглощения	1	2	3
Центральная длина волны пика поглощения λ_0, нм	1290	1383	1800
Ширина пика поглощения $\Delta\lambda$, нм	30	30	1
Амплитуда пика поглощения g, дБ·нм/км	2	10	2000

Общий коэффициент затухания ОВ может быть рассчитан по выражению:

$$\alpha(\lambda) = \alpha_{rr}(\lambda) + \alpha_a(\lambda).$$

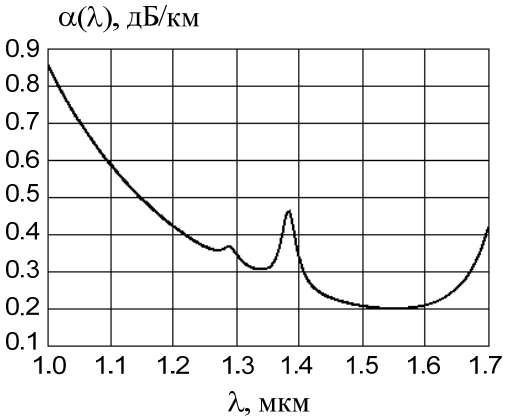


Рис. 4. Зависимость коэффициента затухания в стандартном ОВ от длины волны

Результаты расчета α(λ) представлены на рис. 4.

Из рис. 4 и формулы (1) следует, что на длинах волн накачки 980 и 1480 нм и сигнала 1550 нм коэффициент затухания кварцевого волокна составляет 0,927, 0,213 и 0,2 дБ/км соответственно. Таким образом, для удаленной накачки целесообразно использовать источник с длиной волны 1480 нм, на которой коэффициент затухания меньше.

В третьей части работы рассмотрена волоконно-оптическая система передачи (ВОСП) с одним линейным ОУ EDFA с удаленной накачкой (рис. 5).

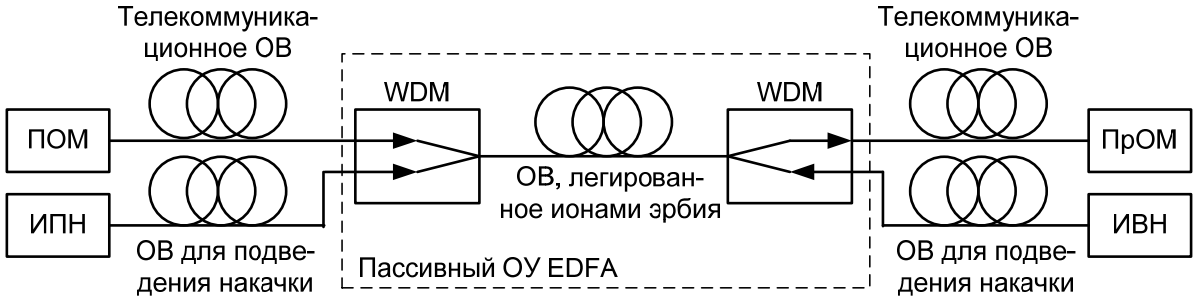


Рис. 5. ВОСП с линейным ОУ EDFA с удаленной накачкой:
ПОМ и ПрОМ – передающий и приемный оптические модули,
ИПН и ИВН – источники попутной и встречной накачек

Предположим, что усилитель полностью компенсирует затухание сигнала в телекоммуникационном ОВ на участке от ПОМ до ОУ. Значит его коэффициент усиления должен быть равен:

$$G = \alpha(\lambda_s)L, \qquad (1)$$

где λ_s – длина волны сигнала, L – длина телекоммуникационного ОВ. Таким образом, при L = 100 км ОУ должен иметь G = 20 дБ. Из рис. 2 следует, что для достижения такого коэффициента усиления при мощности попутной или встречной накачки 10 дБм, необходимо АОВ I-6 длиной 8,5 м или I-25 длиной 1,7 м.

На рис. 6 показаны результаты расчетов зависимости необходимого уровня мощности ИПН и ИВН p_p от L при различных значениях мощности накачки на входах мультиплексоров WDM.

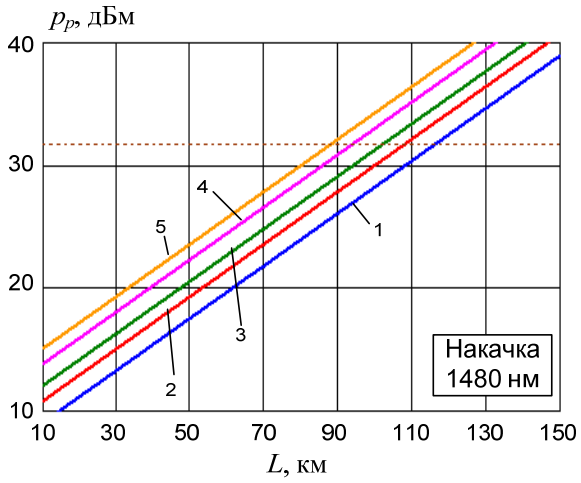


Рис. 6. Зависимость p_p от L при мощности накачки на входе мультиплексора WDM: 1 – 5 мВт, 2 – 7.5 мВт, 3 – 10 мВт, 4 – 15 мВт, 5 – 20 мВт.

Пунктирной линией показано пороговое значение накачки, при котором в подводящем ОВ возникает нелинейное рассеяние Рамана. Поэтому длина подводящего ОВ ограничивается сверху значением L_{max}, которое для представленных на рис. 6 графиков составляет от 88 км (при мощности накачки на входе мультиплексора WDM 20 мВт) до 116 км (при мощности накачки на входе мультиплексора WDM 5 мВт).

Список используемых источников

1. Becker P. C., Olsson N. A., Simpson J .R. Erbium-Doped fiber amplifiers. Fundamentals and Technology. Academic Press, 1999. 480 p.

2. Листвин В. Н., Трещиков В. Н. DWDM системы: научное издание. М. : Издательский дом «Наука», 2013. 300 с.

3. GainMaster: Amplifier Design Software Manual [Электронный ресурс] // Fibercore Limited, 2004. URL: http://fibercore.com/product/gainmaster-simulation-tool (дата обращения 01.06.2017).

4. Листвин А. В., Листвин В. Н., Швырков Д. В. Оптические волокна для линий связи. М.: ЛЕСАРарт, 2003. 288 с.

УДК 654.739

ОТТ 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.

LTE, CS Fallback, IMS, OTT.

На сегодняшний день стоит остро проблема передачи голоса в сетях четвертого поколения LTE. Было придумано несколько решений этой проблемы, но наиболее удачные из них – это процедура CS Fallback и платформа IMS [1].

Изначально было введено решение CS Fallback как наиболее простое в исполнении. Суть данного решения заключается в том, чтобы организовать перевод вызова на сеть 3G или 2G. Оно не требует больших материальных вложений и сильной модернизации сети. Все, что нужно – это соединить MME (*Mobility Management Entity*) и MSC (*Mobile Switching Center*) для передачи сигнального трафика при передаче вызова на сети предыдущих поколений.

К появлению сетей четвертого поколения уже существовало решение для передачи голоса в пакетных сетях для мобильных пользователей – IMS (IP *Multimedia Subsystem*). Но внедрение данной платформы откладывалось не только из-за дороговизны, но и абонентские терминалы не поддерживали данное нововведение.

В наше время операторы связи, в том числе и российские, активно запускают IMS в своих сетях. Платформа IMS позволяет предоставлять пользователям больше услуг по сравнению с предыдущими поколениями связи. Самым же главным преимуществом является гарантия качества передачи голосового трафика. Но платформа IMS на сегодняшний день попрежнему является не самой дешевой вещью для операторов мобильной связи, и это замедляет ей внедрение.

Ниже в таблице будут приведены основные плюсы и минусы обоих решений для передачи голоса, которые может предоставить оператор на сегодняшний день.

Помимо возможностей передачи голоса, которые предоставляет оператор связи, все больше давят на рынок телекоммуникаций OTT услуги.

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.

ТАБЛИЦА. Сравнение двух решений для передачи голоса

CS Fallback	IMS
Плюсы	
Возможность передачи голоса без глобального изменения сети	Высокое качество голоса
Качество связи	Повышение скорости соединения
Гарантируемая пропускная способность	Повышение емкости сотовых сетей
	Возможность одновременной передачи данных и голоса
Минусы	
Требуется модернизация MME и MSC	Высокие затраты на установку IMS платформы
Требуется перекрытие зон GERAN/UTRAN и E-UTRAN	Малое количество устройств с поддержкой данной функции
Увеличение задержки при установлении голосового соединения	Отсутствие качественного LTE покрытия
	Трудности перехода на сети

Но, как и во всех услугах для передачи голоса, есть некоторые проблемы при использовании [2]:

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

Помимо минусов, которые несут OTT услуги для конечных пользователей, операторы связи недосчитываются своей прибыли. С каждым годом доля OTT услуг на рынке телекоммуникаций растет. Особенно быстро этот рост ощущается с 2015 г. Из доклада ITU [3], доходы OTT провайдеров могут превысить доходы телекоммуникационных компаний к 2021 г. Следовательно, в идентификации и контроле за OTT услугами должны быть заинтересованы и операторы связи.

На следующих рис. 1 и 2 изображены данные, предоставленные ITU, которые связаны ростом доли OTT услуг на рынке телекоммуникаций. На рис. 1 изображен график предполагаемых доходов операторов связи и провайдеров OTT услуг до 2021 г. Именно к этому году возможно превосходство доходов OTT услуг над услугами операторов связи.

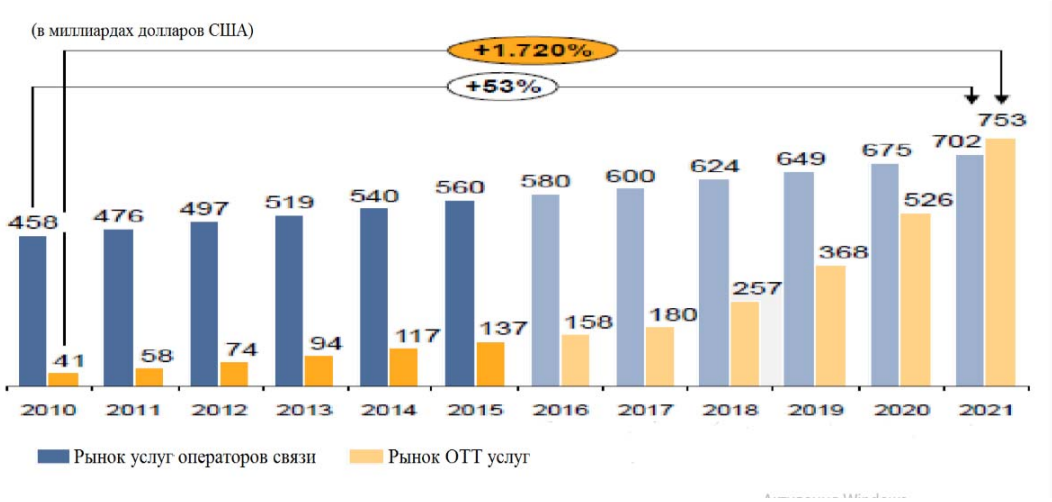


Рис. 1. Развитие рынка операторов связи и OTT услуг

На рис. 2 представлен график недобор прибыли операторов связи из-за OTT услуг, связанных с голосом. К 2016 г. операторы связи могли недосчитать 50 миллионов долларов США, что составляет 7 % от прибыли голосового трафика. И данный показатель будет расти с каждым годом.

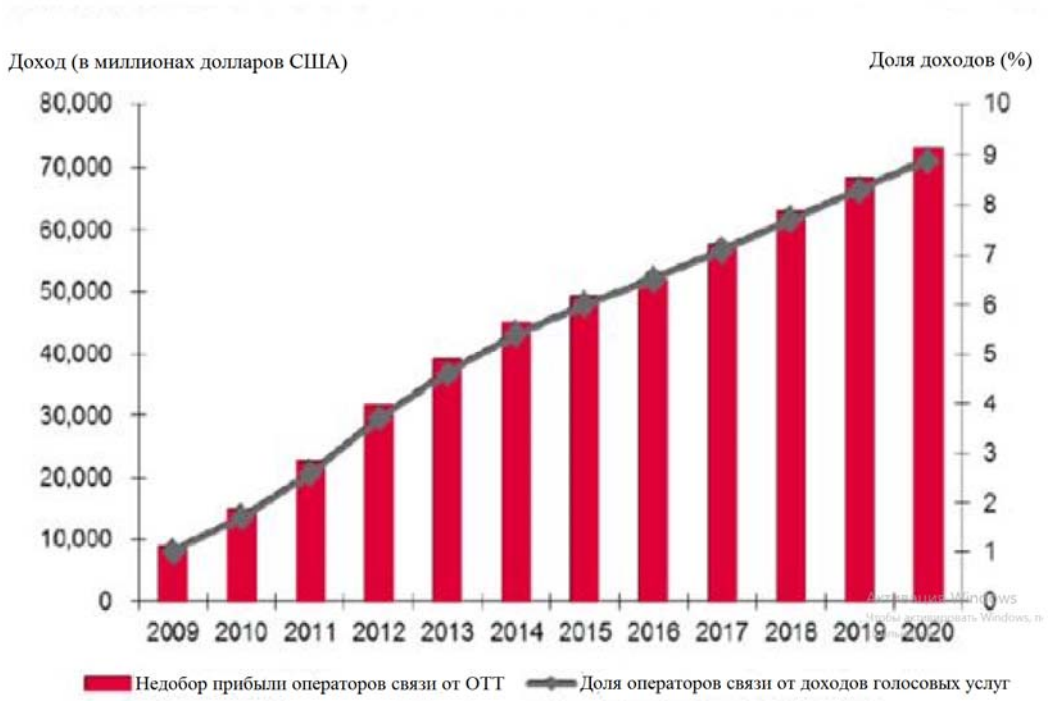


Рис. 2. Недобор прибыли операторов связи

Чтобы быть более наглядным, 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. На рис. 3 представлена схема для измерения основных характеристик качества связи.

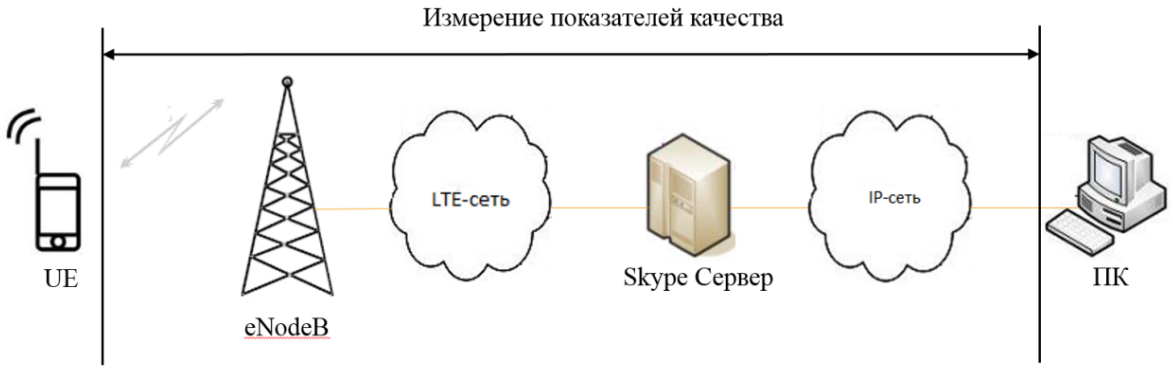


Рис. 3. Установка для измерения показателей качества

Ниже (рис. 4–6) приведены результаты измерений.

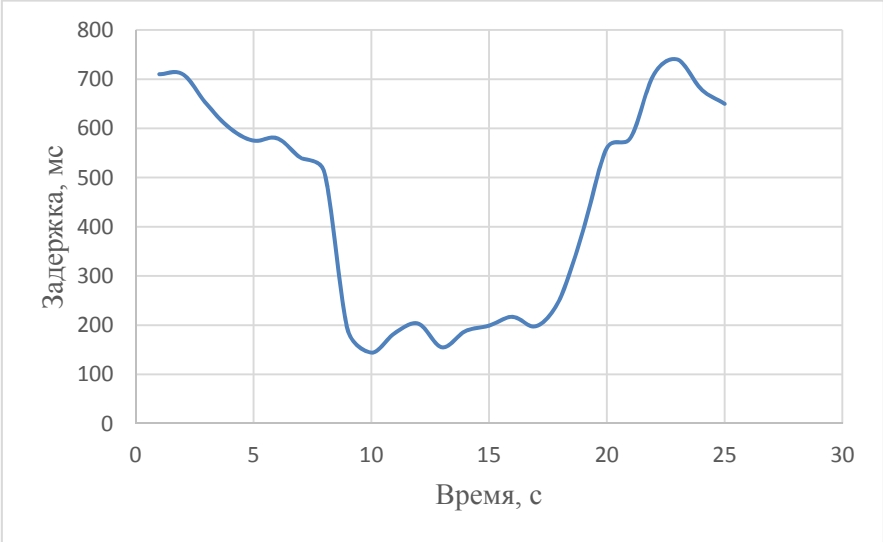


Рис. 4. Показатели задержки

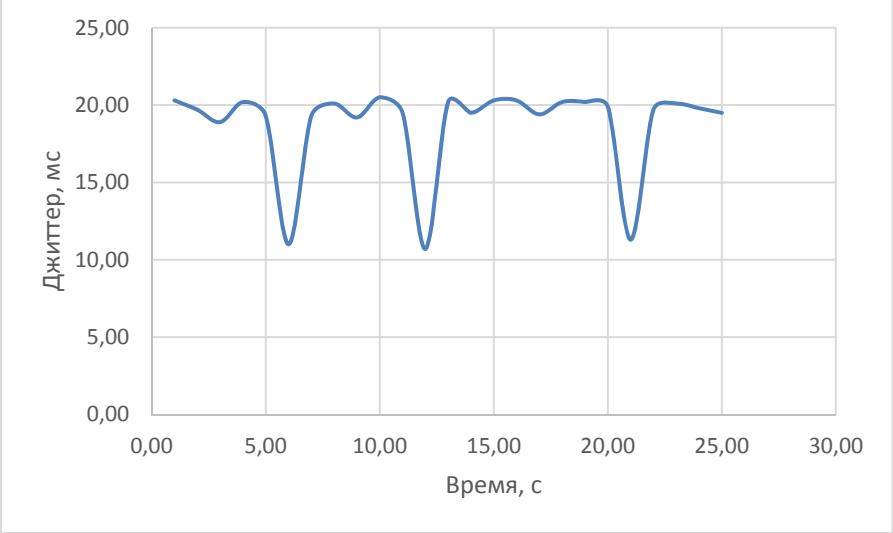


Рис. 5. Показатели джиттера

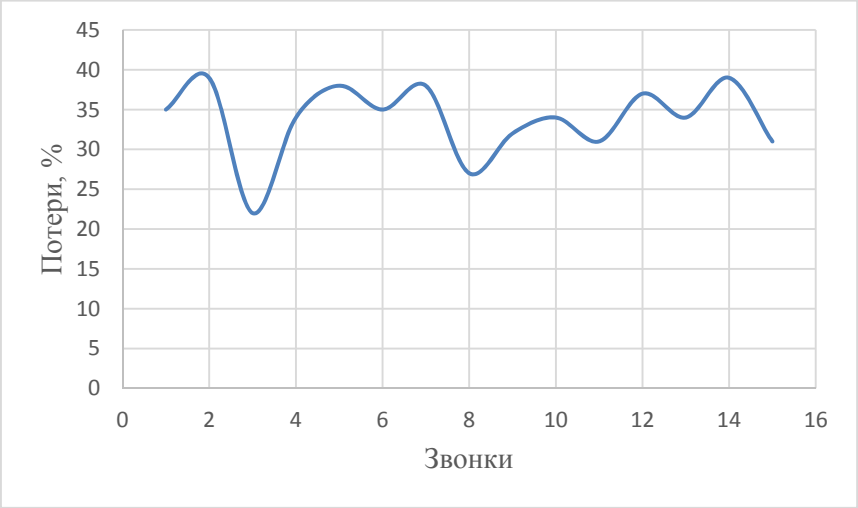


Рис. 6. Показатели потерь

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.

Список используемых источников

1. Cox C. An introduction to LTE: LTE, LTE-advanced, SAE and 4G mobile communications. West Sussex, UK: John Wiley and Sons Ltd, 2012. 352 p. ISBN 978-1-119-97038-5

2. Кущ И. «Голос» в LTE: Российская реальность [Электронный ресурс]. Дата публикации: 23.01.2015. URL: http://nag.ru/go/text/26801/ (дата обращения 31.10.2016).

3. Mnakri M. Over-The-Top Services: Enablers of Growth and Impacts on Economies. ITU, 2015.

УДК 004.056

ЗАЩИТА ИНФОРМАЦИИ В БАЗАХ ДАННЫХ

Э. В. Бирих, Л. А Виткова, В. В Гореленко, Д. Б. Казаков

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

Одним из самых эффективных способов хранения и работы с большим объемом информации являются базы данных. Широкая популяризация применения данной технологии ставит актуальность проблем безопасности информационных ресурсов, которые использует база даных, на достаточно высокий уровень. Для поддержания конфиденциальности информации, хранящейся в базе данных, существует ряд средств. В данной статье автором рассмотрены данные средства защиты информации (основные и дополнительные).

СУБД, SQL, угроза, права доступа, шифрование, пароль, метки безопасности.

База данных (БД) используются в большинстве организаций и хранят в себе различного рода информацию, в том числе конфиденциальную. Вследствие чего актуальность защиты от угроз безопасности баз данных является одной из первостепенных задач на предприятии.

Базы данных размещаются на локальной машине пользователя или на специально выделенной ЭВМ (сервере).

В вычислительных сетях базы данных размещаются на серверах. В локальных и корпоративных сетях, как правило, используются централизованные базы данных. Общедоступные глобальные сети имеют распределенные базы данных. В таких сетях серверы размещаются на различных объектах сети. В качестве серверов часто используются специализированные ЭВМ, приспособленные к хранению больших объемов данных, обеспечивающие сохранность и доступность информации, а также оперативность обработки поступающих запросов. В централизованных базах данных проще решаются проблемы защиты информации от преднамеренных угроз, поддержания актуальности и непротиворечивости данных. Достоинством распределенных баз данных, при условии дублирования данных, является их высокая защищенность от стихийных бедствий, аварий, сбоев технических средств, а также диверсий [1].

Для работы с базами данных используют систему управления базами данных (СУБД). СУБД – совокупность программных и лингвистических средств общего или специального назначения, обеспечивающих управление созданием и использованием баз данных [2]. Большинство СУБД со-

зданы для реляционных баз данных и используют язык SQL, так как он удобен для описания логических подмножеств БД.

Для системы управления базы данных важны три основных аспекта информационной безопасности – конфиденциальность, целостность и доступность.

Прежде чем перейти к методам защиты, рассмотрим кто из пользователей взаимодействует с СУБД.

Пользователи СУБД разделяются на три группы:

1. Прикладной программист (работает над созданием программ, использующих базу данных).

2. Конечный пользователь (работает с СУБД).

3. Администратор (является лицом осуществляющим контроль за функционированием СУБД) [3].

Непосредственно за сохранность информации, хранящейся в БД, отвечает администратор баз данных. Для этого используется ряд средств, описанных ниже.

К основным средствам защиты информации можно отнести:

1. Защита с помощью пароля.

2. Шифрование.

3. Установление прав доступа к объектам БД.

4. Защита полей и записей таблиц БД.

5. Резервирование БД.

Использование защиты с помощью пароля подразумевает применение определенного кодового слова для входа в систему управления баз данных. Ключевое слово может быть, как единое для всех пользователей, так и различаться в случаи применения различных полномочий относящихся к определенным типам пользователей.

Для обеспечения защиты информации в базах данных применяется несколько типов шифрования данных. Одним из них является прозрачное шифрование, которое подразумевает использование шифрование при вводе-выводе файлов БД. Помимо этого, применяется зашифровка на уровне столбцов, что обеспечивает более глубокую защиту. Наиболее гибким подходом является шифрование на уровне приложений. Данный подход обеспечивает запись в базу данных уже зашифрованных файлов, что существенно осложняет кражу конфиденциальной информации.

При использовании разграничений прав доступа к объектам БД возможно применение дискреционного и мандатного управления доступом. В случаи дискреционного управления доступом субъекты получает права к объектам на основе списков управления доступом или матрицы доступа [4]. Уязвимость данного подхода заключается в том, что доступ ограничивается только к именованным объектам, а не собственно к хранящимся данным. Использование мандатной защиты решает данную проблему,

так как разграничение доступа субъектов к объектам, основано на назначении метки конфиденциальности для информации, содержащейся в объектах, и выдаче официальных разрешений (допуска) субъектам на обращение к информации такого уровня конфиденциальности.

Защита данных в полях таблиц осуществляется путем разграничения уровней прав доступа (полный запрет, только чтение, разрешение всех операций).

Посредством резервного копирования возможен процесс восстановление базы данных при различного рода случаях, что является защитой данных на физическом уровне.

Помимо основных средств защиты информации в базах данных существую дополнительные. Применение данных средств является, как правило, привязано к отдельно разработанной системе безопасности.

Одним из подобных средств является ограничение числа возможных подключений к базе данных. Данная процедура подразумевает установление максимального числа одновременно работающих с базой данных пользователей и отсеивания всех лишних.

Для предотвращения входа в СУБД нелегитимных пользователей возможно применение усложнение подбора пароля. Для этого используется ограничение времени для аунтификации, установление конкретного формата имени пользователя, а также зависимость от регистра.

Средства повышения достоверности вводимых данных, такие как шаблоны или ограничения на максимальные и минимальные значения, также являются способом защиты данных в БД. В более продвинутых системах используются хранимые процедуры, которые представляют собой программы, алгоритмы которых предусматривают выполнение некоторых функций (в том числе контрольных) над данными.

В распределенных информационных системах, работающих с базами данных, возникает проблема разрешения конфликтов между различными действиями над одними и теми же объектами БД. Для организации совместного использования объектов БД в сети используются блокировки, которые возникают при параллельной попытке входа в режим разработки этих объектов.

Одним из организационных моментов является предотвращение доступа к физическим носителям информации. Данное мероприятие позволит защитить информацию от выноса за пределы контролируемой зоны и предотвратит установку на рабочей станции постороннего ПО [5].

В случаи использования распределенных корпоративных систем, работающих с СУБД, необходимо применять шифрование канала передачи данных, что обеспечит сохранность данных на пути между этими системами.

В заключении стоит отметить, что придерживаясь данным рекомендациям при построении и обслуживании базы данных, возможно, обеспечить должную защиту по всем трем аспектам информационной безопасности – конфиденциальности, целостности и доступности.

Список используемых источников

1. Завгородний В. И. Комплексная защита информации в компьютерных системах. М. : Логос, 2001. 204 с.

2. Карпова Т. С. Базы данных: модели, разработка, реализация. СПб. : Питер, 2002. 304 с.

3. Козленко Л. Х. Информационная безопасность в современных системах управления базами данных [Электронный ресурс] // КомпьютерПресс: электрон. науч. журн. 2002. N 3.URL: http://compress.ru/article.aspx?id=10099 (дата обращения 25.02.2017).

4. Андрианов В. И., Красов А. В., Липатников В. А. Инновационное управление рисками информационной безопасности : учебное пособие // Федер. агентство связи, С.-Петерб. гос. ун-т телекоммуникаций им. М. А. Бонч-Бруевича. СПб. : СПбГУТ, 2012. 396 с. ISBN: 978-5-91891-092-4.

5. Бирих Э. В., Сахаров Д. В. Модель нарушителя распределенной информационно-вычислительной сети // Актуальные проблемы инфотелекоммуникаций в науке и образовании. V Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 3-х т. СПб. : СПбГУТ, 2016. Т. 1. С. 235–238.

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

УДК 004.056.2

РАЗВИТИЕ СТАНДАРТОВ И РУКОВОДСТВ В СФЕРЕ ОБЛАЧНЫХ ТЕХНОЛОГИЙ

Э. В. Бирих, Л. А. Виткова, М. В. Левин, М. В. Чмутов

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

По всему миру происходит активное развитие облачных вычислений и документов по их реализации. Изучение и использование международных стандартов и руководств в этой области позволит сократить сроки разработки отечественных документов и повысить их качество. Облачные ресурсы и технологии имеют большой потенциал, но при их применении можно столкнуться с рядом проблем, которые авторы исследуют в своей работе.

Облачные ресурсы, облачные вычисления, информационная безопасность, интероперабельность.

Для широкого и эффективного внедрения технологий нужны методические и нормативные документы, разъясняющие, правовые рамки применения этих технологий, имеющиеся проблемы и риски и способы их минимизации. Еще 5 лет назад стандарты, применяющиеся к облачным вычислениям, были разработаны для «дооблачных» технологий, таких как веб-сервисы и Интернет. Происходила активная разработка стандартов и руководств, предназначенных именно для облачных вычислений [1, 2].

Создание нормативно-методической базы начинается с разработки методических документов на национальном уровне, после национальных стандартов появляются международные. В данной статье описаны международные стандарты Международной организации по стандартизации (ISO). Во многих странах мира разрабатываются стандарты и руководства, содержащие рекомендации по использованию облачных вычислений, и в статье дан их обзор.

Обзор

Стандарт ISO/IEC 17788 «Информационные технологии. Облачные вычисления. Общие положения и терминология» описывает концепцию облачных вычислений и содержит ряд терминов и определений. Он является терминологической основой для дальнейшей работы по стандартизации в сфере облачных вычислений.

Стандарт ISO/IEC 17789 «Информационные технологии – Облачные вычисления – Эталонная архитектура» содержит обзор общих понятий и характеристик облачных вычислений, типов облаков, компонент облачных вычислений участвующих сторон, а также взаимоотношений между этими элементами. В нем сделан упор на требования к тому, что должны обеспечивать облачные сервисы, а не на вопросы проектирования и внедрения соответствующих решений.

ISO/IEC 27017 «Информационные технологии - Руководство по мерам информационной безопасности для использования сервисами облачных вычислений, основанное на стандарте ISO/IEC 27002». Стандарт содержит рекомендации по обеспечению информационной безопасности при облачных вычислениях. Он опирается на пересмотренную версию ISO/IEC 27002 и содержит главным образом рекомендации по реализации многих описанных в этом документе мер информационной безопасности в контексте облачных вычислений. Отдельного стандарта, специфицирующего систему менеджмента информационной безопасности в облаке, не будет, поскольку считается, что вполне достаточно существующего стандарта ISO/IEC 27001. Соответственно, нет и планов по отдельной сертификации информационной безопасности у поставщиков облачных вычислений [3].

Стандарт ISO/IEC 27018 «Свод практик по мерам защиты персональных данных при оказании публичных облачных услуг» предназначен для поставщиков услуг «публичного облака», которые ведут обработку персональных данных (и, возможно, являются операторами персональных данных). Он содержит рекомендации по различным аспектам и элементам защиты персональных данных и неприкосновенности личной информации в публичном облаке. Стандарт не дублирует или модифицирует рекомендации стандарта ISO/IEC 27002. В нем определены дополнительные цели и меры контроля и управления, связанные с защитой персональных данных в облачной среде.

Стандарт ISO/IEC 27040 «Информационные технологии – Безопасность хранения данных» содержит детальные технические рекомендации относительно того, как организациям определить соответствующий уровень мер снижения рисков путем планирования, разработки и реализации системы безопасности при хранении данных. В нем дан обзор общих представлений о безопасности при хранении данных и соответствующие определения, а также рекомендации, касающиеся типичных технологий и сценариев хранения. Стандарт применим при обеспечении безопасности устройств и носителей и относящейся к ним управленческой деятельности; при обеспечении безопасности приложений и сервисов. Также охватываются вопросы безопасности, связанные с конечными пользователями. Этот стандарт имеет косвенное отношение к облачным вычислениям, так как тема хранения данных в облаках затронута в ограниченной степени [4].

Стандарты и руководства США

CIO правительства США поручил Национальному институту стандартов и технологий взять на себя лидерство в разработке стандартов облачных вычислений. В NIST была создана специальная рабочая группа по стандартам в сфере облачных вычислений, которая провела обследование существующего ландшафта стандартов. В качестве приоритетных выделили три области:

- информационной безопасности;
- интероперабельности (совместимости);
- требования к переносимости облачных услуг.

Рабочая группа выявила ряд пробелов в имеющихся стандартах, начиная от таких фундаментальных вопросов, как обеспечение безопасности и защиты личной информации, до пользовательских интерфейсов и бизнес-ориентированных функций. Также были сформулированы приоритеты в области стандартизации для нужд правительства США, в частности в области аудита безопасности и соответствия законодательным актам, управления идентификацией и доступом. Как результат этих исследований весной 2011 г. рабочая группа опубликовала «Дорожную карту разработки стандартов». Кроме того, с целью решения беспокоящих руководителей

федеральных органов вопросов безопасности в институте создали отдельную рабочую группу по безопасности облачных вычислений.

Заключение

Облачные технологии, как и любые другие технологии, не являются «хорошими» или «плохими». У них большой потенциал, но при их применении можно столкнуться с рядом проблем. Задача организаций при работе в облаках заключается в том, чтобы максимально использовать преимущества облачных вычислений, избегая при этом рисков. Для того чтобы перевод деятельности в облака дал ожидаемые результаты, нужна соответствующая нормативно-правовая и методологическая базы, поэтому на формирование таких баз следует обратить самое серьезное внимание. Изучение и активное использование национальных и международных руководств и стандартов позволит сократить сроки разработки отечественных документов, повысить их качество и усилить взаимоотношения с мировой практикой.

Список используемых источников

1. Андрианов В. И., Красов А. В., Липатников В. А. Инновационное управление рисками информационной безопасности : учебное пособие // Федер. агентство связи, С.-Петерб. гос. ун-т телекоммуникаций им. М. А. Бонч-Бруевича. СПб. : СПбГУТ, 2012. 396 с. ISBN: 978-5-91891-092-4.

2. Бирих Э. В., Сахаров Д. В. Модель нарушителя распределенной информационно-вычислительной сети // Актуальные проблемы инфотелекоммуникаций в науке и образовании. V Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 3-х т. СПб. : СПбГУТ, 2016. Т. 1. С. 235–238.

3. Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services [Электронный ресурс]. URL: https://www.iso.org/standard/43757.html (дата обращения 30.03.2017).

4. Международная организация по стандартизации [Электронный ресурс]. URL: https://www.iso.org (дата обращения 30.03.2017).

5. Дорожная карта разработки стандартов [Электронный ресурс]. URL: http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=909024 (дата обращения 30.03.2017).

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

УДК 004.056.53

МЕТОД ПОВЫШЕНИЯ БЕЗОПАСНОСТИ РАСПРЕДЕЛЕННОЙ ВЫЧИСЛИТЕЛЬНОЙ СИСТЕМЫ НА БАЗЕ СППР И С УЧЕТОМ ПРОГНОЗИРОВАНИЯ СОСТОЯНИЯ

Э. В. Бирих, Л. А. Виткова, Д. В. Сахаров, И. Ю. Сергеева

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

Актуальность вопроса повышения безопасности распределенных вычислительных систем связана с увеличением количества атак на информационную систему, в частности, относящуюся к государственным органам. При постоянном появлении новых уязвимостей система не способна выявлять и предотвращать атаки, то есть противостоять изменяющимся условиям. Возникает потребность в создании средств для автоматического поиска атак, способных накапливать опыт нейтрализации существующих угроз и адаптировать систему под новые. Таким образом, предполагается создание метода использования системы поддержки принятия решений, с учетом прогнозирования состояния распределенной вычислительной системы в ближайшем будущем.

СППР, атака, безопасность, информационная система, DSS.

Вопрос защиты конфиденциальной информации далеко не новый. Как правило, в любой организации обрабатывается несколько категорий данных, утечка которых может привести к серьезным негативным последствиям.

Поэтому обеспечение состояния защищенности информационных систем организации – это одна из важнейших задач, требующих решения.

Введение

Каждая информационная система (ИС) имеет свой набор уязвимостей и параметров, следовательно, и перечень возможных угроз. Таким образом, необходимо для каждой ИС выбирать меры защиты, позволяющие противостоять имеющимся угрозам, тем самым снижая риски. При этом сегодня вопрос защиты конфиденциальной информации приходится решать в условиях ограничения трудовых и финансовых ресурсов.

Решением данной проблемы может стать экспертная система, которой является проектируемая система поддержки принятия решений (СППР) по обеспечению и управлению безопасностью данных.

Одной из главных задач, требующих решения, является сокращение времени реагирования и снижение вероятности принятия ошибочных решений оператором при возникновении нештатной ситуации. Обычно правильность принятия решений носит субъективный характер, так как на лицо принимающее решение влияет множество факторов.

Постоянный рост скорости появления новых вредоносных воздействий на информационную систему организации приводит к увеличению числа средств защиты информации (СЗИ). Администратору непросто создать систему защиты, которая смогла бы закрыть все уязвимости и свести риск реализации угроз к минимуму. Еще более непростым является настройка всех СЗИ в зависимости от сложившейся ситуации и возникающих инцидентов.

Автоматизация процесса выбора средств защиты, настройки созданной системы или ее переконфигурирования позволит увеличить эффективность реагирования на попытки нарушения защиты информационной системы организации, предотвратить ошибки администратора, допускаемые при ручной настройке СЗИ, увеличить скорость принятия управленческих решений по ее защите [1].

Авторы данной работы предполагают, что наиболее эффективным средством, на данный момент может стать система поддержки принятия решений.

Анализ

Система поддержки принятия решений – СППР, имеющая англоязычное название Decision Support System (DSS) – это компьютерная автоматизированная система, задачей которой является помощь людям, принимающим решение в сложных условиях для полного и объективного анализа предметной деятельности. Система поддержки принятия решений представляет собой комплекс программных инструментальных средств, используемых для анализа данных, моделирования, прогнозирования и принятия управленческих решений.

СППР возникли в результате слияния управленческих информационных систем и систем управления базами данных [2].

Типовыми задачами защиты информации, для решения которых можно применять СППР, являются следующие:

– обнаружение вторжений на автоматизированную информационную систему;

– организация соответствующего информационного реагирования и противодействия вредоносным воздействиям;

– проведение периодического активного контроля имеющихся СЗИ;

– организация автоматизированного аудита информационной безопасности организации [1].

Информационная сложность определяется необходимостью учета большого объема данных, обработка которых без помощи современной вычислительной техники практически невыполнима. В этих условиях число возможных решений, как правило, велико, и выбор наилучшего из них без всестороннего анализа может приводить к грубым ошибкам [3].

Система поддержки решений СППР решает две основные задачи:

1. Выбор наилучшего решения из множества возможных (оптимизация).

2. Упорядочение возможных решений по предпочтительности (ранжирование).

В обеих перечисленных задачах первым и наиболее принципиальным моментом является выбор совокупности критериев, на основе которых в дальнейшем будут оцениваться, и сопоставляться возможные решения.

Для анализа и выработок предложений в СППР используются разные методы. Это могут быть:

– информационный поиск;
– интеллектуальный анализ данных;
– поиск знаний в базах данных;
– рассуждение на основе прецедентов;
– имитационное моделирование;
– эволюционные вычисления и генетические алгоритмы;
– нейронные сети;
– ситуационный анализ;
– когнитивное моделирование и другие [4].

Близкие к СППР классы систем – это экспертные системы и автоматизированные системы управления [2].

Метод

Для того чтобы построить систему защиты информации необходимо разработать модель нарушителя. Как известно, нарушители делятся на два типа внешние и внутренние.

Существует распределенная вычислительная система – сервер и рабочие станции. Система поддержки принятия решений с помощью датчиков поведения системы распознает вторжение в ИС, как внешнего нарушителя, так и внутреннего. Система предоставляет оператору возможность мониторинга актуального состояния угроз в режиме реального времени. Так, для каждой потенциальной угрозы отображается вероятность ее осуществления в процентах, в виде отношения последовательности прошедших шагов системы к общему их числу, означающему полную реализацию

угрозы. Оператор на основании дополнительной информации о состоянии системы (трафик, его интенсивность по времени) принимает собственное решение относительно правдивости предсказания угрозы системой. В случае положительного решения оператор осуществляет запуск защитных действий, выбирая их из списка предлагаемых СППР. Если вероятность устойчивого функционирования не достигла критического уровня, и время принятия решения также не достигло критического уровня, включается блок прогнозирования состояния, который включает алгоритм сначала.

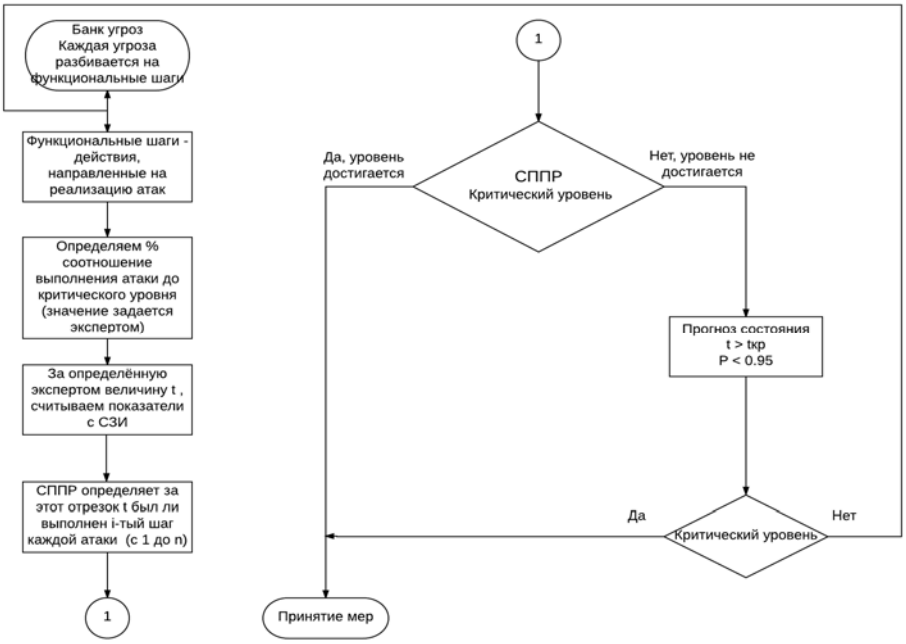


Рисунок. Блок схема метода

Выводы

Неосторожность, неосмотрительность, несвоевременное информирование сотрудника службы безопасности о состоянии ИС повышают риски и становятся основными источниками угроз в информационных системах. На основании вышеперечисленных задач и отсутствия в настоящее время специально предназначенных для целей защиты информации СППР, авторы делают вывод об их востребованности и актуальности [1, 5, 6].

Список используемых источников

1. Витенбург Е. А., Никишова А. В., Чурилина А. Е. Системы поддержки принятия решений в информационной безопасности [Электронный ресурс]. Сайт: umka.volsu.ru/newumka2. URL: http://umka.volsu.ru/newumka3/upload/590174393497603.compressed.pdf. (дата обращения 01.03.2017).

2. Системы поддержки принятия решения как составная часть ИС. Компоненты системы поддержки принятия решения [Электронный ресурс]. Сайт: life-prog.ru. URL:

http://life-prog.ru/2_94828_sistemi-podderzhki-prinyatiya-resheniya-kak-sostavnaya-chast-is-komponenti-sistemi-podderzhki-prinyatiya-resheniya.html (дата обращения 03.03.2017).

3. Дьяконова В. В. Проблемы системы управления производственной компании по разработке программного обеспечения на основе поддержки и принятия решений // Молодой ученый. 2016. № 10. С. 684–686.

4. Жаманкарин М. М., Кабдушев А. С. Основные направления систем информационной поддержки руководителя предприятия // Молодой ученый. 2015. № 8. С. 139–141.

5. Васильев В. И., Пестриков В. А., Красько А. С. Вопросы создания системы поддержки принятия решений в рамках программы «Безопасный город» [Электронный ресурс] // Вестник УГАТУ = Vestnik UGATU. 2008. № 2. URL: http://cyberleninka.ru/article/n/voprosy-sozdaniya-sistemy-podderzhki-prinyatiya-resheniy-v-ramkah-programmy-bezopasnyy-gorod (дата обращения 28.03.2017).

6. Штеренберг С. И., Виткова Л. А., Просихин В. П. Методика применения концепции адаптивной саморазвивающейся системы // Информационные технологии и телекоммуникации. СПб. : СПбГУТ. 2014. Т. 4. № 8. С. 126–133.

УДК 004.056.53

АЛГОРИТМЫ BIG DATA И МОНИТОРИНГ ИТ ИНФРАСТРУКТУРЫ ПРЕДПРИЯТИЯ

Э. В. Бирих, Л. А. Виткова, Д. В. Сахаров, В. С. Шашкин

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

Управление и контроль над событиями и инцидентами все чаще становится приоритетным в информационной безопасности. Все большее количество организаций несут убытки из-за хищения информации. Контроль над всей инфраструктурой предприятия позволяет снизить риски несанкционированных вторжений и отследить основные тенденции угроз.

контроль, BIG DATA, Большие данные, мониторинг, ущерб, распределение ресурсов, выход из строя, информационная безопасность.

Введение

Реалии сегодняшнего дня таковы, что количество и многообразие данных, поступающих в системы обработки информации, постоянно увеличивается. Объём данных настолько велик, что его обработка стандартными программными и аппаратными средствами является крайне сложной задачей, а возможностей традиционных систем хранения и обработки данных, как правило, оказывается недостаточно для оперативного анализа

и формирования актуальных решений. В связи с этим в последние несколько лет специалисты в сфере информационных технологий проявляют заметный интерес к технологиям Больших Данных (*Big Data*). Само понятие «Большие Данные» появилось примерно 8 лет назад – впервые его использовали в журнале Nature в 2008 г., однако согласно Google Trends начало активного роста употребления этого термина началось в 2011 г. [1, 2, 3, 4, 5].

У термина «Большие Данные» нет чёткого определения, однако наиболее эффективным является осознание его как совокупности трёх основных аспектов. Во-первых – это очень большой объём информации, требующий специфических инструментов обработки и хранения. Данных не просто много относительно «стандартных» сценариев, а их непрерывно становится всё больше и больше. Во-вторых – это разнообразие информации, непостоянность и неоднородность потока данных, отсутствие строгой структуры потока. Технологии обработки Больших Данных должны уметь работать как со структурированными, так и с неструктурированными данными. В-третьих – это необходимость обработки и получения выводов с минимальными задержками.

Анализ

Для решения проблемы обработки Больших Данных существует множество конкретных методик, способов и подходов. В основе одного из таких подходов лежит система распределённых вычислений, при которой обработка производится не на одной высокопроизводительной машине, а на группе таких машин, объединённых между собой в некую систему, называемую кластером. Следует также понимать, что методики, которые эффективно работают с Большими Данными, могут также с успехом применяться и для обработки намного меньших по объёму массивов.

На предприятиях, имеющих дело с гостайной, имеет место быть наличие аттестованных рабочих мест (АРМ).

Аттестации на соответствие требованиям по защите государственной тайны, подлежат любой объект информатизации (помещение, компьютер, ксерокс), который участвует в обработке сведений составляющих государственную тайну. Для успешного прохождения аттестации необходимо провести комплекс подготовительных мероприятий, в который входит проведение специальной проверки техники, проведение специальных исследований техники, установка и настройка сертифицированных ФСТЭК средств защиты информации. Для каждого вида объектов, будь то ВП (выделенное помещение), АРМ (автоматизированное рабочее место), ЗЛВС (защищенная локальная вычислительная сеть), или СИРД (средство изготовления-размножения документов), существуют свои требования

по технической защите информации. Которым необходимо строго соответствовать. И только после подготовки объекта можно приступать к проведению аттестационных испытаний. Финалом которых будет Аттестат соответствия объекта информатизации.

Использование технологии BIG DATA позволит в реальном времени отслеживать и контролировать объекты информатизации. В данном случае приемлемыми мерами будет контроль и запрет на использование не аттестованными периферийными устройствами, запрет на использование съемных накопителей, а так же анализ действий пользователя и выявление подозрительной активности.

Выводы

Использование технологии обработки Больших данных, в сфере ИБ, не ограничивается анализом сетевого трафика. Эта технология может быть использована для мониторинга ИТ ресурсов компании. Благодаря технологии Больших данных, появляется возможность обновлять информацию о каждой из машин, с минимальным интервалом, ограниченным лишь быстродействием ответа машины находящейся на контроле.

Уменьшая интервал между обновлениями, мы можем более детально получать информацию, обо всех внештатных ситуациях, таких как хищение запоминающих устройств, хранящих в себе любую конфиденциальную информацию, выход из строя отдельных частей устройств, что повысит оперативность их замены, прогнозирование пиков повышенной загруженности ресурсов и их более рациональному распределению.

Немаловажным аспектом при работе с большими данными является машинное обучение – метод анализа данных, который автоматизирует построение аналитической модели. Используя алгоритмы, которые итеративно обучаются на данных, машинное обучение позволяет получать алгоритмы анализа данных по каким-либо критериям без явного задания программной модели. Итеративный аспект машинного обучения необходим, так как позволяет полученным алгоритмам работать на новых данных и, возможно, адаптироваться к ним. В результате такого обучения алгоритм сможет производить надежные и воспроизводимые решения и давать достаточно точные результаты на данных.

Список используемых источников

1. Big Data от А до Я. Часть 1: Принципы работы с большими данными, парадигма MapReduce [Электронный ресурс]. Социальное СМИ. URL: https://habrahabr.ru/company/dca/blog/267361 (дата обращения 26.12.2016).

2. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К) [Электронный ресурс]. URL: http://www.rfcmd.ru/sphider/docs/InfoSec/RD_FSTEK_requirements.htm (дата обращения 11.01.2017).

3. Аттестация по требованиям безопасности Гостайны [Электронный ресурс]. URL: http://www.apsecurity.ru/services/state-secret-certification.html (дата обращения 26.12.2016).

4. Дубровин Н. Д., Ушаков И. А., Чечулин А. А. Применение технологии больших данных в системах управления информацией и событиями безопасности // Актуальные проблемы инфотелекоммуникаций в науке и образовании сборник научных статей. V Международная научно-техническая и научно-методическая конференция: сб. науч. Ст. в 3-х т. СПб. : СПбГУТ, 2016. Т. 1. С. 348–353.

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.

УДК 004.056.53

МЕТОДОЛОГИЯ ФОРМИРОВАНИЯ МОДЕЛИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ

Э. В. Бирих, Е. Ю. Рябов, Д. В. Сахаров

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

В рамках данной работы рассматривается понятие модели угроз безопасности информационных систем. Раскрываются особенности её формирования, анализируется существующая нормативно-правовая база, посвященная данному вопросу. Обосновывается необходимость формирования модели угроз, предлагается подход к её реализации.

модель угроз, информационная система, защита информации, методика, персональные данные.

Информационная система является одним из основных активов множества организаций. Этот факт определяет необходимость в качественной системе защиты, создание которой невозможно без определения существующих и анализа актуальных угроз [1]. Для решения данной задачи в организациях разрабатывается модель угроз, но не всегда понятно каким образом она должна быть составлена, какие требования и рекомендации при этом должны быть учтены.

Модель угроз безопасности информации – физическое, математическое, описательное представление свойств или характеристик угроз безопасности информации [2]. В процессе обеспечения защиты информации модель угроз необходима не только на этапе формирования требований к защите информации, но и при аттестации информационной системы, ес-

ли проведение такого мероприятия требуется на основании законодательства. Соответственно можно выделить следующие нормативно-правовые акты, определяющие наличие модели угроз как обязательное требование:

1. Приказ Федеральной службы по техническому и экспортному контролю от 11.02.2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» [3].

2. Приказ Федеральной службы по техническому и экспортному контролю от 14.03.2014 г. № 31 «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды» [4].

Отдельно следует отметить Федеральный закон от 27.07.2006 г. № 152-ФЗ «О персональных данных», который не требует составления модели угроз, в отличие от перечня актуальных угроз [5]. Тем не менее, для информационных систем персональных данных составление модели угроз является рекомендательным.

В целях исполнения требований вышеупомянутых нормативно-правовых актов следует использовать утверждённые методики, представленные в таблице.

ТАБЛИЦА. Методики определения угроз безопасности информации

<table>
<tr><th>Федеральный закон от 27.07.2006 г.
№ 152-ФЗ «О персональных данных»</th><th>Приказ Федеральной службы
по техническому и экспортному контролю
от 14.03.2014 г. № 31</th></tr>
<tr><td>«Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных»,
ФСТЭК, 2008 год [6]</td><td>«Методика определения актуальных угроз безопасности информации в ключевых системах информационной инфраструктуры»,
ФСТЭК, 2007 год [9]</td></tr>
<tr><td>«Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных»,
ФСТЭК, 2008 год [7]</td><td rowspan="2">«Базовая модель угроз безопасности информации в ключевых системах информационной инфраструктуры»,
ФСТЭК, 2007 год [9]</td></tr>
<tr><td>«Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности», ФСБ, 2015 год [8]</td></tr>
</table>

Аналогичных утверждённых методик для реализаций требований, определённых в Приказе ФСТЭК от 11.02.2013 г. № 17, на данный момент не существует. Однако в 2015 году ФСТЭК разработала проект методического документа «Методика определения угроз безопасности информации в информационных системах». Плюсом данной методики является то, что она может применятся не только во исполнение Приказа ФСТЭК от 11.02.2013 г. № 17, но по решению оператор и для реализации требований Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных», а также организациями, осуществляющими работы по [10]:

1. Созданию (проектированию) информационных систем.
2. Защите информации в ходе создания (проектирования) и эксплуатации информационных систем.
3. Аттестации (оценке соответствия) информационных систем требованиям о защите информации.

Важными являются два первых пункта, которые говорят, что данную методику можно применять при защите информации, составляющей коммерческую тайну.

Основываясь на требованиях законодательства и соответствующих методиках, выделим следующие составляющие модели угроз безопасности информации, обрабатываемой в информационных системах:

1. Описание информационной системы и ее структурно-функциональных характеристик.
2. Описание возможностей нарушителей (модель нарушителя).
3. Описание возможных уязвимостей информационной системы.
4. Описание перечня реализуемых и определение актуальных угроз безопасности информации.
5. Описание способов реализации угроз безопасности информации.
6. Описание последствий от нарушения свойств безопасности информации.

Способы раскрытия данных пунктов даются в указанных ранее методиках, однако кроме них также можно использовать следующие стандарты:

1. ГОСТ Р 52448-2005 «Защита информации. Обеспечение безопасности сетей электросвязи. Общие положения» [11].
2. ГОСТ Р 51275-2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения» [12].
3. ГОСТ Р 56545-2015 «Защита информации. Уязвимости информационных систем. Правила описания уязвимостей» [13].

Таким образом, подход к формированию модели угроз можно представить в виде следующей последовательности шагов (рис.):

1. Необходимо определить, какая информация подлежит обработке в информационной системе, требует ли данная информация защиты, кто является собственником информационной системы.

2. На основе полученных данных определить, выступает ли модель угроз в качестве требования со стороны действующего законодательства.

3. Использовать существующие методики формирования модели угроз, если таковые имеются для данной информационной системы.

4. Использовать имеющиеся стандарты для раскрытия структурных составляющих модели угроз.

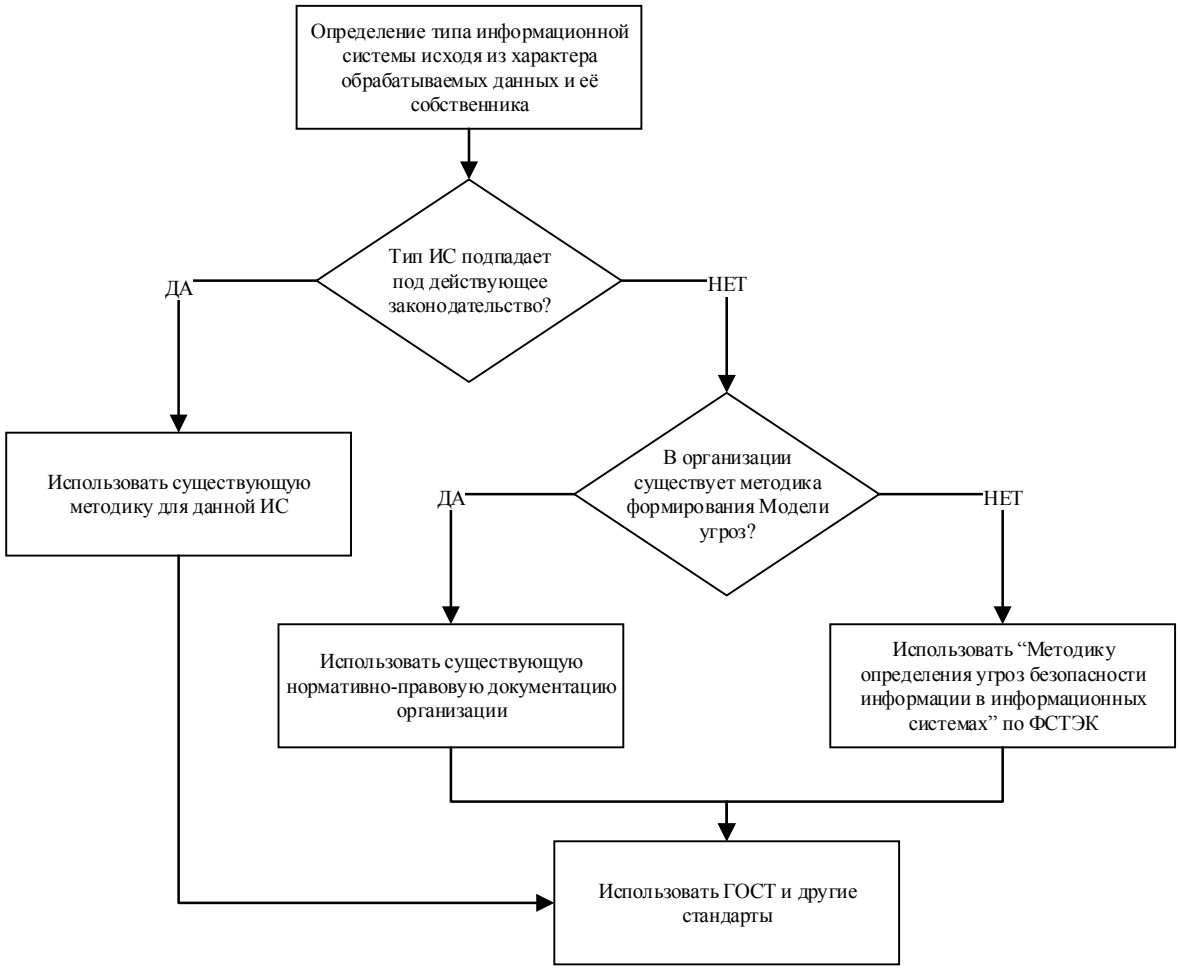


Рисунок. Подходы к формированию модели угроз безопасности информации

Список используемых источников

1. Андрианов В. И., Красов А. В., Липатников В. А. Инновационное управление рисками информационной безопасности : учебное пособие // Федер. агентство связи, С.-Петерб. гос. ун-т телекоммуникаций им. М. А. Бонч-Бруевича. СПб. : СПбГУТ, 2012. 396 с. ISBN: 978-5-91891-092-4.

2. ГОСТ Р 50922–2006. Защита информации. Основные термины и определения. М. : Стандартинформ, 2006. 8 с.

3. Приказ Федеральной службы по техническому и экспортному контролю от 11.02.2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» [Электронный ресурс]. Сайт: ФСТЭК России. URL: http://fstec.ru/component/attachments/download/567 (дата обращения: 29.03.2017).

4. Приказ Федеральной службы по техническому и экспортному контролю от 14.03.2014 г. № 31 «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды» [Электронный ресурс]. Сайт: ФСТЭК России. URL: http://fstec.ru/component/attachments/download/718 (дата обращения 29.03.2017).

5. Федеральный закон от 27.07.2006 г. № 152-ФЗ «О персональных данных» (с изменениями на 22 февраля 2017 года) [Электронный ресурс]. Сайт: КонсультантПлюс. URL: http://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения: 29.03.2017).

6. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК России, 14 февраля 2008 г. [Электронный ресурс]. Сайт: ФСТЭК России. URL: http://fstec.ru/component/attachments/download/290 (дата обращения 29.03.2017).

7. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка). ФСТЭК России, 15 февраля 2008 г. [Электронный ресурс]. Сайт: ФСТЭК России. URL: http://fstec.ru/component/attachments/download/289 (дата обращения 29.03.2017).

8. Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности. ФСБ России, 31 марта 2012 г. [Электронный ресурс]. Сайт: Кодекс. URL: http://docs.cntd.ru/document/420336137 (дата обращения 29.03.2017).

9. Информационное сообщение ФСТЭК России от 25 июля 2014 г. N 240/22/2748 [Электронный ресурс]. Сайт: ФСТЭК России. URL: http://fstec.ru/component/attachments/download/715 (дата обращения 29.03.2017)

10. Методический документ. Методика определения угроз безопасности информации в информационных системах. Проект ФСТЭК России. 2015 [Электронный ресурс]. Сайт: ФСТЭК России. URL: http://fstec.ru/component/attachments/download/812 (дата обращения 29.03.2017).

11. ГОСТ Р 52448-2005 Защита информации. Обеспечение безопасности сетей электросвязи. Общие положения [Электронный ресурс]. Сайт: Кодекс. URL: http://docs.cntd.ru/document/1200044726 (дата обращения 29.03.2017).

12. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. [Электронный ресурс]. Сайт: Кодекс. URL: http://docs.cntd.ru/document/1200057516 (дата обращения 29.03.2017).

13. ГОСТ Р 56545-2015 Защита информации. Уязвимости информационных систем. Правила описания уязвимостей [Электронный ресурс]. URL:http://docs.cntd.ru/document/1200123701 (дата обращения: 29.03.2017).

УДК 004.056.5

СРАВНИТЕЛЬНЫЙ АНАЛИЗ МОДЕЛЕЙ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ИНТЕРЕСАХ ПРИМЕНИМОСТИ ДЛЯ МНОГОЭТАПНЫХ СХЕМ АТАК

А. А. Бирюков, К. Е. Израилов

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

Рассматриваются существующие модели угроз информационной безопасности. Дается описание и назначение моделей, выделяются их основные достоинства и недостатки. Обосновывается вывод относительно недостаточности моделей для решения ряда актуальных задач информационной безопасности, таких, как прогнозирования новых угроз, нахождения возможных путей реализации атак и их вероятностей. Предлагается новая модель, решающая указанные задачи и построенная на новом принципе.

модель угрозы, защита информации, информационная безопасность, многоэтапная атака.

В настоящее время существуют множество методов и средств обеспечения информационной безопасности (ИБ). Одним из фундаментальных «кирпичей» можно по праву считать разработку модели угроз. Модель угроз – это описание существующих угроз ИБ, их актуальности, возможности реализации и последствий. Необходима она для определения требований при построении адекватной системы зашиты информации.

Существующие модели, в том числе и те, которые были взяты на сравнительный анализ, рассматривают угрозы как следствие одноэтапной атаки, хотя есть и исключения [1]. На рис. 1, показана типовая реализация такой атаки. Идея разработки новой модели угроз информационной безопасности, заключается в рассмотрение угроз в контексте многоэтапной атаки, где каждая угроза порождает новую. Более подробно рассмотрение и описание происходит после сравнительного анализа четырех моделей угроз.

Первая модель – базовая. Данными моделями угроз являются созданные специальными службами, описанные в нормативно-методических документах: под редакциями ФСБ и ФСТЭК. Первым рассмотренным документом была взята базовая модель угроз ФСТЭК России (от 15 февраля 2008 г.).

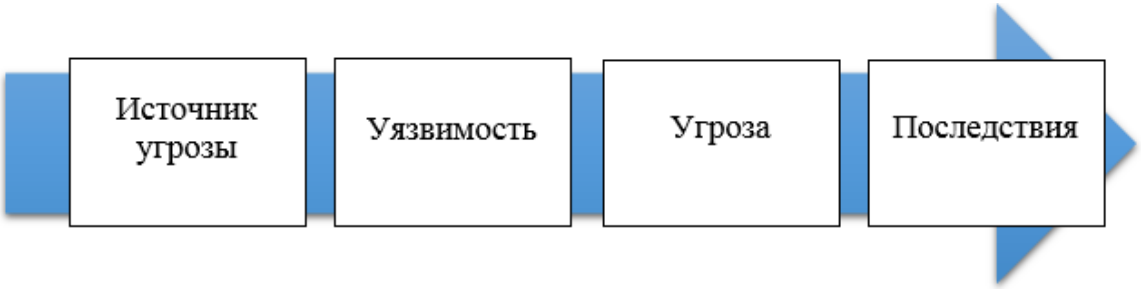


Рис. 1. Типовая реализация атака

Модель обладает достоинствами, поскольку является:

– является документом специальных служб (ФСТЭК России, ФСБ России), регулирующих и контролирующих вопросы защиты персональных данных, в соответствии с действующим российским законодательством;

– является методическим документом.

Тем не менее, у модели есть следующие недостатки:

– угрозы, приведенные в модели, устарели и далеко не всеобъемлющи;

– невозможна программная реализация.

Второй моделью угроз взята модель, используемая в Банке России и описанная в стандарте СТО БР ИББС-1.0-2014. Стандарт был принят и введен в действие Распоряжением Банка России от 17 мая 2014 года № З-399, взамен СТО БР ИБСС-1.0-2010.

Модель обладает следующими достоинствами:

– является основным инструментом организации Банковской Системы РФ при развертывании, поддержании и совершенствовании Системы Обеспечения Информационной Безопасности;

– информационная инфраструктура, которая обеспечивает реализацию банковских технологий, может быть представлена в виде иерархии основных уровней, на каждом из уровней угрозы и их источники методы и средства защиты и подходы к оценке эффективности являются различными [3];

– имеются процедуры регулярного анализа необходимости пересмотра модели угроз.

Модель также обладает и недостатками:

– перечислены возможные источники угроз с каждого уровня, но в общих чертах; нет развернутого описания угроз;

– используется лишь в банковских системах;

– невозможная программная реализация.

Третьим примером является частная модель угроз безопасности информации под авторством И. В. Бондарь.

У модели следующие достоинства:

– позволяет решать задачи разработки частных моделей угроз безопасности информации в конкретных системах с учетом их назначения, условий и особенностей функционирования;

– возможен контроль уровня защищенности Информационной Системы методами анализа риска и разработка эффективной системы защиты информации, обеспечивающей нейтрализацию предполагаемых угроз [4];

– возможность стать основой для разработки универсальных алгоритмических, а затем и математических моделей безопасности, эффективно сочетающих в себе требования нормативно-методических документов, методологию построения моделей угроз, моделей нарушителя и т. д. [4];

– методика ее построения для автоматизированных систем основана на геометрической модели.

Других существенных и видимых недостатков у модели не обнаружено.

Четвертая модель, тоже частная, применяется в основном для моделирования оценки угроз безопасности информационных систем персональных данных (авторы А.С. Шабуров, С. А. Юшкова, А. В. Бодерко). И хотя данная модель является исключением из предыдущих рассмотренных (весь упор происходит на оценку угроз) тем не менее, ее анализ так же может быть полезен.

Достоинства модели следующие:

– применяется в оценочной методике реализуемости угрозы;

– возможная программно-аппаратная реализация;

– при использовании алгоритмов объектного программного моделирования на основе разработки системы информационно-аналитической поддержки оптимизирует процедуры оценки, позволяет осуществлять моделирование как самих угроз информационной безопасности, в частности, так и систем защиты информации в целом [5].

Основным ее недостатком является неполноценность, как модели.

После проведенного анализа и определения основных достоинств и недостатков моделей угроз появляется возможность создать систему критериев для их сравнения в интересах моделирования многоэтапных атак. В результате было произведено сравнение приведенных моделей угроз ИБ по следующим критериям:

– «Применимость в разных сферах информационных системах (ИС)» – можно ли применить модель в другой сфере ИС;

– «Использование в методических целях» – можно ли применить модель в качестве методического документа при создании новой модели угроз;

– «Актуальность» – устарела ли модель;

– «Возможность программной реализации» – можно ли модель преобразовать в программное средство.

Сравнительная таблица, в которой столбцы соответствуют критериям, а строки – моделям, представлена далее (табл.).

ТАБЛИЦА. Сравнительная таблица моделей угроз ИБ

Критерий / Модель	Применимость в разных сферах ИС	Использование в методических целях	Актуальность	Возможность программной реализации
ФСТЭК	+	+	–	–
Банк России	–	–	+	–
Частная модель Бондарь	–	+	+	+
Частная модель Шабуров	+	–	+	+

Как было указано раннее, основным отличием всех рассматриваемых моделей является то, как они рассматривают угрозы. Все они не позволяет полноценно решить ряд актуальных задач ИБ, таких, как прогнозирования новых угроз, нахождения возможных путей реализации атак и их вероятностей. Предлагается новая модель, построенная на новом принципе. Главной идеей является рассмотрение угрозы как многоэтапной атаки. Так каждая угроза может вести к новой угрозе, которая в свою очередь порождает новую угрозу и так до завершающей угрозы. Стоит отметить, что одна угроза может вести к нескольким, а несколько угроз совместно к одной.

На рис. 2, приведен пример многоэтапной атаки по новому принципу построения модели угроз. Есть три угрозы – угроза 1 (У1), угроза 2 (У2) и угроза 3 (У3). Из угрозы У1 появляются две угрозы – угроза 11 (У11) и угроза 12 (У12), с коэффициентом (вероятностями) их появления, К1 и К2 соответственно. Из угрозы У2, с вероятностью К3, образуется угроза У12. Угрозы У11 и У12 создают с вероятностью К4 угрозу 111 (У111). В свою очередь, угроза У111 ведет к угрозе 1111 (У1111) с вероятностью К5 и угрозе 1112 (У1112) с вероятностью К6, если угрозы У111 и У3 произойдут совместно.

Рассматриваемая идея построения новой модели угроз позволяет решить задачи построения частных моделей в различных информационных системах. Особенностью такой модели, построенной по типу многоэтапной атаки, является обеспечение контроля защищённости ИС за счет прогнозирования новых угроз, нахождения новых путей реализации и их вероятностей.

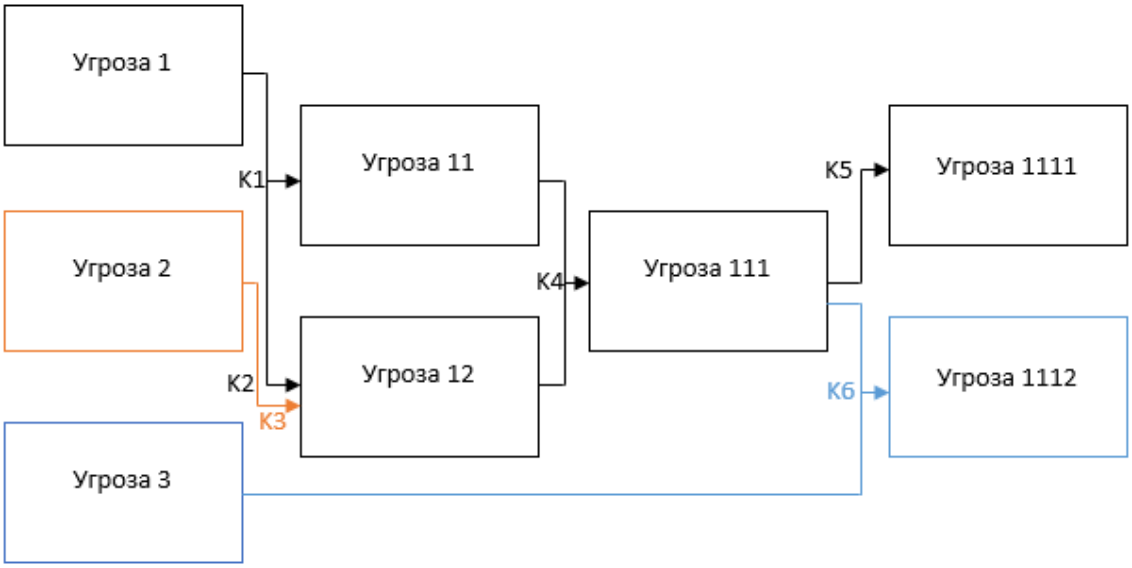


Рис. 2. Пример многоэтапной атаки

Перспективы новой модели являются в ее дальнейшем развитие как, возможно, алгоритмического так и математического аппарата в ИБ. А также последующей программной реализации для пригодной эксплуатации пользователями, достоверного источника знаний об угрозах и уязвимостях. Такая модель угроз позволит сделать процесс разработки систем защиты информации более качественным, что позволит поднять уровень защищенности информационных систем.

Список используемых источников

1. Израилов К. Е. Модель прогнозирования угроз телекоммуникационной системы на базе искусственной нейронной сети // Вестник ИНЖЭКОНа. Серия: Технические науки. 2012. № 8 (59). С. 150–153.

2. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (утверждена заместителем директора ФСТЭК России 15 февраля 2008 г.) [Электронный ресурс]. URL: http://fstec.ru/ component/attachments/download/289 (дата обращения 01.02.2017).

3. СТО БР ИББС-1.0-2014. Стандарт Банка России: «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» [Электронный ресурс]. URL: https://www.cbr.ru/credit/Gubzi_docs/st-10-14.pdf (дата обращения 01.02.2017).

4. Бондарь И. В. Методика построения модели угроз безопасности информации для автоматизированных систем // Вестник СибГАУ имени академика М. Ф. Решетнева. 2012. Вып. 3 (43). С. 7–10.

5. Шабуров А.С., Юшкова С.А., Бодерко А. В. Моделирование оценки угроз безопасности информационных систем персональных данных // Вестник ПНИПУ. 2013. Вып. 7. С. 149–159.

Статья представлена научным руководителем, кандидатом технических наук, доцентом В. Н. Волкогоновым.

УДК 004.9

ИССЛЕДОВАНИЕ СИГНАЛОВ ГЕМОДИНАМИКИ И ИСПОЛЬЗОВАНИЕ ВЗАИМНОЙ ИНФОРМАЦИИ

Л. Б. Бузюков, Т. В. Ермакова

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

Проведен сравнительный анализ использованных методов обработки гемодинамических сигналов. Отмечены их достоинства и недостатки. Для устранения одного из недостатков, а именно, величины временного лага предлагается воспользоваться взаимной информацией.

Известно, что в теории информации для измерения взаимной зависимости между двумя случайными величинами используется взаимная информация. Взаимная информация является мерой сходства между двумя переменными.

гемодинамический сигнал, фрактальные характеристики, взаимная информация.

Разрабатывается программное обеспечение, позволяющее анализировать сигналы гемодинамики с использованием различных существующих методов и подходов.

Сигналы гемодинамики – это сложные, нестационарные сигналы, имеющие некоторые локальные особенности. Для анализа таких сигналов могут быть использованы различные методы цифровой обработки [1].

Для работы с этими сигналами были проанализированы и использованы:

– статистические методы анализа;
– спектральный анализ на основе классического ДПФ;
– вейвлет-анализ;
– фрактальный анализ.

Был проведен сравнительный анализ всех указанных методов и сделан вывод относительно их плюсов и минусов при работе с гемодинамическими сигналами.

Спектральный анализ на основе классического ДПФ

Так как сигнал гемодинамики – нестационарный, его спектр нельзя рассчитать за весь временной интервал исследования. Приходится выбирать отрезок сигнала постоянной длительности и методом «скользящего окна» с некоторым сдвигом просматривать весь интервал. Спектр приходится рассчитывать для каждого участка [2].

Недостаток преобразования Фурье заключается в том, что частотные компоненты не могут быть локализованы во времени. Именно поэтому его чаще применяют к анализу стационарных сигналов.

То есть мы работаем с нестационарным сигналом как со стационарным, предварительно разбив его на сегменты.

Вейвлет-анализ

Рассматриваемый медицинский сигнал состоит из близких по времени короткоживущих высокочастотных компонентов и долговременных, близких по частоте низкочастотных компонентов. Это значит, что нам нужен метод, способный обеспечить хорошее разрешение и по частоте (для локализации низкочастотных составляющих), и по времени (для разрешения компонентов высокой частоты) [2].

Поэтому в этом случае выбирают вейвлет – преобразование. Нестационарный сигнал анализируют путем разложения по базисным функциям, полученным из материнского вейвлета путем сжатий, растяжений и сдвигов. Материнский вейвлет выбирается наиболее подходящим для исследования конкретного сигнала.

Оба метода – и спектральный анализ, и вейвлет-анализ обладают общим недостатком – в них отсутствует возможность предсказания.

Тогда на помощь приходят *фрактальные методы*. Почему?

Потому что фрактальные методы обладают *свойством инвариантности* – при изменении временного масштаба они могут давать оценки поведения состояния организма в будущем, то есть делать для больного прогноз. В медицине это очень важно [3, 4].

И если доказать фрактальную природу медицинского сигнала, то есть его самоподобие, то безусловно, имеет смысл воспользоваться фрактальным анализом гемодинамического сигнала с целью построения фрактальной математической модели нашего медицинского сигнала.

Итак, методы анализа, в основе которых лежит вейвлет-анализ, позволяют строить сигнал по заданному базису и обеспечивают частотно-временное представление сигнала.

В основе же фрактальных методов лежит построение сигнала «по подобию».

В предыдущих работах на экспериментальных сигналах гемодинамики было показано, что они обладают фрактальной статистикой на основе показателя Херста и с помощью R/S –метода, и с помощью показателя Херста, основанного на вейвлетах. Результаты эксперимента подтвердили возможность работы с этими сигналами с помощью фракталов [1].

Это было продемонстрировано и при нахождении временного лага методом автокорреляционной функции (АКФ). Метод АКФ показал, что временной ряд гемодинамического сигнала убывает по степенному закону при увеличении временной задержки. Однако, значение временного лага хотелось бы увеличить.

Поэтому предлагается использовать взаимную информацию для работы с гемодинамическим сигналом, а именно, для нахождения временного лага пульсовой волны и при измерении активности сердца (рис.).

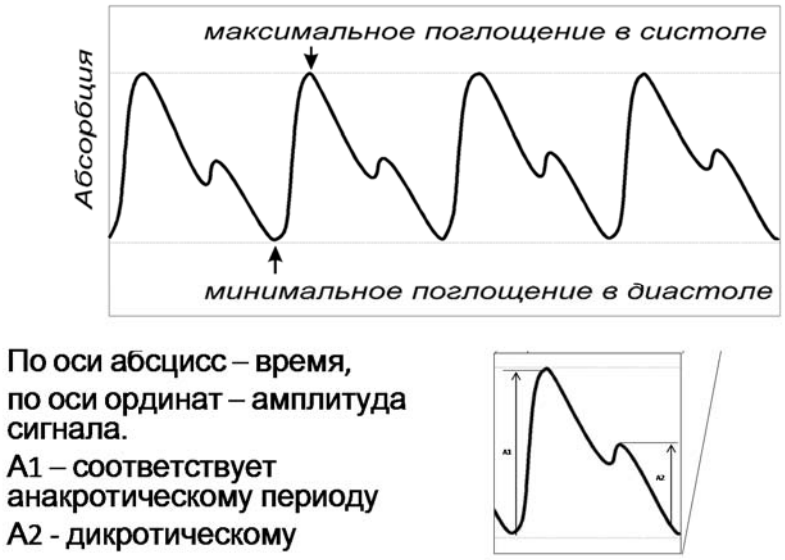


Рисунок. Пульсовая волна

Метод взаимной информации предполагает, что законы самоорганизации одинаковы для различных сложных систем. Именно этот метод позволяет нам определить закономерности и корреляции на основании очень небольшого количества данных. В данном конкретном случае применение метода взаимной информации оказалось приблизительно в четыре раза точнее при нахождении временного лага, чем традиционные статистические методы.

Имеем дискретный гемодинамический сигнал, представляющий собой набор временных отчетов $U(n)$, где $n = 1, \ldots, N$ (N – общее количество отсчетов):

$$x(n) = U(n) - \frac{1}{N} * \sum_{i=1}^{n} U(i),$$

Введем обозначение взаимной информации через энтропию и условную энтропию двух случайных величин:

$$I(x; y) = H(x) + H(y) - H(x, y),$$

Чем больше взаимная информация, тем теснее связь, тем меньше энтропия.

Окончательно, для оптимизации вычислительного процесса можно использовать следующее выражение:

$$I(\tau) = -\sum\sum_{1}^{Д}[P(A_i\,B_j\,)\,(\tau) - P(A_i)(\tau)\,P(B_j)(\tau)]^2,$$

Эта формула сохраняет положение максимумов и минимумов функции.

Следует отметить, как недостаток – достаточно кропотливую работу с матрицами корреляции.

Выводы

1. Взаимная информация по сравнению с другими фрактальными методами способна обнаруживать нелинейную корреляцию между двумя переменными, что в медицине позволяет производить визуализацию процессов.

2. Взаимная информация позволяет определять закономерности и корреляцию на основе очень небольшого количества данных

3. Взаимная информация в несколько раз точнее при поиске упорядоченных состояний, чем традиционные статистические методы.

4. В дальнейшем предполагается добавить доказательства персистентности на основе значений корреляционной размерности и показать, как это свойство может быть использовано медиками для прогнозирования состояния больного. (Для этого должна подойти теория хаоса с ее корреляционной размерностью, размерностью пространства вложений и т. п.).

Список используемых источников

1. Бузюков Л. Б., Ермакова Т. В. Использование вейвлет-анализа для исследования и оценки зависимости параметров гемодинамики от комплекса параметров специализированного измерительного устройства искусственной вентиляции легких // Актуальные проблемы инфотелекоммуникаций в науке и образовании. III Международная научно-техническая и научно-методическая конференция: сб. научных статей. СПб.: СПбГУТ, 2014. С. 203–208.

2. Афончикова Т. В., Гойхман В. Ю. Анализ трафика распределенного узла коммутации с помощью вейвлет-преобразования // Информационные технологии в мире коммуникаций: сборник тезисов участников V Всероссийской научно-практической конференции, 13-18 мая 2012 г. Москва, 2012. 125 с.

3. https://ru.wikipedia.org/wiki/Лёгкие#mediaviewer/File:Respiratory_system_complete_ru.svg

4. Шелухин И. О., Осин А. В., Смольский С. М. Самоподобие и фракталы. Телекоммуникационные приложения / Под ред. О. И. Шелухина. М. :ФИЗМАТЛИТ, 2008. 368 с. ISBN: 978-5-9221-0949-9.

УДК 004.056.53

ТЕОРЕТИЧЕСКИЕ АСПЕКТЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ПРЕДПРИЯТИИ

Н. А. Булатов, Л. А. Виткова, В. С. Шашкин

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

Всю конфиденциальную информацию на предприятии необходимо контролировать, отслеживать, и, при ее несанкционированной передаче, блокировать. Большинство организаций теряют существенную прибыль из-за безответственных сотрудников, которые по каким-либо причинам (случайным или нарочным) сливают служебную информацию за пределы корпоративной сети. В данной статье авторами рассмотрены основные способы защиты предприятия от утечек данных.

DLP, SIEM, угроза, уязвимость, атака, вредоносное ПО, утечка информации, инциденты.

Введение

В эпоху развития новейших технологий информация стала для нас самой дорогой, и, несомненно, неотъемлемой частью нашей жизни. «Кто владеет информацией, тот владеет миром» – так говорил Н. М. Ротшильд. Данную цитату можно применить и к компаниям, которые тщательно контролируют весь поток информации, который проходит на предприятии. У каждой, без исключения, компании есть своя конфиденциальная информация, распространения которой она бы не пожелала. И защита такой информации – обязательная мера, которую должны соблюдать все без исключения.

Как только появились первые средства защиты информации, встали многочисленные вопросы – а как нам узнать, что эти средства информационной безопасности (далее – ИБ) действительно работают и приносят необходимую защиту? Как наиболее быстро реагировать на угрозы? Каким образом можно автоматизировать все процессы ведения журналов событий нарушения безопасности, которые при ручном прочтении займут неисчисляемое количество времени, ибо каждому ответственному сотруднику придется открывать различные приложения, консоли и только потом читать эти журналы…? [1].

К утечке информации может привести что угодно: но, в первую очередь, ни что так не вредит безопасности компании, как человеческий фактор. Для того, чтобы бороться с этой проблемой были придуманы системы

предотвращения утечки данных или так называемые DLP-системы, а также системы анализа и сбора информации SIEM.

Анализ

Для начала рассмотрим понятие самых базисных вещей: что же такое DLP-система?

Data Leak Prevention (DLP) – это система, предназначенная для выявления и предотвращения утечки конфиденциальной информации за пределы сети предприятия. Так же под DLP понимают программное обеспечение (далее – ПО), которое позволяет администратору сети контролировать те данные, которые сотрудники могут передавать за пределы компании. Само же ПО обнаруживает потенциальную передачу информации и предотвращает ее, контролируя, находя и блокируя доступ к уязвимым данным. К уязвимым данным относятся: внутренняя информация компании, интеллектуальная собственность, финансовая информация, данные кредитных карт.

Программные продукты DLP используют т. н. «бизнес политику», чтобы классифицировать и защитить конфиденциальную информацию таким образом, чтобы несанкционированные пользователи не могли случайно или умышленно отослать данные, которые при раскрытии могут поставить организацию под угрозой. Например, если сотрудник попытается переслать служебное письмо на внешний домен (который компании не принадлежит), или загрузить служебную информацию на облачное хранилище, такое как, например, Dropbox, то сотруднику будет отказано в доступе. Более того к нему могут быть применены определенные санкции за такую попытку.

В дополнении к способности мониторить и контролировать конечные действия пользователя, некоторые инструменты в DLP позволяют фильтровать потоки данных внутри сети предприятия и защищать информацию «на лету».

DLP-системы позволяют работать администратору с тремя типами данных:

1. Устаревшая информация или неиспользуемые данные (*data at rest*).
2. Используемые данные (*data in use*).
3. Передаваемая информация (*data in motion*).

«Data at rest» – это информация, хранимая на каких-либо физических носителях в цифровом виде и в данный момент времени не используемая. К ней относятся базы данных, старые архивы, записи и т. д.

«Data in use» – это данные, с которыми в данный момент взаимодействует пользователь. Системы DLP позволяют контролировать и отмечать все несанкционированные действия. Например, к таким данным относятся печать, снимки экрана.

«Data in Motion» – это данные, которые проходят через сеть в какую-либо точку назначения. Системы DLP дают возможность наблюдать за перемещением секретных сведений через различные каналы связи [2].

В общих чертах, DLP-система состоит из трех взаимосвязанных компонентов:

Управление

Политика DLP-системы определяет, какие данные нужно считать «важными», какие действия позволено совершать над ними и как защищать эту информацию.

Предположим у нас есть личный номер социального страхования, и мы хотим предотвратить незашифрованную передачу этого номера на посторонний e-mail. С виду простая задача оказывается на самом деле сложной в виду того, что нам будет трудно создать политику, которая описывала бы этот случай. Пусть у нас есть некое письмо, где можно найти определенный набор цифр, который будет содержать этот номер. Вопрос заключается в том, каким образом DLP-система поймет, что именно этот набор цифр будет являться номером социального страхования, а не случайным совпадением или, например, частью ссылки на сайт [3].

Политика DLP так же подсказывает, каким именно компонентом защиты необходимо воспользоваться, если будет идентифицирована важная информация. В случае со страховым номером, компонент защиты может зашифровать сообщение и отправить его получателю, или же он может уведомить отправителя, который нарушил политику защиты информации о необходимости зашифровать сообщение перед его отправкой.

Возможности компонента управления ограничены разнообразием форматов данных, для которых можно создать политику. Каждый формат файла шифруется по-разному. DLP необходимо отличать эти форматы: чем больше форматов знает DLP, тем более тщательные и точные проверки на наличие важной информации она будет проводить. Соответственно имеем выше шанс обнаружения и защиты необходимых данных.

Идентификация

Компонент идентификации DLP-системы использует политику, которой пользуется компонент управления для нахождения важной информации. Во всех, кроме самых простых случаев, это означает, что компонент идентификации будет проводить статистический тест и, используя результаты определять, была ли найдена необходимая информация или нет. Так как компоненты идентификации используют только статистические тесты, они не в состоянии все время выдавать безошибочные решения.

Все статистические тесты имею шансы ложного обнаружения (*false positive*) или ложного не обнаружения (*false negative*). Например, ложное обнаружение происходит тогда, когда данные идентифицируются как «важные», хотя таковыми они не являются. Ложное не обнаружение происходит в обратном случае: когда, например, секретная информация опознается как «не важная». В этом случае данные защищены не будут, что может привести к их утечке или потере.

Защита

Как только компонент идентификации DLP-системы сообщает о том, что он нашел важную информацию, компоненты защиты предпримут все действия по их защите, которые прописаны в политике. Блокировка и шифрование – два основных способа защиты.

Если пользователь копирует данные особой важности на flash-накопитель, то компонент защиты может заблокировать передачу данных и не дать пользователю совершить копирование. В других случаях компонент защиты может зашифровать данные таким образом, что только санкционированные пользователи смогут их расшифровать. Блокировка действий пользователей обычно не приводит к каким-либо серьезным техническим проблемам, однако это может привести к повышенному количеству звонков администратору или службе поддержки [4].

Способы перехвата данных с помощью DLP:

1. Зеркалирование трафика.

Копирование всех данных, проходящих через сетевые устройства и отправка их на свой сервер.

2. Интеграция с ПО предприятия.

3. Перехват с помощью агентов.

Наиболее широко используемый и самый эффективный способ – установка приложения для сбора информации на конечном устройстве пользователя.

4. Перехват и разрыв.

Отслеживание и блокировка информации до принятия мер администратором безопасности.

Выводы

Для того, чтобы сильнее обезопасить предприятие от внутренних угроз можно совместить DLP-системы вместе с т. н. системами SIEM.

SIEM – это система управления инцидентами. Она собирает и анализирует всю информацию, полученную от DLP-систем, маршрутизаторов, антивирусов и т. д. Стоит отдельно отметить, что эта система никак не защищает – она нужна лишь для сбора статистики и нахождения подозрительных отклонений.

SIEM помогает нам расправляться со следующими задачами:

1. Контролировать и оповещать обо всех подозрительных действиях пользователя, которые ранее были для него не характерны. Эту информацию SIEM получает с помощью анализа сетевого трафика.

2. Оформляет читабельную, гибко настраиваемую отчетность по инцидентам. Могут использоваться диаграммы, графики.

3. Корреляция – далеко не всегда можно что-то сказать об одном инциденте. Например, если сотрудник забыл пароль, то он начнет его подбирать – после трех неправильных вводов паролей, система SIEM создаст инцидент и оповестит администратора о попытке подбора пароля.

4. Создание специальных оповещений (рассылка которых производится, как правило, автоматически) для всех заинтересованных лиц [5].

К тому же, SIEM тщательно собирает всю информацию по инцидентам. Она мониторит события от всех устройств, серверов, и создает оповещения. Прибавив к этому подробную отчетность, мы имеем почти идеальную систему, с помощью которой можно доказать вину того или иного человека в утечке каких-либо данных.

Основную информацию SIEM получает из таких источников, как:

1. Сетевое оборудование (анализ сетевого трафика, контроль изменений).

2. Антивирусы (базы данных, различные события о вирусных атаках, изменения настроек).

3. DLP-системы.

4. Журналы событий от серверов и рабочих станций.

5. Сканеры уязвимостей.

6. NetFlow (сетевой протокол мониторинга трафика) и др.

Основным способом перехвата информации, так же, как и у DLP-системы, являются установка агентов (специальных приложений) на необходимую информационную систему. Агент собирает всю необходимую информацию и передает ее на нужный сервер-коллектор, который будет получать всю полученную от агентов информацию. Агент работает в совокупности с коллекторами, которые используются для понимания определенного журнала событий и системы.

Все данные, полученные от агентов и коллекторов, отправляются на сервер-коррелятор, который обрабатывает все данные в соответствии с политикой безопасности и алгоритмами корреляции и затем отправляет их в хранилище, где будут храниться все журналы событий и записи об инцидентах.

Список используемых источников

1. 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.

2. Дубровин Н. Д., Ушаков И. А., Чечулин А. А. Применение технологии больших данных в системах управления информацией и событиями безопасности// Актуальные проблемы инфотелекоммуникаций в науке и образовании. V Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 3-х т. 2016. Т. 1. С. 348–353.

3. Understanding DLP [Электронный ресурс] // Сайт: infosectoday.com. URL: http://www.infosectoday.com/Articles/DLP/Understanding_DLP.htm (дата обращения 05.01.17).

4. Обзор DLP-систем на мировом и российском рынке [Электронный ресурс] // Сайт: anti-malware.ru. URL: https://www.anti-malware.ru/analytics/Technology_Analysis/DLP_market_overview_2014 (дата обращения 07.01.17).

5. Что такое SIEM? [Электронный ресурс] // Сайт: securitylab.ru. URL: http://www.securitylab.ru/analytics/430777.php (дата обращения. 07.01.17).

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

УДК 621.391.6

МЕТОДЫ КОМПЕНСАЦИИ ХРОМАТИЧЕСКОЙ ДИСПЕРСИИ В ОПТИЧЕСКИХ ЛИНЕЙНЫХ ТРАКТАХ

М. С. Былина, С. С. Попова

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

Рассмотрены методы компенсации хроматической дисперсии и предложены методики расчета длины регенерационного участка ВОЛС с компенсаторами дисперсии на основе специального волокна DCF, волоконной брэгговской решетки с переменным периодом и фотонно-кристаллического волокна PCF.

длина регенерационного участка, хроматическая дисперсия, компенсация дисперсии, волокно для компенсации дисперсии, волоконная брэгговская решетка, фотоннокристаллическое волокно.

Известно, что длина регенерационного участка (РУ) волоконно-оптической системы передачи (ВОСП) может ограничиваться одним из двух факторов – затуханием или хроматической дисперсией (ХД). Рассчитать длины РУ l_{pe} и l_{pd}, ограниченные затуханием и ХД соответственно, для одноканальной ВОСП на основе одномодового ОВ можно по выражениям [1]:

$$l_{pe}(\lambda) = \left(p_{out} - p_n - 2 \cdot a_p - a_d - a_{df} - a_{ez}\right) \Big/ \left(\alpha(\lambda) + a_n / l_{sd}\right), \quad (1)$$

$$l_{pd}(\lambda) = \frac{\pi \cdot c \cdot K^2 \cdot t_T^2}{2 \cdot \lambda^2 \cdot D(\lambda)} \cdot \sqrt{\frac{2 \cdot \left(K_1^2 - 1\right)}{2 + \left(\pi \cdot \Delta\nu \cdot K \cdot t_T\right)^2}}, \quad (2)$$

где p_{out} – уровень сигнала на выходе передатчика; p_n – уровень чувствительности ФПУ; a_p и a_n – средние потери в разъемном и неразъемном соединении оптических волокон (ОВ) соответственно; a_d и a_{df} – дополнительные затухания, вызванные уширением импульса из-за ХД и АЧХ фотоприемного устройства; a_{ez} – энергетический запас, α и D – коэффициент затухания и ХД ОВ; l_{sd} – строительная длина оптического кабеля, λ – длина волны; K – коэффициент, равный отношению ширины гауссовского импульса на выходе регенератора к ширине тактового интервала t_T; $\Delta\nu$ – ширина гауссовского спектра излучения источника на уровне $1/e$; c – скорость света в вакууме; K_1 – коэффициент, учитывающий допустимое дисперсионное расширение импульса и равный отношению ширины импульса на входе регенератора к ширине импульса на выходе регенератора.

Результирующая длина РУ определяется по выражению:

$$l_p(\lambda) = \min\left[l_{pe}(\lambda), l_{pd}(\lambda)\right]. \quad (3)$$

Если $l_{pd}(\lambda) < l_{pe}(\lambda)$, длина РУ ограничена ХД и ее можно увеличить путем компенсации дисперсии. Компенсация ХД может осуществляться как оптическими, так и электронными методами.

Наиболее актуальной задача компенсации является для ВОСП, построенных на основе стандартных одномодовых ОВ, имеющих в окнах прозрачности O, S и L относительно большую положительную ХД. Оптические методы компенсации положительной ХД основаны на включении в ВОСП пассивного оптического устройства – компенсатора с отрицательной ХД. В работе рассмотрены компенсаторы на основе ОВ.

В [3] предлагается считать оптимальным такой компенсатор, при установке которого длины регенерационных участков по дисперсии и затуханию будут одинаковыми. Для расчета длины РУ и длины ОВ в компенсаторе при оптимальной компенсации справедливо:

$$l_{popt}(\lambda) = \frac{A \cdot \alpha_k(\lambda) - B \cdot D_k(\lambda)}{D(\lambda) \cdot \alpha_k(\lambda) - \left(\alpha(\lambda) + a_n / l_{sd}\right) \cdot D_k(\lambda)}, \quad (4)$$

$$l_k = \frac{D(\lambda) \cdot B - A \cdot \left(\alpha(\lambda) + a_n / l_{sd}\right)}{D(\lambda) \cdot \alpha_k(\lambda) - \left(\alpha(\lambda) + a_n / l_{sd}\right) \cdot D_k(\lambda)}. \quad (5)$$

где $A = \frac{\pi c K^2 t_T^2}{2\lambda^2}\sqrt{\frac{2\cdot\left(K_1^2-1\right)}{2+\left(\pi\Delta\nu K t_T\right)^2}}$; $B = p_{out} - p_n - 2a_p - a_d - a_{df} - a_{ez} - a_{dop}$; α_k и D_k – коэффициент затухания и ХД ОВ в компенсаторе; a_{dop} – дополнительные потери, возникающие при вводе и выводе излучения из компенсатора.

В статье рассмотрены два вида компенсаторов ХД – на основе специального ОВ и на основе волоконной брэгговской дифракционной решетки (*Fiber Bragg Grating*, FBG) с переменным периодом. Схемы включения компенсаторов представлены на рис. 1.

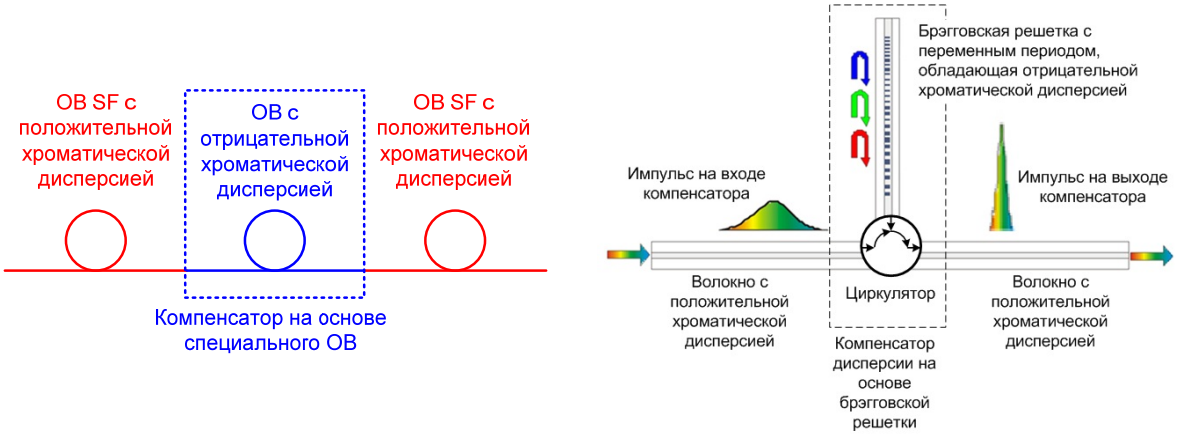


Рис. 1. Схемы включения компенсаторов дисперсии на основе специального ОВ (а) и FBG с переменным периодом (б)

В работе рассматривались два специальных ОВ – ОВ для компенсации дисперсии (*Dispersion Compensation Fiber*, DCF) и фотонно-кристаллическое ОВ (*Photonic Crystal Fiber*, PCF).

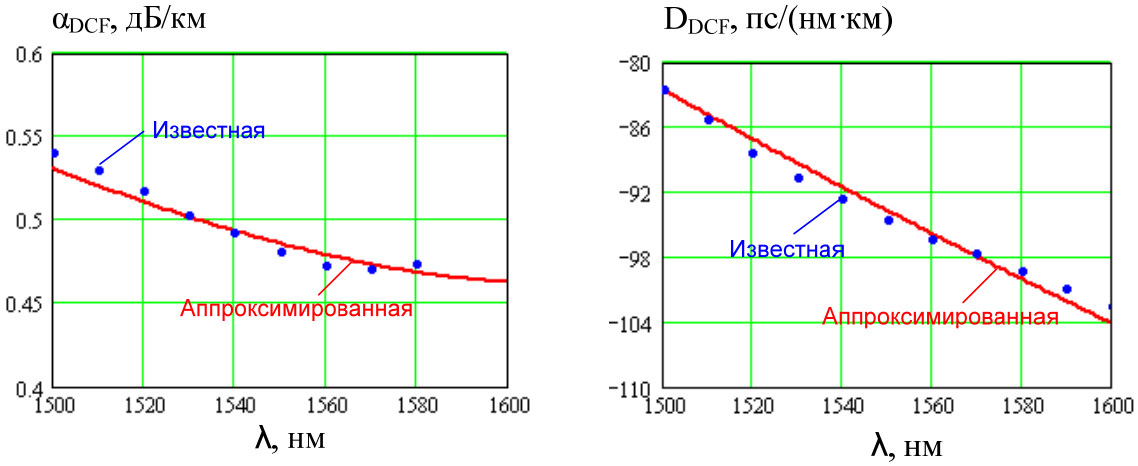


Рис. 2. Спектральные зависимости коэффициента затухания и хроматической дисперсии волокна DCF

На рис. 2 (см. выше) представлены зависимости коэффициента затухания α_{DCF} и хроматической дисперсии D_{DCF} ОВ DCF от длины волны λ [2], которые можно аппроксимировать следующими выражениями:

$$\alpha_{DCF}(\lambda) = \chi/\lambda^4 + g_{\text{inf}} \cdot \Delta\lambda_{\text{inf}} \Big/ \left(2 \cdot \pi \cdot \left[(\lambda - \lambda_{\text{inf}})^2 + (\Delta\lambda_{\text{inf}}/2)^2\right]\right), \quad (6)$$

$$D_{DCF}(\lambda) = S_0\left(\lambda - \lambda_0^4/\lambda^3\right)\Big/4. \quad (7)$$

Значения входящих в (6) и (7) параметров представлены в таблице 1.

ТАБЛИЦА 1. Параметры, полученные в результате аппроксимации

Параметр	Значение
Коэффициент релеевского рассеяния χ, дБ·мкм^4/км	2,469
Резонансная длина волны пика поглощения λ_{inf}, мкм	1,800
Ширина пика поглощения $\Delta\lambda_{\text{inf}}$, нм	1,0
Амплитуда пика поглощения g_{inf}, дБ·мкм/км	20
Длина волны нулевой ХД λ_0, мкм	1,100
Наклон ХД S_0 на длине волны нулевой дисперсии, пс·нм^2/км	–0,39

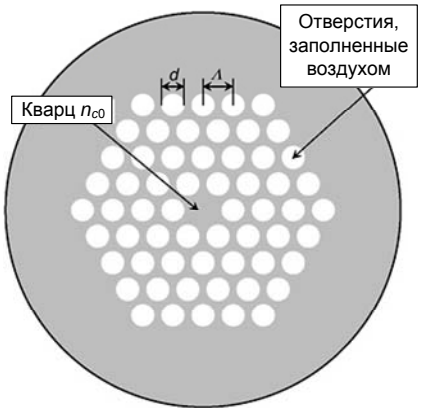


Рис. 3. Конструкция PCF

На рис. 3 показано поперечное сечение ОВ PCF. Известно, что ХД PCF D_{PCF} зависит от диаметра отверстий d и расстояния между ними Λ. На рис. 4 представлены зависимости ХД D_{PCF} от длины волны λ [4]. Из рис. 4 (см. ниже) видно, что наиболее эффективно в качестве компенсатора PCF с $d / \Lambda = 0{,}6$.

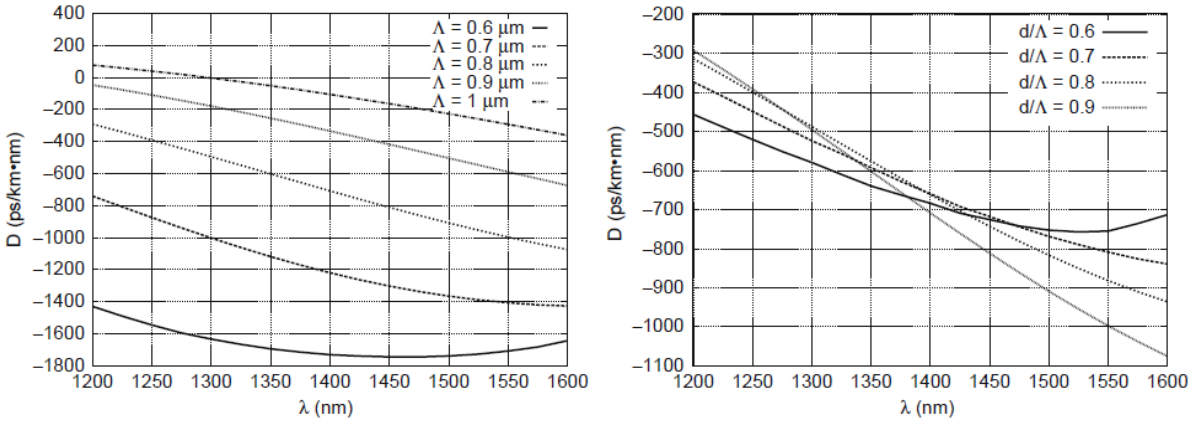
Из рис. 4*а* видно, что для компенсаторов на основе DCF и PCF $a_{dop} = 2a_s$, где a_s – потери в стыке между стандартным ОВ и специальным.

Во второй части работы рассмотрен компенсатор ХД на основе FBG. FBG, период которой меняется от $\Lambda_{\min}$ до $\Lambda_{\max}$:

$$\Lambda_{\min} = \frac{\lambda - \Delta\lambda_{chirp}/2}{2n_{eff}}, \Lambda_{\max} = \frac{\lambda + \Delta\lambda_{chirp}/2}{2n_{eff}} \quad (8)$$

обладает отрицательной ХД, которую можно рассчитать по выражению:

$$D_G = 2n_{eff} \Big/ \left(c \cdot \Delta\lambda_{chirp}\right). \quad (9)$$



а) б)

Рис. 4. Дисперсионные характеристики PCF волокна
при: а) различных Λ и фиксированном d/Λ; б) различных d/Λ и фиксированном Λ

В (8), (9) n_{eff} – эффективный показатель преломления; $\Delta\lambda_{chirp}$ – ширина диапазона, в котором работает решетка, которая принималась равной ширине спектра оптического сигнала $\Delta\lambda_{chirp} = \Delta\lambda \approx \Delta\nu \cdot \lambda^2/c$.

Из рис. 4*б* видно, что для компенсатора на основе FBG $a_{dop} = 4a_{pk} + a_c$, где a_{pk} – потери в соединениях между циркулятором и ОВ, a_c – потери в циркуляторе.

По выражениям (1–9) были проведены расчеты длин РУ без использования компенсации и с использованием оптимальной компенсации дисперсии. Расчеты проведены при следующих параметрах: λ = 1550 нм; p_{out} = 10 дБм; l_{sd} = 6 км; a_p = 0,2 дБ; a_n = 0,05 дБ; a_s = 0,8 дБ; a_{ez} = 3 дБ; a_d = 0,67 дБ; a_{df} = 0,67 дБ; K = 0,55; K_1 = 1,17; a_{pk} = 0,2 дБ; a_c =1 дБ; n_{eff} = 1,44. Значения p_n для различных систем передачи приведены в таблице 2. Результаты расчетов представлены в таблице 3 (см. ниже).

ТАБЛИЦА 2. Значения чувствительности ФПУ

Система передачи	STM-1	STM-4	STM-16	STM-64
Скорость передачи B, Гбит/с	0,155	0,622	2,5	10
p_n, дБм	–34	–28	–24,5	–21

По результатам расчетов можно сделать следующие выводы:

1) С увеличением ширины спектра излучения источника и скорости передачи длина РУ уменьшается.

2) Использование компенсаторов ХД позволяет существенно увеличить длину РУ.

3) При компенсации дисперсии в узком диапазоне длин волн эффективность компенсаторов на основе FBG и PCF выше, чем компенсаторов на основе ОВ DCF.

ТАБЛИЦА 3. Результаты расчета длины РУ

Δν, ГГц	Система передачи	B, Гбит/с	Длина РУ без компенсации l_p, км	Длина РУ с оптимальной компенсацией, км					
				DCF		FBG		PCF, $d / \Lambda = 0{,}6$	
				$l_{p\,opt}$, км	l_k, км	$l_{p\,opt}$, км	l_k, мм	$l_{p\,opt}$, км	l_k, км
100	STM-1	0,155	105,72	135,6	9,2	164,06	83,05	164,30	0,62
	STM-4	0,620	24,43	105,0	16,1	137,78	166,11	135,23	1,15
	STM-16	2,5	6,55	89,5	16,6	122,45	172,98	119,66	1,20
	STM-64	10	1,62	77,0	15,1	107,12	158,18	104,88	1,09
10	STM-16	2,5	62,37	99,1	8,8	122,45	8,96	122,60	0,64
	STM-64	10	12,68	80,5	13,6	107,12	19,93	105,32	1,01
1	STM-64	10	36,11	81,5	12,6	107,12	13,08	105,46	0,98

Список используемых источников

1. Глаголев С. Ф. Особенности проектирования современных высокоскоростных волоконно-оптических систем передачи // Фотон-экспресс. 2006. № 6. С. 28–38.

2. Листвин А. В., Листвин В. Н., Швырков Д. В. Оптические волокна для линий связи. М.: ЛЕСАРарт, 2003. 288 с.

3. Былина М. С., Глаголев С. Ф., Кузнецова Н. С., Рык О. Н. Компенсация дисперсии в оптических линейных трактах с использованием DWDM // Фотон-Экспресс. 2009. № 7. С. 32–35.

4. Poli F., Cucinotta A., Selleri S. Photonic Crystal Fibers: Properties and Applications. Springer, 2007. 234 p.

УДК 004.056.53

МЕТОДЫ СБОРА И АНАЛИЗА СЕТЕВОГО ТРАФИКА НА ОСНОВЕ ТЕХНОЛОГИЙ БОЛЬШИХ ДАННЫХ

Н. С. Василишин, Н. Д. Дубровин, И. А. Ушаков, А. А. Чечулин

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

В настоящее время, доля применения технологий «Больших данных» для быстрой обработки огромных объемов неструктурированных данных, таких как поток сетевого

трафика, растет. Технологии «Больших данных» построены на методах и алгоритмах сбора и анализа информации, позволяющих на основе заранее заданных условий получать результат анализа в требуемой форме, удобной для восприятия и принятия решения. В статье рассмотрены методы сбора и анализа сетевого трафика с использованием технологий «Больших данных».

Большие данные, методы сбора и анализа данных, обнаружение компьютерных атак, сетевой трафик.

Парадигма распределенных вычислений MapReduce впервые описана компанией Google в 2004 г. На основе этой парадигмы была разработана платформа Hadoop – набор свободно распространяемых программных средств с открытым исходным кодом, предназначенный для обработки огромных массивов неструктурированных данных на кластерах из большого количества узлов [1]. В настоящее время использование систем распределенной обработки Больших данных становится все более распространенным в области торговли, экономики, инфокоммуникаций, средств массовой информации. При внедрении таких систем важными аспектами являются методы и алгоритмы сбора, предобработки и анализа информации, так как от них зависит точность и актуальность полученных при обработке данных результатов, и как следствие возможность их использования с целью получения прибыли.

Сбор и предобработка являются важным этапом, позволяющим подготовить информацию к ее дальнейшему анализу. Предобработка необходима независимо от того, какие методы и алгоритмы используются непосредственно при обработке данных. Основные методы предобработки:

– очистка – исключение факторов, затрудняющих работу алгоритмов анализа, восстановление целостности, преобразование форматов;

– оптимизация – выявление и исключение незначащих признаков из поступающих данных, адаптация исходной информации для каждой конкретной задачи.

Для сбора, формирования потоков и предобработки сетевого трафика в технологиях Больших данных существует несколько инструментов – Apache Sqoop, Apache Kafka, Apache Chukwa и Apache Flume.

Рассматриваемый в статье, Apache Flume предназначен для управления потоками данных [2]. Он собирает информацию из различных источников и направляет в HDFS. Организация потоков с использованием Apache Flume представляет собой «конвейер», состоящий из нескольких узлов, которые управляют потоками данных и их предобработкой.

– событие (*event*) – полезная нагрузка с дополнительными заголовками, которая принимается за единицу данных, передаваемых от источника к конечному узлу назначения;

– поток (*flow*) – перемещение событий от источника отправления до конечного узла назначения;

– агент (*agent*) – процесс, в рамках которого функционирует группа компонентов Apache Flume. Имеет возможность получать, хранить и передавать события следующему узлу;

– клиент (*client*) – внешнее приложение или сервис, работающее в точке возникновения событий и передающее их агенту;

– канал (*channel*) – буфер для событий, полученных от источника. Пассивный компонент, не инициирует действий самостоятельно;

– источник (*source*) – реализация интерфейса, который передает события, полученные с помощью различных механизмов, в канал;

– сток (*sink*) – реализация интерфейса, которая извлекает событие из канала и отправляет на следующий этап обработки – агенту или распределенной файловой системе [2].

Структура потока выглядит следующим образом: 1. Клиент отправляет событие агенту; 2. Источник, входящий в состав агента, передает событие в канал, которых может быть несколько; 3. Сток, работающий в этом же агенте, забирает событие из канала. Пример структуры потока представлен на рисунке.

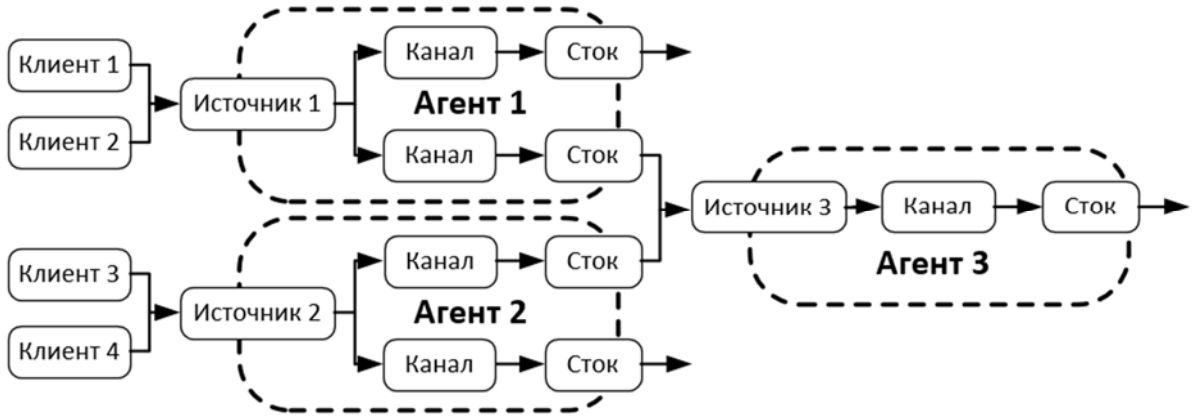


Рисунок. Общая структура потока

Каналы отделяют источники от стоков, используя привычную модель обмена данными между производителем и потребителем. Это позволяет источникам и стокам иметь разную производительность и характеристики времени выполнения, а также эффективно использовать физические ресурсы, доступные для системы.

Для гарантированной надежной доставки данных используются транзакции. При перемещении события между двумя агентами, запускаются две транзакции: одна на агенте, который отправляет событие, вторая на агенте, который принимает событие. Для завершения транзакции отправляющий

агент должен получить подтверждение об успешности действия от принимающего агента. При правильной настройке цепочки узлов не может быть ситуации, когда данные потеряются или будут переданы не полностью.

Кроме алгоритмов сбора данных, для защиты компьютерный сетей и систем от сетевых угроз требуется разработать алгоритмы, позволяющие анализировать и систематизировать сетевой трафик, поступающий в вычислительный кластер. Методы анализа напрямую зависят от типа сетевых атак, например, DDoS, SQL-инъекции, DNS-туннелирование. В качестве признаков, по которым производится анализ пакета, взяты протоколы IP, TCP, DNS, HTTP.

На этапе работы функции Map собирается статистика всех перечисленных признаков:

– сетевой уровень – IP-адрес источника;

– транспортный уровень – наличие флагов SYN или ACK при использовании протокола TCP;

– прикладной уровень – классифицировать пакеты по размеру, в соответствии с количеством полезной нагрузки на пакет, если используется DNS;

– прикладной уровень – отметка об использовании HTTP.

На этапе работы функции Reduce полученная статистика по признакам агрегируется. Результатом выполнения MapReduce задачи является информация о суммарном количестве пакетов в сети в минуту, с помощью которой, имея усредненное общее значение, можно детектировать всплески сетевой активности и классифицировать их как DDoS-атаки транспортного уровня – соотношение запросов SYN к ACK в ходе установления TCP-соединений в минуту [3]; открытый DNS-туннель – определение наличия вложенного трафика по общему количеству DNS-сообщений с малой и большой длиной; количество HTTP-запросов на прикладном уровне. Полученный результат передается SIEM-системе, которая после анализа и корреляции предоставляет информацию оператору в виде отчета о событиях безопасности сети [4].

В данной статье рассмотрен принцип работы и основные части системы Apache Flume, которая позволяет сгруппировать потоки данных, передать и подготовить их к обработке в распределенной файловой системе вычислительного кластера, реализованного с использованием Apache Hadoop и SIEM-системы OSSIM [1]. Обработка поступающих в кластер Больших данных выполняется на основе представленного метода и признаков, по которым можно обнаружить присутствие «постороннего» трафика и наличие атак на компьютерную сеть [5, 6].

Работа выполнена при финансовой поддержке РНФ грант № 15-11-30029 в СПИИРАН.

Список используемых источников

1. Дубровин Н. Д., Ушаков И. А., Чечулин А. А. Применение технологии Больших Данных в системах управления информацией и событиями безопасности // Актуальные проблемы инфотелекоммуникаций в науке и образовании. V Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 3-х т. 2016. Т. 1. С. 348–353.
2. Apache Flume – Architecture of Flume NG / Arvind Prabhakar – Cloudera Engineering Blog, December 2011. 364 p.
3. Чечулин А. А., Котенко И. В. Комбинирование механизмов защиты от сканирования в компьютерных сетях // Информационно-управляющие системы. 2010. № 12. С. 21–27.
4. Алейников А. А., Билятдинов К. З., Красов А. В., Левин М. В. Контроль, измерение и интеллектуальное управление трафиком: монография. СПб. : Центр научно-информационных технологий «Астерион», 2016. 92 с.
5. Котенко И. В., Десницкий В. А., Чечулин А. А. Исследование технологии проектирования безопасных встроенных систем в проекте Европейского сообщества SecFutur // Защита информации. Инсайд. 2011. № 3 (39). С. 68–75.
6. Kotenko I., Stepashkin M. Analyzing Vulnerabilities and Measuring Security Level at Design and Exploitation Stages of Computer Network Life Cycle // Lecture Notes in Computer Science. V. 3685. 2005. P. 317–330.

УДК 004.7 (004.942)

АНАЛИЗ УЯЗВИМОСТИ СЕТИ SIP К ФРОД-УГРОЗАМ ПО РЕЗУЛЬТАТАМ ИМИТАЦИИ АТАК НА СЕТИ ОПЕРАТОРА

И. Ю. Веремийчук, В. С. Елагин

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

С каждым годом увеличивается количество операторов связи, предоставляющих различным компаниям и учреждениям возможность подключения к ТфОП посредством использования протокола SIP. В статье рассмотрены основные схемы взаимодействия операторов SIP-телефонии и их клиентов и возможные атаки со стороны злоумышленников, которые могут быть реализованы на различных участках сети NGN.

SIP-телефония, fraud, SBC, защита от фрода.

В современном мире IP-телефония все чаще заменяет собой классическую телефонную связь. Использование телефонии на базе сетей NGN зачастую дешевле и проще, чем монтаж новых телефонных линий. Но использование телефонии на базе протокола SIP ставит перед IT-подразде-лением

оператора вопрос об обеспечении безопасности своей сети и защите от атак извне, так как последствия таких атак наносят имиджевый урон компании и лишают прибыли.

Наиболее часто встречающимися угрозами для оператора SIP-телефонии и его клиентов являются атаки DoS (*Denial of service*) на операторское оборудование и VoIP Fraud мошенничество. В данной работе будут более подробно рассмотрены варианты фрод-атак злоумышленниками.

Как отмечается в работе [1] со ссылкой на данные Ассоциации CFCA (*Communication Fraud Control Association*) по контролю за угрозой fraud (фрод – использование услуг связи без их оплаты), потери операторов связи во всем мире составляют бóльшую долю от их общих доходов. Это относится ко многим типам сетей связи, причем такие потери операторов от фрод-угроз в сетях передачи данных по сетям IP выше, чем во многих сетях связи других типов.

Данная работа посвящена анализу риска информационной безопасности (ИБ) некоторых из фрод-угроз по результатам тестов, проведенных на стенде, имитирующем SIP-транк между двумя операторами. Под риском ИБ рассматривается характеристика последствий реализации фрод-угроз в сети SIP. При этом учитывалось, что одним из наиболее чувствительных к угрозам фрода является участок взаимодействия разных операторов связи. Широкое применение на сетях операторов связи получили так называемые пограничные контроллеры сессий (*Session Border Controller* – SBC). SBC размещается на границе сети оператора связи, транслирует сигнальный поток и медиа-поток, обеспечивая единую точку входа-выхода операторской сети, и реализует широкий спектр функций контроля безопасности связи (сокрытие топологии сети оператора связи, защиту от угрозы «анализ трафика», контроль обмена сигнальными сообщениями, фильтрацию трафика на разных уровнях и др.).

В настоящее время протокол SIP используется в двух вариантах взаимодействия:

- между программным коммутатором (*SoftSwitch*) и абонентским терминалом – схема SIP-access;
- между двумя программными коммутаторами для обеспечения межстанционного взаимодействия – схема SIP-trunk. Ее особенностью является отсутствие возможности использования механизма SIP-авторизации, что создает предпосылки для MitM (*Man in the middle*) атак злоумышленника.

Имитация фрод-атак производилась на двух тестовых схемах:

1. Схема, моделирующая взаимодействие двух операторов по протоколу SIP, при этом между софтсвичами операторов организован SIP-trunk. На границе каждого оператора установлен SBC. Участок сети между двумя SBC является незащищенным (обозначен как Internet на рис. 1).

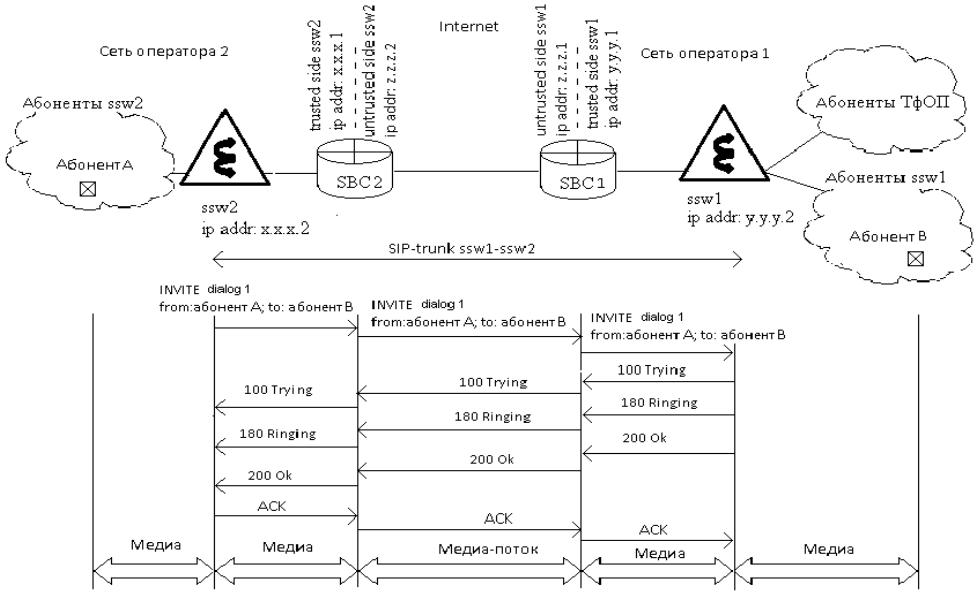


Рис. 1. Схема моделирования канала взаимодействия между двумя операторами связи (SIP-trunk)

2. Схема, моделирующая организацию абонентского SIP-доступа (SIP-access) к софтсвичу через незащищенную сеть (рис. 2), что использовалось при имитации MitM-атаки злоумышленника. Такой вид атак на сеть SIP рассмотрен в публикациях зарубежных авторов (например, [3]).

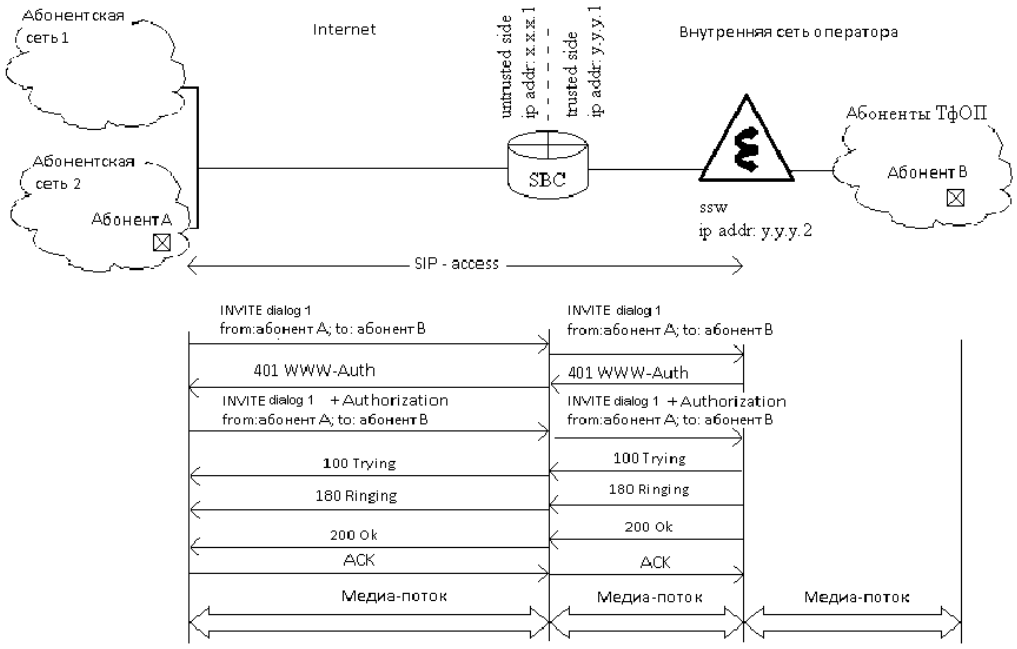


Рис. 2. Схема моделирования канала абонентского доступа (SIP-access)

Далее рассмотрены два алгоритма MitM-атак и указаны возможные варианты защиты.

Перехват и модификация сообщения INVITE от легитимного пользователя.

Данная атака использует возможность SIP-клиента одновременно поддерживать более одной активной сессии и факт отсутствия авторизации при вызове через SIP-trunk. В этом случае злоумышленник перехватывает запрос INVITE, изменяет параметры вызываемого абонента (поле <To:>), медиа-сессии (параметры своего сетевого устройства в SDP) и идентификации диалога и далее перехватывает все последующие сообщения в рамках SIP-сессии и отвечает от имени легитимного пользователя, что позволяет ему установить медиа-сессию между своим SIP-терминалом и вызываемым абонентом (рис. 3).

В данном случае атаку значительно усложнит настройка на SBC строгих правил фильтрации Source Host:Port, т. е. в приведенной схеме допустим обмен SIP и RTP пакетами только между SBC1 и SBC2.

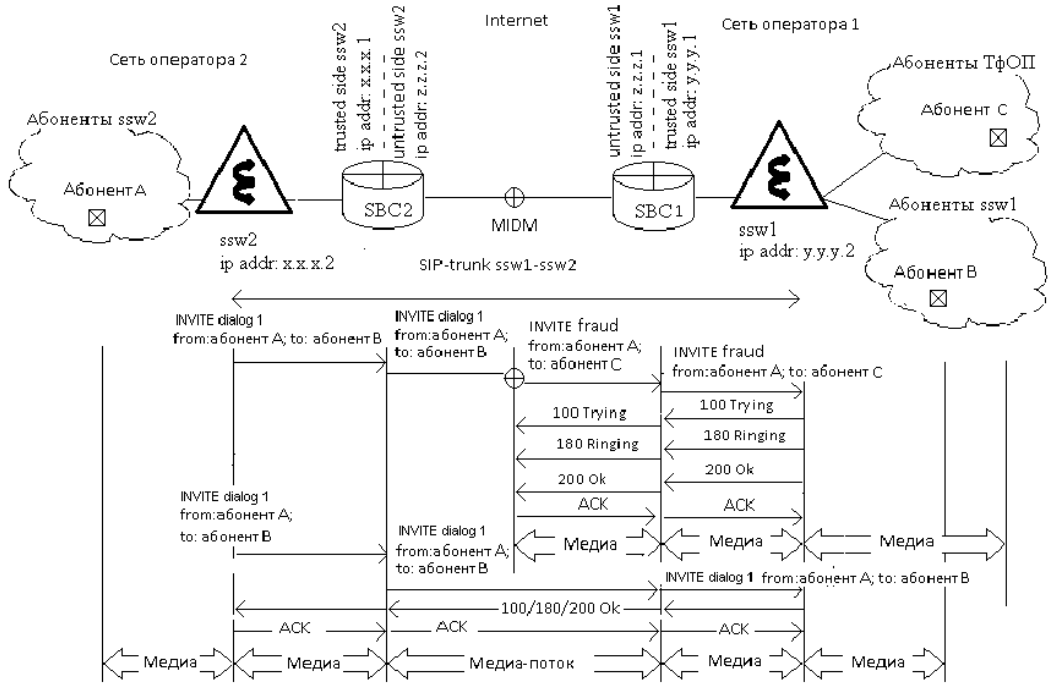


Рис. 3. Схема реализации атаки модификации запроса INVITE в SIP-trunk

Имитация механизма переадресации вызова легитимным пользователем с использованием сообщения 302 Moved Temporarily.

Данная атака обусловлена возможностями протокола SIP по управлению сессиями – реализацию услуги мобильности пользователя с помощью переадресации входящего вызова (RFC 5806) [4].

Атака производится следующим образом: злоумышленник звонит на номер телефона пользователя-жертвы и перехватывает поступающий запрос INVITE, далее формирует и отправляет софтсвичу оператора SIP-сообщение 302 Moved Temporarily в соответствии с RFC 5806 [4], вследствие чего софтсвич устанавливает соединение между злоумышленником и абонентом, на которого был переадресован вызов. Такая атака возможна и на участке SIP-trunk. Защитой от атак такого вида может быть запрет на обработку всех сообщений 302 Moved Temporarily и реализацию всех переадресаций средствами софтсвича, но такой вариант ограничивает возможности SIP-терминала пользователя.

В заключение хотелось бы отметить, что результаты проведенного тестирования показывают актуальность проведения дальнейших исследований – рассмотрение других видов Fraud-мошенничества, защиту от возможных DDoS-атак, а также необходимости операторов использовать дополнительные средства для защиты от мошенничества. В частности, следует:

- использовать дополнительные расширения протокола SIP – SIP-TLS, а также SRTP и ZRTP для защиты медиа-сессии.
- устанавливать SBC на границе сети оператора и производить его тонкую настройку, в том числе выполнять строгую фильтрацию и проверку содержимого поступающих SIP-сообщений.

Список используемых источников

1. Communications Fraud Control Association (CFCA). 2011 Global Fraud Loss Survey. URL: www.cfca.org (дата обращения 05.02.2017).

2. Бельфер Р. А., Морозов А. М. Информационная безопасность сети связи для соединения абонентов ТфОП/ISDN через SIP-T // Электросвязь. 2012. № 3. С. 22–25.

3. Billing Attacks on SIP-Based VoIP Systems/ Zhang R., et al. // Proc. WOOD ’07 Proceedings of the first USENIX workshop on Offensive Technologies, USENIX Association Berkley, CA, USA, 2007.

4. RFC 5806. S. Levy, M. Mohali. Diversion Indication in SIP. 2010. URL: https://tools.ietf.org/html/rfc5806 (дата обращения 05.02.2017).

УДК 004.725.5

ИССЛЕДОВАНИЕ КЛИЕНТСКОГО СОСТАВА В СЕТИ БЕСПРОВОДНОГО ДОСТУПА

А. С. Викулов, А. И. Парамонов

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

В современных реалиях проектные задачи все чаще ставят вопросы, по оценке пропускной способности беспроводных сетей. При этом необходимо понимать состав клиентских устройств и их возможности, ввиду влияния этих факторов на генерируемую ими нагрузку в беспроводной сети. Вместе с тем рекомендации производителей оборудования в данной области зачастую очень приблизительны. В рамках данной работы был проведен 30-дневный мониторинг действующей беспроводной сети доступа. Собраны данные о возможностях клиентских устройств и сделаны выводы об их соответствии рекомендациям лидеров рынка оборудования Wi-Fi.

IEEE 802.11, клиентский состав, Wi-Fi.

Введение

Современные беспроводные локальные сети (БЛВС) ставят перед проектантом задачи, требующие адекватной оценки числа пользователей, их качественных и количественных возможностей, равно как и знаний о предполагаемом пользовательском трафике. Не всегда (а на практике – почти никогда) эти данные возможно получить от заказчика на этапе составления задания на проектирование. Поэтому приходится оперировать рекомендациями, например, [1, 2, 3, 4], дающими лишь ограниченный набор инструкций. С другой стороны, как ранее упоминалось автором [5], клиентский состав и возможности устройств – являются важнейшими параметрами, необходимыми для адекватной оценки производительности БЛВС в том числе и с высокой плотностью пользователей. Без опоры на эти данные очень трудно сделать правильный выбор числа, характеристик и местоположения точек доступа (ТД) проектируемой БЛВС.

Решению этих задач должен способствовать сбор данных статистического мониторинга нагруженных трафиком БЛВС с целью анализа клиентского состава и технических возможностей клиентских устройств. Такому анализу и посвящена данная работа.

Постановка задачи

Для оценки соотношения числа клиентов разных версий стандарта IEEE 802.11 а также обработки данных об установленных соединениях был

произведен сбор и анализ статистической информации в БЛВС, построенной на базе решения Avaya Networking. За период длительностью в один месяц с 19 сентября по 19 октября 2016 года были проанализированы данные системы мониторинга сети Wi-Fi. Сбор статистической информации выполнялся программным комплексом Avaya Wireless Orchestration System (WOS) версии 8.1. Помимо данного периода времени, был проведен сбор статистики сети Wi-Fi во время работы под нагрузкой во время проведения IT-семинара в конференц-зоне здания. Семинар проводился в течение одного дня 14.12.2016. Характеристики сети и основные параметры мониторинга приведены в таблице 1.

ТАБЛИЦА 1. Параметры сбора данных

Параметр	Ед. изм.	Значение за период	
		30 дней	1 день
Число точек доступа в сети WLAN	шт.	33	2
Совокупное время мониторинга	Час	720	6
Время недоступности ТД за период мониторинга	ТД* мин	53	0
Площадь покрытия сети WLAN	кв. м	14797	320
Средняя площадь покрытия на ТД	кв. м	448	160

БЛВС состоит из 33 точек доступа, с двумя радиомодулями каждая. Сбор статистики производился на всех 33 ТД в течение месяца, и на двух ТД во время проведения семинара. Время простоя всех ТД в течение месяца составило 53 ТД*мин, т. е. 0,0037 % от совокупного времени мониторинга. Под временем простоя понимается совокупное время недоступности ТД для клиентов:

$$T_{\text{ПР}} = \sum_{i=1}^{N} T_i \ ,$$

где T_i – время для каждой ТД в течение периода мониторинга, когда она по каким-либо причинам отсутствовала в сети (например, перезагружалась из-за сбоя питания).

Результаты

В таблице 2 приведены возможности клиентских устройств с точки зрения поддерживаемых версий стандарта 802.11.

ТАБЛИЦА 2. Характеристики клиентских устройств

Поддерживаемые версии 802.11	Число устройств за период		Поддерживаемые версии 802.11	Число устройств за период	
	30 дней	1 день		30 дней	1 день
g	9	0	agn	81	0
ag	3	0	bgn	583	22
an	5	0	anac	1	0
bg	18	0	abgn	457	43
gn	177	0	abgnac	454	43
abg	6	0	N/A	54	0

Всего за месячный период в сети было зарегистрировано 1848 уникальных клиентских устройств (MAC-адресов). За однодневный период число уникальных MAC-адресов составило 108, т. е. порядка 1 устройства на 2 кв. м площади, что является значением близким к значению характерному для БЛВС высокой плотности.

Соотношение между наиболее современными версиями стандарта IEEE802.11 поддерживаемыми теми клиентами, для которых такая информация доступна, приведено в таблице 3.

ТАБЛИЦА 3. Последняя поддерживаемая версия за оба периода мониторинга

Последняя поддерживаемая версия стандарта 802.11	Число устройств		% от общего числа	
	30 дней	1 день	30 дней	1 день
g	36	0	2	0
n	1303	65	72,6	60,2
ac	455	43	25,4	39,8

Соотношение между ассоциациями клиентов в двух различных частотных диапазонах приведено в таблице 4.

ТАБЛИЦА 4. Активность в частотных диапазонах за оба периода мониторинга

Диапазон, ГГц	Число ассоциаций		% от общего числа	
	30 дней	1 день	30 дней	1 день
2,4	1809	59	59,2	54,6
5	1246	49	40,8	45,4

Число ассоциаций превышает число уникальных устройств ввиду того, что некоторые устройства ассоциировались с сетью несколько раз в течение месячного мониторинга.

Выводы

1. Хотя устройства, работающие в диапазоне 5 ГГц, пока не преобладают, их доля стабильно растет. Поэтому данная тенденция должна быть соответствующим образом поддержана сетевой инфраструктурой. В целом, по сравнению с обычным пользователем сети Wi-Fi, посетители ИТ-семинара пользуются гораздо более современными устройствами с позиции поддержки ими новейшей версии стандарта 802.11, и диапазона 5 ГГц.

2. Если нет прямой необходимости, нет смысла разрешать ассоциацию с БЛВС по стандарту 802.11b, поскольку такие пользовательские устройства на практике уже не встречаются. Этот факт хорошо соотносится с рекомендациями производителей.

3. Средняя доля потерь кадров в сети за месяц составила 1,75 %, что является хорошим показателем. В литературе, например, [6, стр. 11] и [7, стр. 39], обычно встречаются рекомендации ориентироваться на процент потерь порядка 10 %.

Дальнейшая работа

С целью дальнейшего уточнения и обобщения поднятых вопросов предполагается сделать анализ следующих данных:

– сбор статистики на той же БЛВС за период 6 месяцев;
– сбор статистики на более нагруженной БЛВС большего масштаба;
– анализ характеристик трафика с целью обобщения и выявления закономерностей.

Список используемых источников

1. Andrew von Nagy. Aerohive Design & Configuration Guide. High Density Wi-Fi. Aerohive Networks. 2013.

2. Chuck Lukaszewski. Aruba VHD 802.11ac Networks VRD. Engineering and Configuration Guide. 2015.

3. Meru Networks Best Practices Guide for High-Density Design and Deployment. 2012.

4. Meraki High Density Wi-Fi Deployment Guide (Cisco Validated Design). AID 4567. 2016.

5. Викулов А. С. Проблемы оценки производительности Wi-Fi высокой плотности // ИТ-Стандарт 2016. VII межд. конф. 6–7 декабря 2016 года: сб. тр. М. : МИРЭА, 2016. С. 235–241.

6. Timo Vanhatupa. Wi-Fi Capacity Analysis for 802.11ac and 802.11n: Theory & Practice. 2013. 21 p.

7. Chuck Lukaszewski, Liang Li. Aruba very high density 802.11ac networks. Theory Guide. 2015.

УДК 621.396.49

ЭФФЕКТИВНОСТЬ ПРИМЕНЕНИЯ АЛГОРИТМА ОПТИМИЗАЦИИ МУРАВЬИНОЙ КОЛОНИИ В ЗАДАЧЕ СОВМЕСТНОЙ ДИНАМИЧЕСКОЙ МАРШРУТИЗАЦИИ

Ю. С. Винтенкова, С. В. Козлов

Казанский национальный исследовательский технический университет им. А. Н. Туполева – КАИ

Статья посвящена разработке и моделированию эвристического алгоритма оптимизации муравьиной колонии с целью снижения вычислительной сложности метода совместной динамической маршрутизации, применяемого для уменьшения влияния внутрисистемных помех на характеристики сети широкополосного радиодоступа.

маршрутизация, алгоритм оптимизации муравьиной колонии, метод совместной динамической маршрутизации, целочисленное программирование.

Метод совместной динамической маршрутизации был разработан для повышения пропускной способности и уменьшения времени доставки информации в сетях широкополосного радиодоступа за счет снижения потока внутриситсемных помех [1]. Для объяснения принципа работы этого метода рассмотрим сеть широкополосного радиодоступа (рис. 1).

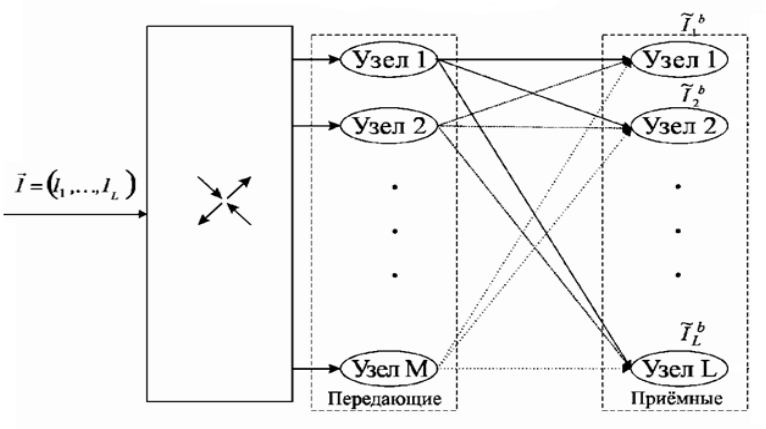


Рис. 1. Структура сети широкополосного радиодоступа

На вход маршрутизатора поступает вектор информации, содержащий количество пакетов, которое нужно доставить до каждого из приемных узлов за время T^I. В соответствии с количеством передающих и приемных узлов сети рассчитывается множество допустимых маршрутов B.

Обозначим за T^A единый интервал времени, за который осуществляется доставка пакетов во всех каналах сети связи. Оптимальный вектор кратности использования маршрутов выбирается по критерию минимума времени доставки при условии доставки всех пакетов, поступивших за время T^I:

$$\begin{cases} \vec{N}^{w\_opt} = \arg\min\limits_{\vec{N}^w}\left(\sum\limits_{b=1}^{B} N_b^w\right) \\ \sum\limits_{b=1}^{B} N_b^w \cdot V_{lb} \cdot T^A \geq I_l, \quad l = \overline{1,L} \\ N_b^w \geq 0, \qquad\qquad b = \overline{1,B} \\ N_b^w \in Z, \end{cases}$$

где V_{lb} − скорость доставки данных до приёмного узла I по маршруту b.

Нахождение оптимального вектора кратности использования маршрутов решается с помощью методов целочисленного линейного программирования. Эти методы позволяют найти оптимальный вектор кратности использования маршрутов, но имеют высокую вычислительную сложность, поэтому применение алгоритма маршрутизации, основанного на целочисленном программировании, в реальных маршрутизаторах затруднительно.

Для уменьшения вычислительной сложности были рассмотрены варианты перехода от целочисленного программирования к нецелочисленному (использование симплекс-метода) и использования эвристического алгоритма оптимизации, в качестве которого было решено использовать алгоритм оптимизации муравьиной колонии, так как он обладает меньшей вычислительной сложностью по сравнению с генетическим алгоритмом и алгоритмом имитации отжига [2].

Для использования алгоритма оптимизации муравьиной колонии в методе совместной динамической маршрутизации за уровень феромона принимались объемы данных, которые нужно передать, а за видимости (величина, выражающая предпочтительность выбора маршрута) были приняты скорости передачи для каждого из вариантов маршрута. Формула вычисления вероятности перехода из одного узла в другой принимает вид:

$$P = \frac{\sum\limits_{l=1}^{L} I_l^{\alpha} \cdot V_{lb}^{\beta}}{\sum\limits_{b=1}^{B}\sum\limits_{l=1}^{L} I_l^{\alpha} \cdot V_{lb}^{\beta}}.$$

Затем определяется вариант с наибольшей вероятностью, а величина объема данных, которые нужно передать по этому варианту, уменьшается в соответствии с объемом данных $V_{lb} \cdot T^A$.

Алгоритма оптимизации муравьиной колонии имеет настраиваемые параметры α (вес феромона) и β (вес видимости), которые влияют на качество решения. Для определения величины этих параметров было проведено моделирование муравьиного алгоритма для сети со смешанным трафиком. Установлено, что при значениях α = 1 и β = 1 время доставки пакетов было минимальным.

Для этих параметров было проведено моделирование сети связи, результаты которого представлены в таблице.

ТАБЛИЦА. Результаты моделирования метода совместной динамической маршрутизации

	Статическая маршрутизация	Целочисленное программирование	Симплекс-метод	Оптимизация муравьиной колонии
Среднее время доставки, с	0,00248	0,00209	0,00209	0,00212
Суммарная скорость, Мбит/с	104,56	121,4	121,35	118,05

Результаты моделирования показывают, что алгоритм оптимизации муравьиной колонии несколько уступает методам целочисленного линейного программирования и симплекс методу по полученным характеристикам сети связи, в то же время количество операций, необходимое для реализации алгоритма оптимизации муравьиной колонии, линейно зависит как от количества маршрутов, так и от объёма передаваемой информации, что позволяет эффективно использовать для формирования оптимального набора маршрутов.

Кроме того, применение алгоритма оптимизации муравьиной колонии для формирования оптимального набора маршрутов позволяет реализовать итерационный алгоритм маршрутизации и снизить задержки в сети связи.

Список используемых источников

1. Винтенкова Ю. С., Козлов С. В., Спирина Е. А. Анализ эффективности метода совместной динамической маршрутизации в сетях широкополосного радиодоступа с трафиком протоколов TCP, HTTP, FTP [Электронный ресурс] // Журнал радиоэлектроники. 2016. № 1. С. 17. URL: http://jre.cplire.ru/jre/jan16/3/text.pdf (дата обращения: 01.03.2017).

2. Штовба С. Д. Муравьиные алгоритмы // Математика в приложениях. 2003. № 4. С. 70–75.

УДК 004.056.5

РИСКИ РАЗВИТИЯ ПРОЕКТОВ НА ОСНОВЕ ОТКРЫТЫХ ДАННЫХ С ПОЗИЦИИ НОВОЙ ДОКТРИНЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Л. А. Виткова[1], Е. И. Денисов[1], О. Н. Рябова[2], Д. В. Сахаров[1]

[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 (Роскомнадзор) по Северо-Западному федеральному округу

Открытые данные активно развиваются во всем мире. Не является исключением и наша страна. Интерес к открытым данным проявляет в том числе и государство. Однако, на данный момент угрозы информационной безопасности только возрастают. В статье рассматриваются актуальные возможные проблемы дальнейшего развития открытых данных с точки зрения новой Доктрины информационной безопасности.

открытые данные, большие данные, доктрина, информационная безопасность, управление информационной безопасностью и событиями.

В середине первого десятилетия XXI века заметно возрос интерес к теме открытых данных («*Open Data*»). Основной смысл, составляющий основу этой идеи – предоставить абсолютно любому пользователю интернета данные в машиночитаемой формате, то есть в виде определенного массива, для осуществления свободного использования без каких-либо рамок лицензионных ограничений.

Важно, что информация, выложенная в виде открытых данных, должна отвечать требованиям актуальности, первичности и полноты [1]. Качество продукта, созданного на основе открытых данных, во многом зависит от соблюдения этих требований. Результатом обработки «открытых данных» является приложение «Яндекс.Транспорт», значительно облегчающее использование общественного транспорта. Другим примером, позволяющим буквально «узнать на что тратятся наши налоги» является приложение «ГосЗатраты».

Сейчас открытые данные все теснее и теснее сплетаются с такими понятиями как «большие данные» («*Big Data*», комплекс технологий, позволяющих эффективно обрабатывать и структурировать очень большие объемы информации). В скором времени ожидается экспоненциальный рост «интернета вещей» («*Internet of Things*») – огромного количества предметов, связанных в единую сеть для взаимодействия, как и с внешней средой так

и между собой. Сбор информации об этом взаимодействии и возможное опубликование в открытом доступе, для дальнейшего использования также приводит к «открытым данным». Открытые данные, являются также основой «открытого правительства» («*Open Government*», концепция государственного управления, предусматривающего гражданский контроль за государственным регулированием). Здесь Россия в числе лидеров по открытости данных о госконтрактах, тендерах, информации о госучреждениях.

Однако, несмотря на огромные преимущества использования всех этих технологий, вызовы для всего современного мира заставили многие страны создать различные документы, регулирующие безопасное взаимодействие в рамках информационной среды. В частности, и российское руководство страны выработало «Доктрину информационной безопасности Российской Федерации», утвержденную Президентом России 5 декабря 2016 года [2]. В ней, помимо всего прочего, можно выделить представленные ниже положения.

«Национальными интересами в информационной сфере являются:

– обеспечение устойчивого и бесперебойного функционирования информационной инфраструктуры, в первую очередь критической ... и единой сети электросвязи Российской Федерации...

– развитие в Российской Федерации отрасли информационных технологий и электронной промышленности, а также совершенствование деятельности ... по разработке, производству и эксплуатации средств обеспечения информационной безопасности, оказанию услуг в области обеспечения информационной безопасности;

– содействие формированию системы международной информационной безопасности, направленной на противодействие угрозам использования информационных технологий в целях нарушения стратегической стабильности...».

Важно отметить, что предыдущая доктрина была утверждена в 2000 г. и признана в текущем документе «утратившей силу».

Известно, что анализ нескольких несекретных источников в результате может оказаться секретной информацией, например, информация о ключевых энергетических объектах городов по отдельности может казаться совершенно безобидной, но в масштабах страны приобретает стратегический характер и может использоваться, как и в мирных, так и в военных целях. Особенно опасными могут оказаться и сведения о транспорте, которые так прочно вошли в нашу жизнь в виде приложений-справочников и электронных карт. Потенциальная угроза исходит от сведения о загруженности линий метрополитена и количестве человек в часы пик, которые, к сожалению, могут быть использованы террористическими организациями.

Сегодня нередки случаи кражи персональных данных из различных госучреждений. Волна подобных преступлений захлестнула все страны и динамика во многом пока не утешительна. Это происходит ввиду ценности на «черном рынке» персональной и медицинской информации из учреждений охраны правопорядка или здравоохранения [3]. Согласно отчетам компании «Cisco», занимающей информационными технологиями вообще и безопасностью в частности, масштабы крупнейших краж персональных данных пользователей достигают цифры в 80 млн [4].

Вообще говоря, некоторые «открытые данные» являются, по своей сути, агрегированными персональными данными граждан. Естественно, правительством, выкладывающим в открытый доступ такие массивы, проводятся меры по анонимизации. Тем не менее, аналитики компании Neustar Research в 2014 г. на основе выложенных открытых данных обо всех передвижениях такси Нью-Йорка, опубликованных властями города в 2013 г., отследили передвижение знаменитостей и нанесли посещаемые ими заведения на карту [5]. Таким образом, специалистам удалось получить персональные данные из «открытых».

В связи с потенциальной угрозой использования «открытых данных» злоумышленниками в противозаконных целях, организация или государственное учреждение должно с должным вниманием относится ко всем этапам работы с открытыми данными – от агрегирования первичной информации в массивы данных до хранения и контроля за использованием наборов открытых данных посетителями сайтов.

Если проблемы утечки данных внутри сети решаются путем установления правил безопасности при работе в локальной сети организации, разграничением доступа пользователей/сотрудников, а также использованием системы контроля действий пользователя, то использование открытых данных за пределами ресурса, где они размещены никак не отслеживается и не контролируется. Поэтому возникает необходимость мониторинга трафика использования «Open Data».

Инструменты и методы «Big Data» могут быть применены не только для существенного ускорения сбора и обработки самих открытых данных, но и для решения проблем информационной безопасности, в частности – наблюдения и анализа использования в максимально автоматизированном режиме.

Одной из использующихся в сфере информационной безопасности технологий является «SIEM» (*Security information and event management*). Программные продукты этой категории позволяют выявлять следующие события:

– сетевые атаки во внутреннем и внешнем периметрах;

– вирусные эпидемии или отдельные вирусные заражения, бэкдоры и трояны;

– попытки несанкционированного доступа к конфиденциальной информации;

– фрод и мошенничество;

– ошибки и сбои в работе информационных систем;

– ошибки конфигураций в средствах защиты и информационных системах.

В процессе работы «SIEM» выполняются следующие задачи:

– агрегирование информации, поступающей от различных источников (устройств, датчиков, баз данных и т. д.);

– интерпретация множества несвязных событий внутри сети в кластеры значимой информации, удобной для последующего анализа и поиска уязвимостей;

– анализ кластеров и автоматизированная система вывода оповещений об угрозах безопасности, нарушении работы узлов и т. д.;

– визуализация полученной в результате обработки информации для дальнейшей экспертной оценки.

Средства «SIEM» в большей степени подходят организациям с крупной разветвленной структурой, обладающим временным ресурсом для накопления статистики, широкими финансовыми возможностями и высокими требованиями к защите от различных утечек данных [6]. Таким образом, необходимостью применения и возможностью реализации обладают либо крупные компании, либо государственные органы, использующие в своей работе информацию, представляющую ценность для киберпреступников.

Также использование этой технологии никак не ограничивает свободный доступ к открытым данным со стороны пользователей сети интернет, но позволяет повысить вероятность обнаружения утечки информации, к примеру персональных данных граждан.

Подводя итог всему вышесказанному, необходимо уточнить, что полный запрет различных технологий, связанных с открытыми данными, как и противоположная точка зрения – о полном свободном доступе к абсолютно любой информации, которой обладают государственные учреждения, по меньшей мере недальновидны. Необходимо развивать эту концепцию, опираясь на зарубежный опыт, а также ставить целью создание конкурентоспособного продукта на внешнем рынке. Однако, не стоит пренебрегать угрозами, начиная от коммерческих и правовых, заканчивая внешнеполитическими и военными. Соблюдая требования инфобезпасности и разумно проводя экономическую политику, государство напрямую и опосредованно может добиться развития данной части информационного сектора рынка, в полном соответствии с принятой доктриной информационной безопасности.

Список используемых источников

1. Открытые данные в России [Электронный ресурс] URL: https://opengovdata.ru/definition/ (дата обращения 27.03.2017).
2. Указ Президента Российской Федерации от 05.12.2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» [Электронный ресурс]. URL: http://static.kremlin.ru/media/acts/files/0001201612060002.pdf (дата обращения 27.03.2017).
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. в 3-х т. 2016. Т. 1. С. 227–231.
4. Годовой отчет Cisco по информационной безопасности за 2016 год [Электронный ресурс]. URL: http://www.cisco.com/c/dam/m/ru_ru/internet-of-everything-ioe/iac/assets/pdfs/security/cisco_2016_asr_011116_ru.pdf (дата обращения 27.03.2017).
5. Riding with the Stars: Passenger Privacy in the NYC Taxicab Dataset [Электронный ресурс]. URL: https://research.neustar.biz/2014/09/15/riding-with-the-stars-passenger-privacy-in-the-nyc-taxicab-dataset/ (дата обращения 27.03.2017).
6. A Practical Application of SIM/SEM/SIEM Automating Threat Identification [Электронный ресурс]. URL: http://www.sans.org/reading-room/whitepapers/logging/practical-application-sim-sem-siem-automating-threat-identification-1781 (дата обращения 27.03.2017).

УДК 004.056.53

РАССЛЕДОВАНИЕ ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ЭКСПЛУАТАЦИИ УЯЗВИМОСТИ НУЛЕВОГО ДНЯ

Л. А. Виткова, М. Н. Дудникова, М. В. Левин

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

В данной статье авторы проводят расследование инцидентов информационной безопасности при эксплуатации уязвимости нулевого дня. Проводится исследование и анализ таргетированной атаки с помощью вируса-шифровальщика. Приведены сигнатуры вируса, в антивирусном программном обеспечении, которое уже обнаружило данный вредоносный файл, приведен код исполняющегося файла, описан процесс работы вируса no_more_ransom, последствия заражения, способы предотвращения заражения компьютера, варианты расшифровки данных и современные методы защиты от атак zer0-day.

уязвимость 0-day, вирус-шифровальщик, no_more_ransom. информационная безопасность.

Введение

Человечеству с незапамятных времен известно шифрование. А шантаж, наверное, известен со времен еще более древних. Пару десятков лет назад эти методы объединили и обратили против большого количества людей. Случилось это в 1989 г., когда биолог, доктор Джозеф Л. Попп, создал первого трояна-вымогателя.

Доктор Попп написал вредоносный код и распространил его на конференции, посвященной СПИДу, которую проводила Всемирная организация здравоохранения. Зловред распространялся на дискетах с наклейкой «Вводная информация о СПИДе» с отдельно напечатанным предупреждением о том, что программное обеспечение на носителях может повредить компьютеры.

Но кто читает инструкции? Около 20 тысяч дискет, распространенных Поппом, люди вставили в свои компьютеры. Их системы оказались заблокированы, а на экране появилось требование выкупа – около $189, которые нужно было отправить обычной почтой в Панаму. Звучит знакомо, не правда ли?

По статистике Лаборатории Касперского в 2016 г. произошел всплеск вредоносных программ-вымогателей [1]:

– возникло больше 60 новых семейств;
– количество модификаций вымогателей выросло в 11 раз;
– в 3 раза увеличилось количество атак на компании;
– в 2 раза увеличилось число атак на пользователей;
– 1/5 людей, заплативших выкуп так и не получили расшифрованные файлы.

В 2016 г. в мире началось организованное противостояние вымогателям. В июле был запущен проект No More Ransom, объединивший усилия Национальной полиции Нидерландов, Европола, компаний Intel Security и «Лаборатория Касперского»; в октябре к проекту присоединились ещё 13 организаций. В рамках проекта в открытом доступе были размещены бесплатные утилиты для расшифровки данных.

Содержание

В конце 2016 г. в России вспыхнула активность шифровальщика по иронии названным «no_more_ransom» [2]. Предполагается, что его создатели связаны с такими вирусами как better_call_saul и da_vinci_code.

Интересно, что в подавляющем большинстве случаев сообщения, посредством которых распространялся вирус были «из налоговой». Часть писем сообщают о необходимости оплаты счета, другие предлагают посмот-

реть свежий прайс-лист и т. д. В сообщении был прикреплённый архив, который в свою очередь содержал файл, название и иконка которого на первый взгляд не вызывали подозрений, например, в отчет_xls.js.

Именно при попытке открытия этого файла выполняется javascript-код и происходила активизация вируса. No_more_ransom вирус зашифровывает файлы разнообразных форматов на компьютере жертвы. Со стороны жертвы, всё выглядело так, что после окончания процесса шифрования, все знакомые файлы исчезали, а в папках, где хранились документы, появлялись новые файлы со странными именами и расширением .no_more_ransom. Кроме этого на рабочем столе появлялась устрашающая заставка с сообщением как на слайде (рис. 1).

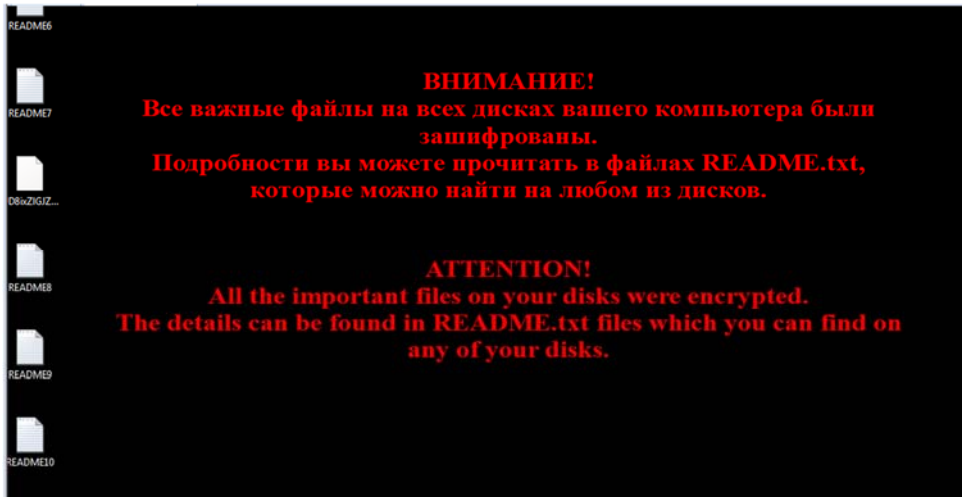


Рис. 1. Рабочий стол зараженного компьютера

Анализ

Сценарий javascript кода очень запутан. При первом запуске No_More_Ransom собирает различную информацию о системе и на её основе генерирует для себя уникальное имя, представляющее собой бессмысленный набор некоторого количества латинских букв, но видно, что он использует объект ActiveXObject, который является расширением Microsoft и поддерживается только в Internet Explorer. Вирус по специальному алгоритму генерирует доменные имена и пытается присоединиться к ним. В случае неудачного соединения попытки подключиться продолжаются. Попытки подключения к серверу продолжаются до тех пор, пока не будет сгенерировано актуальное имя на данный момент. В ходе выполнения сценария JS-код пытается загрузить тело вредоносного файла из других источников: http://clidis.pt/helpconfig.exe либо из 40.77.226.250 IP-адрес (*Microsoft Corporation in Dublin, Dublin, Ireland*) или из 34.172.18.212 IP-адреса *(rev.vodafone.pt*). Затем файл helpconfig.exe загружается на зараженный компьютер. Файл загружется по следующему пути: % AppData% \ Local \

Microsoft \ Windows \ TemporaryInternet Files \ Content.IE5 \ 643WD09Y \ helpconfig.exe. На самом деле, helpconfig.exe используется в качестве установщика.

После выполнения этих шагов вредоносная программа будет пытаться подключиться к некоторым C&C серверам (часть из которых является TOR узлами): 40.77.229.250, 40.77.229.125, 194.109.206.212, 195.154.92.155, 131.215.172.214, 21.219.28.99.

В случае успешного подключения на сервере генерируется пара ключей для RSA шифрования. Публичный ключ передаётся на компьютер жертвы и хранится в реестре, закрытый ключ, предназначенный для расшифровки, остается на сервере, вместе со сгенерированным идентификатором компьютера жертвы.

Вирус вносит изменения в реестр. Для сохранения содержимого ключей No_More_Ransom постоянно мониторит их состояние и восстанавливает в случае необходимости.

На рис. 2 показан добавленный ключ HKCU\Software\System32\ Configuration.

Имя	Тип	Значение
(По умолчанию)	REG_SZ	(значение не присвоено)
shst	REG_SZ	4
xcnt	REG_SZ	708
xi	REG_SZ	F9E72773CA361D53AA60
xmode	REG_SZ	0
xpk	REG_SZ	-----BEGIN PUBLIC KEY-----MIIBojANBgkqhkiG9w0BAQEFAAOCAY8AMIIBigKCAYEAt6G9/Wujf9zKz7sbo6oOyWwdU...
xstate	REG_SZ	5
xsys	REG_SZ	1
xVersion	REG_SZ	4.0.0.1
xwp	REG_SZ	

Рис. 2. Параметры и значений ключа реестра HKCU\Software\System32\ Configuration

На рис. 3 показано, что для обеспечения своего запуска одновременно с запуском системы троян создает в реестре в ветках автозапуска ключ HKCU \ Software \ Microsoft \ Windows \ CurrentVersion \ Run \ Client Server Runtime Subsystem.

(По умолчанию)	REG_SZ	(значение не присвоено)
Client Server Runtime Subsystem	REG_SZ	"C:\ProgramData\Windows\csrss.exe"
Google Update	REG_SZ	C:\Users\bobby\AppData\Local\Google\Update\1....

Рис. 3. Параметры и значений ключа реестра
HKCU \ Software \ Microsoft \ Windows \ CurrentVersion \ Run \

Этим вирус обеспечивал себе возможность продолжить шифрование. если по каким-либо причинам компьютер был выключен. Он будет создавать копию себя под именем процесса CSRSS (процесс Windows, устранение которого приведет к синему экрану смерти). На рис.4 показано дерево процессов вируса.

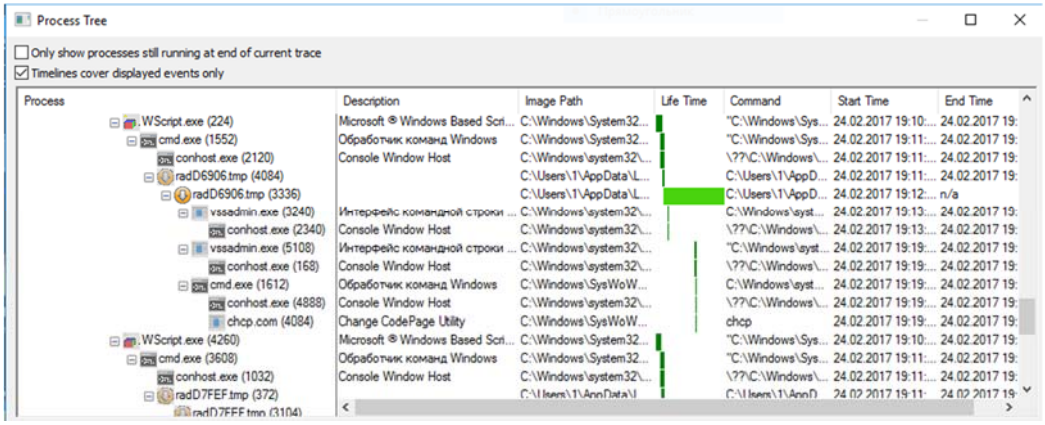


Рис. 4. Дерево процессов вируса .no_more_ransom

На этом этапе начинается процесс шифрования. Вирус шифрует огромное количество разных видов файлов, форматы приведены на слайде. Судя по названиям зашифрованных файлов, в хвосте указан зашифрованный сессионный ключ. При старте шифрования генерируется случайный ключ для AES, им шифруется всё, сам сгенерированный ключ шифруется публичным RSA-3072. В случае неуспешного подключения выбирается один из зашитых в троянец RSA-ключей.

Вирус не шифрует файлы в системных папках, видимо автору важно, чтобы ОС функционировала, для дальнейшего вымогательства. После шифрования файлов вирус создает на всех дисках и рабочем столе идентичные текстовые документы README.txt, README1.txt, README2.txt…

В файле Readme.txt, жертва получает указание связаться с lukyan.sazonov26@gmail.com, чтобы получить дальнейшие инструкции. Этот адрес электронной почты ранее был связан с вымогателями better_call_saul и da_vinci_code.

Если ответ не получен от этого адреса в течение 48 часов, жертва должна заполнить контактную форму, расположенную в сети TOR.

Интересно, что владелец знаменитого среди троянцев адреса искренне удивлялся полученным сообщениям, когда неделю назад требовал деньги у работницы Ставрополя.

Вывод

На сегодняшний день нет доступного декриптора .no_more_ransom файлов. Так как используется очень сильный алгоритм шифрования RSA-3072 без личного ключа, расшифровать файлы практически невозможно. Использовать метод подбора ключа нецелесообразно, из-за большой длины ключа, на это уйдет много лет. К сожалению, только оплата авторам вируса всей запрошенной суммы – единственный способ попытаться вернуть за-

шифрованные файлы. Поэтому настоятельно рекомендуется делать резервные копии важных файлов, или целой ОС. И разумеется, хватит открывать прикрепленные файлы/ссылки от непроверенных отправителей.

В некоторых случаях восстановить файлы можно с помощью утилит, таких как ShadowExplorer, позволяющих восстанавливать теневые копии файлов, которые создаются автоматически ОС.

Для предотвращения заражения компьютера вирусами-вымогателями используйте встроенные средства систем защиты от проникновения и активизации, которые есть у большинства антивирусных программ. Например, используйте CryptoPrevent. Kaspersky Virus Removal Tool (KVRT) и Malwarebytes Anti-malware (MBAM) могут обнаруживать разные типы активных вирусов-шифровальщиков и легко удалят их с компьютера.

Список используемых источников

1. Трояны-вымогатели: чума 2016 года [Электронный ресурс]. URL: https://blog.kaspersky.ru/fighting-ransomware/13650/ (дата обращения 10.02.2017).

2. Virustotal онлайн-сканер вирусов, вредоносных файлов [Электронный ресурс]. URL: https://www.virustotal.com/en/ (дата обращения 10.02.2017).

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

УДК 004.056

ИССЛЕДОВАНИЕ И РАЗРАБОТКА МЕТОДИК ОЦЕНКИ РИСКОВ ОБЛАЧНЫХ РЕСУРСОВ

Л. А. Виткова, А. И. Иванов, И. Ю. Сергеева

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

Развитие Интернета привело к большой популярности облачных технологий. Внедрение их в производственные процессы несёт в себе как плюсы, так и минусы. Для того что бы принять решение – нужно проанализировать возможные риски, которые могут возникать вследствие перехода к облаку. В данной статье автором рассматриваются наиболее актуальные методики оценки риска применительно к облачным вычислениям и делаются выводы по их актуальности для облачных сервисов.

облачные технологии, оценка рисков, информационные технологии, риски.

В последнее время популярность «облачных» технологий неизменно возрастает, это связано со многими факторами. Во-первых, это повсеместная доступность – Вы можете получить доступ к «облаку» из любого места,

где есть интернет. Во-вторых, немаловажную роль играет тот фактор, что это выгодно. Маленьким и средним компаниям не нужно тратиться на обустройство специальной инфраструктуры, они платят за использованные мощностей. В настоящее время вопрос безопасности данных стоит очень остро, и, поэтому, для перевода своих мощностей на облачные вычисления, сперва необходимо оценить все возможные риски и после этого взвесив все доводы «за» и «против» принять взвешенное решение. Недостаток масштабных исследований в вопросе исследования рисков при переводе вычислительных процессов на мощности «облака» может вызывать затруднения у руководителей предприятий при принятии решения о переходе к «облаку» [1].

Если в системе обрабатывается конфиденциальная информация, то, в качестве облачной модели лучше выбрать «частное облако». Данная модель представляет собой инфраструктуру, которая базируется в переделах предприятия или в дата-центре провайдера, сертифицированном на соответствие нормам 152-ФЗ. Стоит отметить, что не все провайдеры облачных сред обладают правом обрабатывать КИ. В отличие от публичных облачных сервисов, частное облако способствует повышению уровня информационной безопасности за счет локализации всех данных в защищенном дата-центре, а не на рабочих станциях пользователей [2]. Для оценки рисков облачных сред можно использовать методики, применяемые для анализа рисков в области информационной безопасности. Методики можно разделить на несколько групп, в частности можно выделить такие группы, как: качественные методики, количественные и методики смешанных оценок

Методика RiskWatch была разработана Национальным Институтом Стандартов и технологий США, а также при поддержке министерства обороны Канады. Данный метод приобрёл широкую известность среди многих организаций во всём мире. RiskWatch представляет собой набор программных продуктов, предназначенных для управления различными рисками и поддержки стандартов.

Условно всю архитектуру RiskWatch можно представить в виде четырёх объектов: база знаний, программный интерфейс, модуль оценки рисков и интерфейсные модули. Всю методику оценки рисков в данной модели так же можно разделить на несколько этапов. На первом этапе определяется предмет исследования, в программе уже имеются шаблоны, позволяющие сразу обозначить тип защищаемой системы (государственная, военная, коммерческая информационная система и т. п.). Вводятся категории активов, рассматриваемые угрозы и применяемые контрмеры.

На втором этапе вводятся данные, описывающие характеристики системы. Среди них можно отметить такие данные как частота возникнове-

ния угроз, ценность активов, задаются вопросы, направленные на определение соотношения стоимости активов и применяемых мер по обеспечению безопасности.

Третий этап представляет собой количественную оценку рисков. В этом этапе задействуются данные полученные в предыдущих двух – проводятся связи между ресурсами, потерями, уязвимостями и угрозами. Средства RiskWatch позволяют выбрать оптимальные контрмеры.

На четвёртом этапе формируются отчёты, позволяющие оценить возможные риски, а также эффективность выбранных средств защиты.

CRAMM предназначена для анализа рисков в компаниях любого масштаба. Она сочетает в себе количественные и качественные методы анализа. Благодаря специально разработанным профилям подходит как для коммерческих, так и для правительственных организаций. Профиль, предназначенный для правительственных ИС, позволяет проводить аудит на соответствие требованиям американскому стандарту ITSEC. Риск-модель предусматривает три этапа по анализу рисков.

На первом этапе анализируются ресурсы системы. Рассматриваются все субъекты и объекты, физические ресурсы оцениваются с точки зрения их стоимости при разрушении. Ценность данных и программных ресурсов определяется на основании базовых принципов ИБ – конфиденциальности, целостности и доступности. Рассматриваются ситуации разрушения, модификации информации, её разглашения третьим лицам, отказ в доступе к информации объектам информационной системы.

Ущерб предлагается оценить по таким параметрам, как: ущерб для здоровья персонала, ущерб репутации, финансовые потери и потери связанные с невозможностью выполнения обязательств, нарушение законодательства и разглашение конфиденциальной информации. Возможный ущерб данным и программным ресурсам оценивается по шкале от 1 до 10. Низкая стоимость ущерба требует базового уровня защиты.

Второй этап предусматривает построение модели информационной системы с точки зрения информационной безопасности. Составляется матрица риска с выявленными угрозами и уязвимостями.

На третьем этапе осуществляется поиск мер противодействия угрозам. CRAMM предоставляет большое количество вариантов обеспечения безопасности, решение о выборе которых принимает организация-заказчик.

К недостаткам данного метода можно отнести большую трудоёмкость процесса, анализ рисков может достигать нескольких месяцев, высокую стоимость лицензии, а также не гибкую базу знаний и необходимость специализированной подготовки аудитора.

Методика Octave была изобретена институтом Software Engineering Institute. Она предназначена для пользования сотрудниками внутри органи-

зации, без привлечения сотрудников из вне. Предполагает создание специальной группы сотрудников, выбранных из штата для проведения анализа возможных рисков, их последствий и принятия необходимых контрмер. Работа по данной методике проходит в три этапа.

Первый этап предполагает всестороннюю проработку угроз. Описываются все возможные угрозы и активы. В ходе второго этапа описывается вся инфраструктура актива, анализируется его окружение, которое может позволить получить доступ к нему. По результатам стадии готовятся отчёты с обнаруженными угрозами и возможным ущербом активам. На третьем этапе разрабатываются меры предотвращения угроз. Разрабатываются стратегии направленные на обеспечение безопасности. Оценивается ожидаемый ущерб, без его вероятности. Его оценка градируется от низкой до высокой. Разрабатываются долговременные, среднесрочные и планы на ближайшее время по снижению рисков.

Octave предлагает каталоги средств, в которых описаны меры борьбы с рисками. При помощи этой методики можно произвести оценку информационной безопасности информационной системы, к которой имеют полный доступ сотрудники организации, поскольку требуется доступ к оборудованию [3].

В заключение нужно отметить, что представленные методики могут быть использованы для частных облачных сред, где необходимое оборудование находится в юрисдикции организации и аудиторы имею доступ ко всей необходимой инфраструктуре для оценки её безопасности. Необходимо иметь постоянный доступ к оборудованию, используемому в информационной системе для своевременного внесения корректировок, влияющих на её безопасность. При использовании услуг провайдеров облачных технологий встаёт вопрос о соблюдении ими стандартов безопасности в области хранения конфиденциальной информации [4]. Оценка информационных рисков в частных облачных сетях не отличается от оценки рисков в информационных системах.

Список используемых источников

1. Николас Дж. Карр. Великий переход: что готовит революция облачных технологий: пер. с англ. М. : МИФ, 2013. 272 с. ISBN: 978-5-91657-892-8

2. Риз Д. Облачные вычисления: пер. с англ. СПб. : БХВ-Петербург, 2011. 288 с.

3. Астахов А. М. Искусство управления информационными рисками . М. : ДМК-Пресс, 2010. 312 с.

4. Нечай О. Риски облаков: угрозы и решения [Электронный ресурс] // Компьютерра: Справочно-информационный интернет-портал. 2013. N 3.URL: http://www.computerra.ru/89963/riski-oblachnyih-resheniy-ugrozyi-i-resheniya/

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

УДК 004.056.5

ИССЛЕДОВАНИЕ ТЕХНОЛОГИЙ ПАКЕТНОГО ТРАНСПОРТА В ГИБРИДНОЙ СРЕДЕ SD-WAN

Л. А. Виткова, И. О. Махова, Д. В. Сахаров

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

В настоящее время сети стали стратегически важным активом, что привело к возникновению необходимости перехода на программно-определяемые WAN сети. Современные технологии позволяют решать проблемы администрирования сетей.

В работе авторы рассматривают возможности реализации технологии SD-WAN в гибридных сетях.

SD-WAN, распределенная сеть, трафик, гибридная сеть, производительность.

Динамичное развитие рынка телекоммуникационных услуг вынуждает ИТ-компании искать новые пути решения таких актуальных проблем как: снижение высоких затрат на поддержку оборудования и пути уменьшения издержек на обслуживание сетевой инфраструктуры. Теперь перед ними ставится задача построения такой ИТ-инфраструктуры, которая смогла бы удовлетворять все потребности клиентов. И если в области вычислительных платформ все же удалось добиться определенных результатов, то область передачи данных по сети до сих пор остается слабым звеном, замедляющим технологическое развитие. Высокая вероятность ошибок, отсутствие гибкости в архитектуре и необходимость конфигурирования напрямую каждого устройства приводят к тому, что обновление на эксплуатацию новых конфигураций может занимать достаточно продолжительное время. Технологическим решением данных проблем стала технология программно-определяемой сети, именуемая Software-Defined Networking (далее-SDN).

Основная концепция SDN заключается в сепаратизации функций управления сетью (*Control Plane*) и коммутации пакетов (*Data Plane*) (рис. 1). Осуществление конфигурации сети выполняется на специальном обособленном устройстве, именуемый контроллером сети. Применение данной концепции позволяет потенциальному клиенту самостоятельно осуществлять контроль над всей сетью и централизованно управлять сетью и политиками маршрутизации данных.

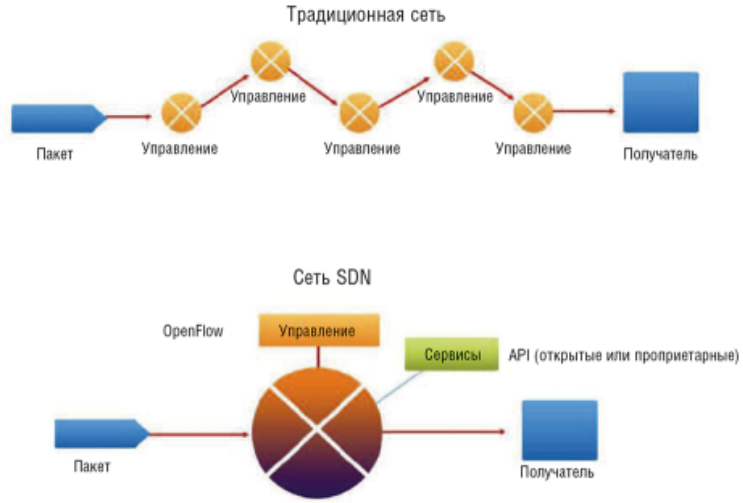


Рис. 1. Основная концепция технологии SDN

Наиболее востребованной областью применения SDN являются корпоративные WAN-сети [1]. Такой спрос обусловлен сложностью обслуживания распределенных сетей, неэффективное использование дорогостоящих частных каналов связи, трудность масштабирования и недостаточный уровень автоматизации процессов. Данная модель предусматривает управление поведением трафика и статическую конфигурацию туннелей. Использование публичных облачных сервисов еще больше усложняет задачу, ввиду того, что данная часть сетевой инфраструктуры находится вне зоны корпоративной сети [2]. Непрерывный рост запросов пользователей также приводит к проблеме увеличения требований к пропускной способности каналов, так как использование интернет-подключения не может обеспечить необходимого качества услуг.

Для решения вышеизложенных проблем призвана система, которая построена с целью реализации концепции Software Defined WAN (далее SD-WAN). Данная технология ставит перед собой задачу предоставления определенно нового подхода к управлению WAN-сетями, выраженная в упрощении подключения новых филиалов и централизовать управление филиальной сетью.

Если рассматривать сеть SD-WAN с технологической точки зрения, то ее концепция довольно проста: конченые устройства на одном конце канала сети WAN направляют трафик к другим устройствам через магистральную сеть, которые управляются централизованно, что позволяет сетевым администраторам осуществлять конфигурацию и контроль трафика, опираясь на централизованные политики и правила безопасности. Используя мониторинг и анализ производительности WAN-сетей, система принимает решения о направлении трафика через определенное подключение, тем самым

осуществляя оптимизацию использования каналов связи. При этом необходимо учитывать одно важное требование к платформе, а именно возможность гарантировать качество сервиса при использовании публичных каналов связи. Анализируя основные преимущества сети SD-WAN, можно выделить главное – возможность управления трафика на уровне приложений. Данная особенность позволяет администраторам сети осуществлять идентификацию и оперативное устранение различных проблем качества предоставления услуг.

SD-WAN применяет облачные технологии для упрощения доставки услуг в удаленные сегменты предприятия. Концепция SD-WAN предоставляет возможность организовывать качественное, быстрое и безопасное подключение к сети интернет, тем самым обеспечивая такие возможности как: высокая пропускная способность, повсеместная и материальная доступность.

Возникновение новых более усовершенствованных технологий означает появление новых регуляторов сетевого трафика в распределенных сетях. Пользователи нуждаются в повышенной пропускной способности, особенно для мультимедийного трафика, и более быстром доступе к облачным сервисам или другим удаленным хранилищам.

Поэтому следует выделить преимущества:

1. Гибкость служб WAN. Осуществление быстрого развертывания различных служб глобальных сетей для удаленных офисов без необходимости организации локальной IT-поддержки. Также присутствует возможность легкого регулирования пропускной способности, в зависимости от потребностей клиентов.

2. Экономия пропускной способности. При сравнении с сетью MPLS, SD-WAN предоставляет более быстрое развертывание сети, легкодоступное подключение к сети интернет и, что не маловажно, меньшая стоимость обслуживания. Software-Defined Networking позволяет обеспечивать такие показатели безопасности и надежности, которые по материальным затратам характеры для служб глобальной сети WAN.

3. Оптимизация с облачной архитектурой. Технология SD-WAN гарантирует безопасность, высокую безопасность и соединение между облаком и офисами, тем самым избавляя от типичных неудобств и ограничений сетей MPLS, что значительно повышает комфортность работы удаленных клиентов при пользовании облачными приложениями или SaaS- сервисами [3].

Оценивая технологию SD-WAN с точки зрения применения и внедрения ее в свою сеть, администраторам сети следует принять во внимание некоторые нижеприведенные факторы. Рассматриваемая технология имеет явное преимущество, так как она является достаточно простой во внедрении в удаленные офисы и эксплуатации, чем исключает необходимость от-

правки ИТ-специалистов в эти офисы. Так как SD-WAN предполагает возможность перехода на гибридные сети, многие корпоративные организации предпочитают разворачивать распределенную сеть MPLS. Так как Software-Defined Networking позволяет внедрять свои решения без внесения изменений в действующую сеть, то со времени можно обеспечить экономически выгодное решение по организации сетевой инфраструктуры.

Также рассматриваемая сеть предлагает такую опцию как автоматическое управление трафиком и назначение ему приоритетов. Некоторые SD-WANs работают при помощи устройств, расположенных на границах каждого локального сегмента сети, остальные организуют сетевую архитектуру с помощью облачных сервисов.

MPLS представляет собой технологию, которая осуществляет управление прямыми связями между сегментами сети. В абстрактном смысле, это довольно специфический способ указать пакету его путь следования по всей сети. Специальная метка служит указателем маршрута, а также для обозначения резервного пути, в случае необходимости. Метка технологии MPLS может также назначать приоритизацию пакетам, тем самым улучшая качество обслуживания для такого важного типа трафика как VoIP-телефония.

Рассматривая случай интегрирования SD-WAN и MPLS (рис. 2), необходимо учитывать, что рассматриваемые технологии не противоречат друг другу. Конфликт может возникнуть только в сочетании SD-WAN и «чистого» MPLS. При помощи только MPLS, весь трафик идет только через специально указанный путь маршрутизации, а SD-WAN может смешивать различные технологии доставки пакетов, поэтому MPLS не несет ответственность за весь трафик.

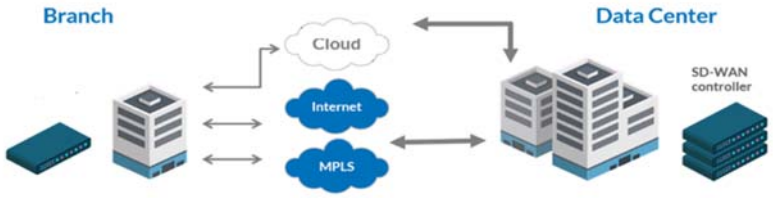


Рис. 2. Представление интегрирования технологий SD-WAN и MPLS

Как уже говорилось выше, SD-WAN сепаратизирует контроль управления трафика и его транспорт, опираясь на некоторые специализированные механизмы. Из этого можно выделить ее преимущество, которое состоит в том, что SD-WAN может смешивать различные подходы. Технология MPLS обеспечивает повышенную скорость прохождения пакетов вдоль всего пути, где важна минимальная задержка [4]. Однако если данный аспект использовать для трафика вдоль всего пути, то возникает ситуация повышенной нагрузки на маршрутизаторы, что приводит к снижению скорости передачи данных. Но возможность избежать такие «узкие» места есть,

но она может потребовать дорогостоящей модернизации. Поэтому, для продуктивной организации структуры сети, можно использовать MPLS только для высокоприоритетного трафика, а остальную его часть можно использовать в качестве стандартного Internet-трафика.

Не стоит считать, что MPLS является устаревшей технологией, наоборот, SD-WAN дополняет ее и делает более полезной. Данное технологическое сочетание можно использовать на определенных путях, где он действительно необходим, что позволит обеспечить дополнительную гибкость. Данный аспект может помочь сократить материальные расходы, так как MPLS нуждается в высокой производительности, чтобы поддерживать продуктивную обработку приоритетного трафика. Также стоит отметить, что обеспечение пропускной способности сети MPLS является достаточно затратным. Поэтому целесообразно использовать технологию SD-WAN, которая позволит обеспечить запасной вариант при возникновении «падения» пути. Несмотря на то, что трафик в таком случае будет идти медленнее, тем не менее соединение не будет прервано.

Переход от «чистого» MPLS к технологии SD-WAN требует более тщательного анализа безопасности, но необходимо учитывать, что SD-WAN часто рассматривается как дополнение к безопасности, а не часть его решения. Весь трафик, проходящий через сеть интернет, должен быть зашифрован, так как даже банальное соединение может выявить больше информации, чем следует. Поэтому шифрование должно быть частью сетевой архитектуры, с end-to-end туннельным шифрованием. Из этого следует, что технология, которая именуется SD-WAN, существенно отличается по функциональности безопасности, которую может предложить [5].

Когда люди говорят, что MPLS уходит в прошлое, они имеют в виду, что спрос падает как на полноценное технологическое WAN-решение. Интеграция технологий MPLS и SD-WAN все еще используется и будет развиваться, а также иметь свои перспективы в дальнейшем.

Список используемых источников

1. 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-х т. 2015. Т. 1. С. 350–354.

2. Олифер В. Г. Компьютерные сети. Принципы, технологии, протоколы. 4-ое изд. СПб. : Питер, 2010. 210 с.

3. RFC 2702 – Requirements for Traffic Engineering Over MPLS, 2005. 15 p.

4. Олвейн В. Структура и реализация современной технологии MPLS: пер. с англ. М. : Вильямс, 2004. 474 с. ISBN 5-8459-0633-4.

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.

УДК004.056.5

УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ РАСПРЕДЕЛЕННЫХ СИСТЕМ ХРАНЕНИЯ И ОБРАБОТКИ ДЕНЕЖНЫХ СРЕДСТВ

Л. А. Виткова, А. Н. Петрова, Д. В. Сахаров

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

В современном мире онлайн-банкинг, электронные деньги, кошельки и прочие нововведения создают иллюзию уверенности в том, что заработанные деньги надежно спрятаны от злоумышленников. Однако эволюция в банковской сфере дала толчок для развития способов незаконной наживы, и других угроз финансовых махинаций, поэтому актуальность данной темы растет изо дня в день. Авторы исследуют понятия распределенных систем хранения данных и обработки денежных средств. Описывают понятия, виды электронного представления денежных средств и рассматривают существующие наиболее типичные уязвимости и угрозы информационной безопасности.

системы хранения данных, распределенные системы, электронные денежные средства, большие данные.

По оценкам международной консалтинговой компании J’son & Partners Consulting, в 2012 г. оборот рынка дистанционных финансовых сервисов увеличился на 48 % по сравнению с аналогичным показателем 2011 г., составив 896 млрд рублей. С 2012 по 2017 гг. среднегодовой темп роста (CAGR) составил 24 %, а к концу 2017 г. рынок превысил 2,6 трлн рублей. За это время рынок ЭПС (электронные платежные системы) рос и увеличивал свою долю относительно других способов оплаты. Ключевым драйвером развития ЭПС стали дистанционные финансовые сервисы, которые увеличили свою долю в ЭПС с 49 % в 2012 г. до 70 % в 2017 г.

Немобильные банковские сервисы (интернет-банкинг), в структуре оборота рынка дистанционных финансовых сервисов, на конец 2012 г. составили 66 %, при этом доля мобильных сервисов составила 3 %. В 2017 г. произошли небольшие изменения в структуре рынка – доля банковских немобильных сервисов увеличилась до 70 % за счет уменьшения доли небанковских сервисов, а доля мобильных сервисов выросла до 4 % [1]. Данная статистика подтверждает, что на сегодняшний день проблемы безопасности дистанционных финансовых систем продолжают оставаться актуальными (рис.).

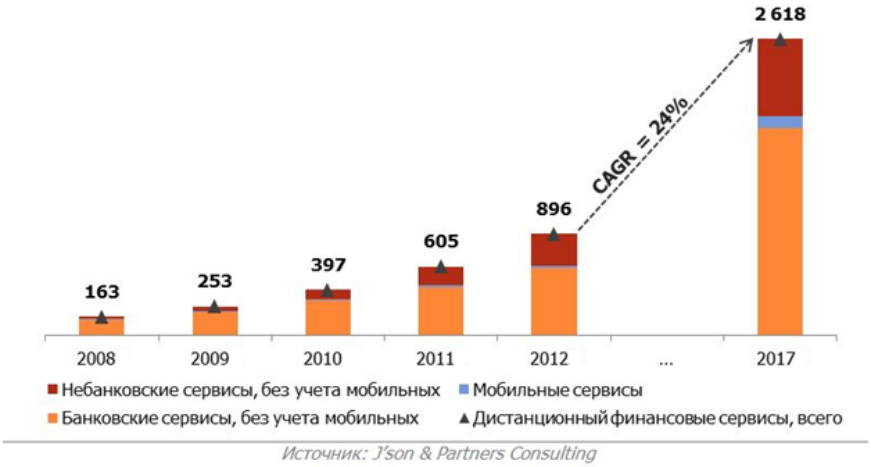


Рисунок. Оборот рынка дистанционных финансовых сервисов, млрд рублей, 2008–2017

Чтобы лучше вникнуть в суть темы, следует вначале разобрать основные понятия. Управление информационной безопасностью – это циклический процесс, включающий в себя несколько этапов и мер:

– сбор и анализ данных о состоянии информационной безопасности в организации и оценка информационных рисков;

– планирование мер по обработке рисков;

– реализация и внедрение соответствующих механизмов контроля, оперативная работа по осуществлению защитных мероприятий;

– мониторинг работы механизмов контроля, а также оценка их эффективности и соответствующие корректирующие воздействия.

Распределенная система – система, для которой отношения местоположений элементов (или групп элементов) играют существенную роль с точки зрения функционирования системы, а, следовательно, и с точки зрения анализа и синтеза системы. Типичной распределённой системой является Интернет.

Система Хранения Данных – это комплексное программно-аппаратное решение по организации надёжного хранения информационных ресурсов и предоставления гарантированного доступа к ним.

Система обработки данных – это комплекс взаимосвязанных методов и средств получения и обработки данных, необходимых для организации управления объектами.

Далее следует разобрать виды представления электронных денег. Их принято классифицировать по форме денежных знаков: фиатные и нефиатные.

Фиатные электронные деньги – электронные деньгиявляющиеся одним из видов денежных единиц платежной системы государства и выраженные в одной из государственных валют. Фиатные электронные деньги могут

быть на базе сетей, туда можно отнести: международную платежную систему PayPal. Также фиатные электронные деньги бывают на базе смарт-карт, к ним относятся: предоплаченные банковские карты Visa Cash, предназначенные для совершения небольших платежей.

Нефиатные электронные деньги представлены широкой сетью различных платежных систем, таких как QIWI, WebMoney, «Яндекс.Деньги», а также «криптовалютными» платежными системами (*Bitcoin*, *Litecoin* и т. п.). Иным примером нефиатных электронных денег является криптовалюта – это подвид электронных валют, эмиссия и учет которых основывается на криптографических методах, а работа самой платежной системы происходит децентрализовано в распределенной компьютерной сети.

Безопасность подключения пользователей к интернет-банкам, которые являются основными системами электронных денег, обеспечивается использованием протоколов SSL/TLS. Существует ряд известных уязвимостей, позволяющих расшифровывать сессии, перехватывать и подменять данные, передаваемые между пользователем и сервером. К примеру, некоторые банки могут по-прежнему использовать небезопасные параметры обмена ключами Diffie-Hellman, а часть банков может быть уязвима к FREAK-атакам. С помощью данной атаки посторонний злоумышленник может перехватывать защищённые соединения и форсировать использование слабой криптографии из «экспортного» набора шифров RSA. Немалая часть веб-ресурсов имеет уязвимость POODLE. С помощью данной уязвимости злоумышленники могут получить доступ к зашифрованной информации, передаваемой между сервером и клиентом. Считается небезопасным использование протоколов SSL2 и SSL3, так как они использует небезопасную криптографическую хеш-функцию MD5 и слабо защищенные шифры. Значительная часть веб-ресурсов может иметь уязвимость Logjam, которая была обнаружена совсем недавно. Как и уязвимость FREAK, Logjam позволяет злоумышленнику форсировать использование клиентским браузером слабой криптографии DH с 512-битными ключами. Также небезопасным считается использование алгоритма хеширования SHA-1, он считается слабым и небезопасным.

Следует помнить о том, что не реализованная или реализована лишь частично настройка безопасности протоколов согласования ключа – Forward Secrecy может повлечь за собой то, что ключи будут скомпрометированы при компрометации закрытого ключа [2].

Далее авторы рассматривают основные типы атак на системы дистанционного банковского обслуживания, зафиксированныецентром мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере главного управления безопасности и защиты информации Банка России FinCERT:

1. Целенаправленные атаки, сопряженные с подменой входных данных для АРМ.

2. Рассылка электронных сообщений, содержащих в себе вредоносное ПО. Данный тип атак является наиболее распространенным.

3. Атаки, направленные на устройства самообслуживания. За отчетный период FinCERT зафиксировал рост количества атак злоумышленников на устройства самообслуживания, в том числе на банкоматы и POS-терминалы.

4. DDoS-атака. Целью данной атаки является отказ в обслуживании легитимных клиентов, вплоть до полной невозможности работы с сервисом. В некоторых случаях, DDoS-атака используется для сокрытия факта целенаправленной атаки;

5. Reversal-атаки. За период с 01 июня 2015 г. по 31 мая 2016 г. FinCERT зафиксировал атаку с использованием поддельных сообщений об отмене платежной операции. Данная атака связана с особенностью обработки сообщений об отмене авторизации переводов денежных средств процессинговым центром. Чаще всего, процессинговые центры не проверяют подлинность такого запроса, в связи с отсутствием контроля ряда полей указанной операции.

Как правило, большинство атак являются мультивекторными, то есть для усложнения атаки используется одновременно несколько способов воздействия на целевую систему, поэтому, защититься от нее становится значительно труднее [3].

Возможным вариантом решения проблем систем дистанционного банковского обслуживания может оказаться использование алгоритмов Big Data.

Big Data – это технологии, которые позволяют быстро обрабатывать большие объемы информации разного формата. Однако представители финансовой отрасли в подавляющем большинстве имеют в виду частный случай Big Data – большие объемы накопленных однородных данных. Как известно, банки и страховые компании хранят все: анкеты, истории транзакций и общения с клиентами, внутреннюю информацию [4].

По оценкам исследовательской компании Gartner, на сегодня 34 % банков по всему миру инвестировали в развитие этих технологий. По данным исследования McKinsey & Company, 25 % Big Data владеет финансовая индустрия, и в среднем на каждую компанию приходится по 3,8 петабайта данных. По результатам опроса того же McKinsey, 76 % банков заявляют, что Big Data позволяют привлекать новых клиентов, лучше взаимодействовать с ними и поддерживать их лояльность.

Современные технологии вполне позволяют обрабатывать накопленные массивы данных. Проблема в том, что они делают это недостаточно

быстро. Именно технологии Big Data способны решить старые долговременные задачи быстро, дав время для маневра и обдуманных действий [5].

Из всего колоссального накопленного количества информации, по различным оценкам участников рынка банковской и страховой автоматизации, в жизни организации используется в наилучшем случае лишь половина информации. Поэтому вопрос монетизации хранения данных так же вечен для банков, как проблема загрязнения окружающей среды – для промышленных мегаполисов. Только технологии Big Data могут обеспечить экономическое обоснование этого хранения, так как без Big Data извлечь ценность из накопленного богатства информации невозможно.

Колоссальные перспективы раскрывает перед банком сочетание Big Data и геоаналитики. Например, клиент заявил о потере карты и одновременно по этой же карте в магазине совершена покупка. Банк оперативно идентифицировал местонахождение телефона клиента и может доказать, что клиент пытается смошенничать (если телефон и карта находятся рядом). Или заблокировать транзакцию, не дожидаясь заявления клиента о потере карты (если телефон и карта находятся на приличном расстоянии друг от друга).

Рассмотренные авторами выше возможные уязвимости и атаки на дистанционные финансовые сервисы подтверждают, что эволюция в банковской сфере дала толчок для развития способов незаконной наживы и других угроз финансовых махинаций. Поэтому в современном мире стоит уже подругому подходить к вопросам управления информационной безопасности таких систем. Авторы обращают внимание на то, что следует рассматривать возможности алгоритмов Big Data для систем финансовой индустрии.

Список используемых источников

1. Российский рынок дистанционных финансовых сервисов: отчет J’son & Partners Consulting. URL: http://json.tv/ict_telecom_analytics_view/rossiyskiy-rynok-distantsionnyh-finansovyh-servisov (дата обращения 03.04.2017).

2. Хант. Т. Безопасность SSL/TLS интернет-банкинга [Электронный ресурс]. URL: https://www.troyhunt.com/2015/05/do-you-really-want-bank-grade-security.html (дата обращения 03.04.2017).

3. Отчет Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Главного управления безопасности и защиты информации Банка России / за период с 01 июня 2015 г. по 31 мая 2016 г.

4. Mayer-Schönberger V., CukierK. Big Data: A Revolution That Will Transform How We Live, Work, and Think, 2014.

5. Карев А. С., Бирих Э. В., Сахаров Д. В, Виткова Л. А. Проблемы информационной безопасности в интернете вещей // Интернет вещей и 5G. 2-я Международная научно-техническая конференция студентов, аспирантов и молодых ученых : сб. науч. ст. 2016. С. 66–70.

УДК 004.056.5

ПРОБЛЕМА ВЫЯВЛЕНИЯ ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОГО ВОЗДЕЙСТВИЯ В ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

Л. А. Виткова[1], И. Ю. Потехин[2], Д. В. Сахаров[1]

[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 (Роскомнадзор) по Северо-Западному федеральному округу

Всё большее количество жителей планеты, стало собираться в социальных сетях и прочих разнообразных проектах, объединяющих людей в сети Интернет. Число таких проектов растёт год от года, а это значит, что проблема выявления информационно-психологического воздействия в информационной инфраструктуре становится все более актуальной для государства.

мониторинг, социальные сети, BigData, SERM, ORM, информационно-психологическое воздействие, информационная война.

Введение

Обновленная Доктрина информационной безопасности Российской Федерации утверждена Указом Президента Российской Федерации от 5 декабря 2016 г. № 646, в ней выделены два основных направления – это информационно-технические аспекты и информационно – психологические аспекты [1].

Если проанализировать отличия между доктриной двухтысячного года и новой, то мы можем увидеть, что в новой Доктрине выражены сильнее: 1) защита духовно-нравственных ценностей; 2) международная информационная безопасность; и 3) террористические и экстремистские аспекты использования информационных технологий.

Информационно-психологическая безопасность, – это, прежде всего, гуманитарный аспект информационной безопасности, связанный в первую очередь с воздействием посредством информационных технологий на психологическое состояние человека в интересах достижения экономического, политического, военного и другого превосходства в сфере личности, общества и государства. В данной статье авторы выделяют три уровня информационно-психологической безопасности: 1) государство; 2) общество и 3) личность.

Исходя из новых требований, перечисленных в Доктрине информационной безопасности, и исходя из национальных интересов государства стоит обратить внимание на то, что сегодня появляются новые требования информационной безопасности.

Авторы считают необходимым обратить внимание на то, что существующие модели угроз решают только вопросы технической составляющей информационной безопасности и включают в себя следующие шаги:

– определение физических и логических границ информационной системы;

– идентификация нарушителей и угроз;

– оценка угроз;

– применение и настройка средств защиты информации.

При этом остаются не решенными проблемы гуманитарной составляющей информационной безопасности:

– нет определения границ информационно-психологического поля объекта;

– нет критериев для нарушителя информационно-психологической безопасности;

– нет типового набора угроз информационно-психологического поля;

– нет метрик нового типа угроз.

Авторам в своей работе выделяют тот факт, что сегодня требуется разрабатывать новые методы, методики в области информационно-психологического противоборства [2].

Анализ

Одним из способов информационно-психологического воздействия на человека, способом манипулирования сознанием является информационная война – это согласованная деятельность по использованию информации как оружия для разрушающего воздействия на противника в различных сферах: экономической, политической, социальной и на поле боя. Информационная война – это война нового типа, которая предполагает, как воздействие на информационные системы и инфраструктуру противника, так и на сознание людей, их поведение и здоровье.

Изучив основные типы источников распространения информации, можно сделать вывод, что сегодня интернет занимает лидирующие позиции по охвату аудитории.

Так, например, в рейтинге ТОП 10 в Европе Россия занимает первое место по числу пользователей сети Интернет, более 103 млн человек пользуется сетями общего доступа (рис. 1) [3].

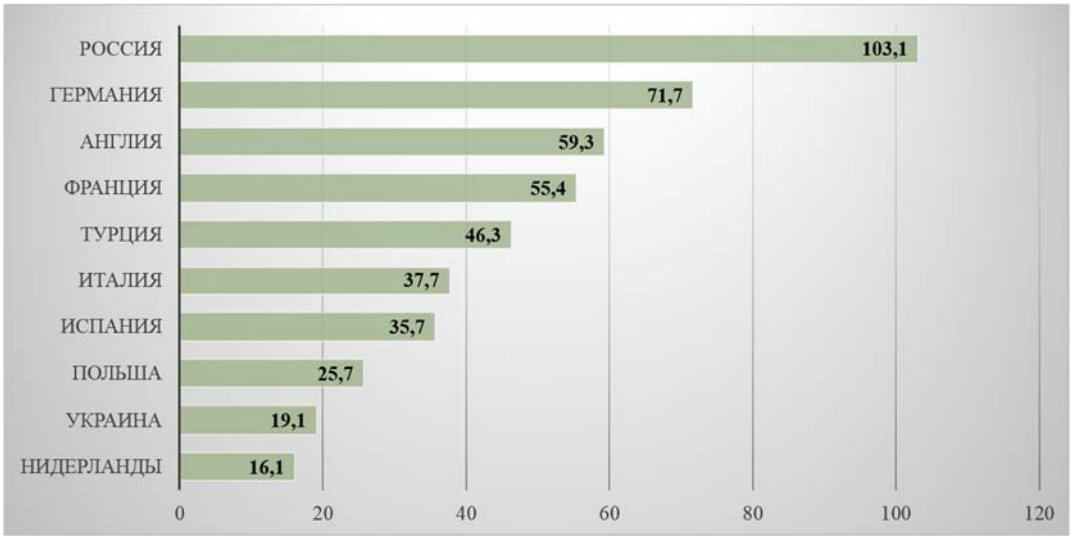


Рис. 1. Топ 10 стран с самым высоким числом интернет – пользователей по состоянию на ноябрь 2015 г. Данные указаны в миллионах пользователей

Исследовательские агентства, в соавторстве с компанией Яндекс собирают информацию о том, как выглядит монитор пользователя сети Интернет. По их данным основными источниками являются социальные сети, видеохостинги, блогохостинги и страницы поисковых систем, которые сегодня сами по себе уже являются источниками новостной информации.

При исследовании данных по статистике того как менялось соотношение пользователей Интернет и тех, кто не пользуется сетями общего доступа на протяжении десяти лет с 2004 по 2014, видно, что выросло целое поколение людей, которое сейчас и стало объектом воздействия противника (рис. 2) [4].

Исследования ТОП 10 сайтов по полярности в России, подтверждают, что по охвату аудитории все же социальные медиа лидируют, и именно они становятся основным инструментом взаимодействия с аудиторией. По результатам исследования группы Яндкс-медиа были представлены домены, которые вошли в ТОП-10 по числу просмотров во всех 26 исследованных российских городах (без учета домена yandex):

1. Vk.com
2. Avito.ru
3. Mail.ru
4. Ok.ru
5. Youtube.com
6. Aliexpress.com
7. Kinogo.com
8. Google.com
9. Wikipedia.org
10. Facebook.com

Период охвата исследования январь-февраль 2016года [5].

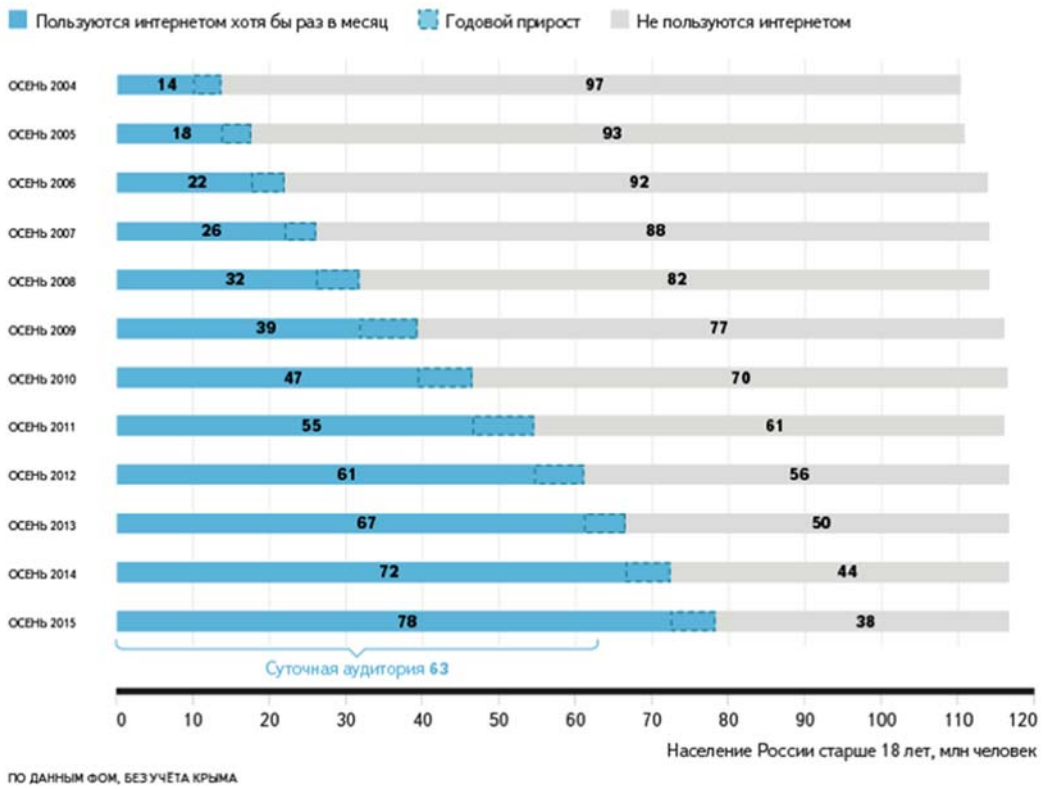


Рис. 2. Изменение соотношения пользователей Интернета и людей, которые не выходят в сеть. По данным без учета Крыма, при учете населения России старше 18 лет. Данные указаны в миллионах пользователей

Выводы

Сегодня проблема выявления информационно-психологического воздействия в информационной инфраструктуре государства должна решаться иначе. Авторы предлагают рассматривать существующие методы анализа информационно-психологического поля, такие как:

– алгоритмы анализа больших данных (*BigData*), которые использовал Дональт Трамп в своей предвыборной компании, при анализе интересов избирателей по регионам;

– системы управление инцидентами (SIEM), позволяющие осуществлять мониторинг событий информационной безопасности, и прогнозировать состояние информационной системы;

– поисковые системы и алгоритмы (SERM), которые можно использовать как способ управления поисковой выдачи по заданной рубрике. Сегодня мы уже можем таким образом настроить доступные новостные ленты в социальных сетях по пользователям, чтобы изолировать общество от воздействия со стороны противника.

– системы мониторинга соцмедиа (ORM), позволяющие управлять информационно-психологическим полем государства в режиме онлайн, снижать или увеличивать интерес пользователей к проблеме, контролировать их вовлеченность.

Подводя итоги, авторы подчеркивают, что привычные способы управления техническими сторонами информационной безопасности государства теперь не обеспечивают и не гарантируют защиту государства и общества в целом. Интернет это уже даже не окно, это новая сфера, в которой мы вращаемся. Появление социальных медиа и вовлечение аудитории зачастую в деструктивную деятельность – это только начало.

Список используемых источников

1. Доктрина информационной безопасности Российской Федерации (утв. Президентом РФ от 9 сентября 2000 г. N Пр-1895) // СЗ РФ, 12.12.2016, N 50, ст. 7074.

2. Карев А. С., Бирих Э. В., Сахаров Д. В, Виткова Л. А. Проблемы информационной безопасности в интернете вещей // Интернет вещей и 5G. 2-я Международная научно-техническая конференция студен-тов, аспирантов и молодых ученых : сб. науч. ст. 2016. С. 66–70.

3. Telecommunications reports that provide statistics and analysis on the European Internet and Telecommunications markets // Internet World Stats. URL: http://www.internetworldstats.com/stats4.htm (дата обращения 01.02.2017).

4. Никушин А. В. Численность интернет-пользователей [Электронный ресурс] // БИТ. Бизнес&Информационные технологии. 2016. № 08 (61). URL: http://bit.samag.ru/archive/article/1748 (дата обращения 01.02.2017).

5. Популярные общероссийские и локальные сайты // Компания Яндекс. Исследование «Развитие интернета в регионах России». URL: https://yandex.ru/company/researches/2016/ya_internet_regions_2016 (дата обращения 01.02.2017).

УДК 004.62

ИССЛЕДОВАНИЕ СПОСОБОВ КОНТРОЛЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОТКРЫТЫХ ДАННЫХ

Л. А. Виткова, О. Н. Рябова, Д. В. Сахаров, Э. Н. Тихонова

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

В современном мире открытые данные являются неотъемлемой частью повседневной жизни, вследствие чего они подвержены различного рода неправомерному и недобросовестному использованию. Авторы анализируют угрозы, оценивают риски и исследуют способы обеспечения безопасности открытых данных.

открытые данные, общедоступные данные, публичные данные, открытые ресурсы, информационная безопасность.

Открытые данные сегодня становятся одним из источников экономического роста, развития инновационного, малого и среднего бизнеса. Основным поставщиком наборов открытых данных являются госорганы, но согласно статистике Портала открытых данных порядка 3 % наборов ОД поставляются негосударственными организациями и их число с каждым годом увеличивается.

На едином портале открытых данных data.gov.ru на декабрь 2016 г. опубликовано более 11,5 тыс. наборов данных, востребованность которых подтверждается более чем 1,5 млн просмотров и 44,4 тыс. скачиваний, из них только 21 набор – это данные негосударственных структур. На рис. 1 представлен рейтинг открытости федеральных органов исполнительной власти по состоянию на 2016 г. [1].

Комплексный индекс открытости федеральных органов исполнительной власти (ФОИВ)* *(приведены значения в пунктах, в скобках - прирост в местах по отношению к результатам 2015 года)*	
I группа (безусловно открытые)	
МЧС России	**58,7** (+1)
Минобороны России	**57,5** (-1)
Россельхознадзор	**53,7** (+18)
II группа (скорее открытые)	
Роскомнадзор	**53,4** (+2)
Минкультуры России	**52,8** (+18)
МИД России	**52,7** (+5)
Минкомсвязь России	**52,0** (+5)

Рис. 1. Рейтинг открытости федеральных органов исполнительной власти на 2016 г.

Данный рейтинг составлен Всероссийским центром изучения общественного мнения (ВЦИОМ) совместно с Открытым правительством. Он отражает качество реализации Концепции открытости в работе федеральных органов исполнительной власти.

Использование приложений на основе ОД делает информацию о деятельности власти более доступной для граждан, предпринимателям помогает создавать и усовершенствовать коммерческие сервисы [2].

Организация свободного доступа к общедоступной информации в форме открытых данных осуществляется в соответствии с требованиями:

а) доступ к общедоступной информации в форме открытых данных не требует регистрации и авторизации, в случаях, если иное не предусмотрено постановлениями Правительства Российской Федерации; б) пользование общедоступной информацией в форме открытых данных не может быть обусловлено требованием использования пользователями определенных веб-обозревателей или установки на технические средства пользователей специального программного обеспечения [3]. В нашей стране направление открытых данных появилось сравнительно недавно и вопросы информационной безопасности при их использовании еще недостаточно проработаны. Схематично процесс формирования открытых данных в органах власти приведен на рис. 2.

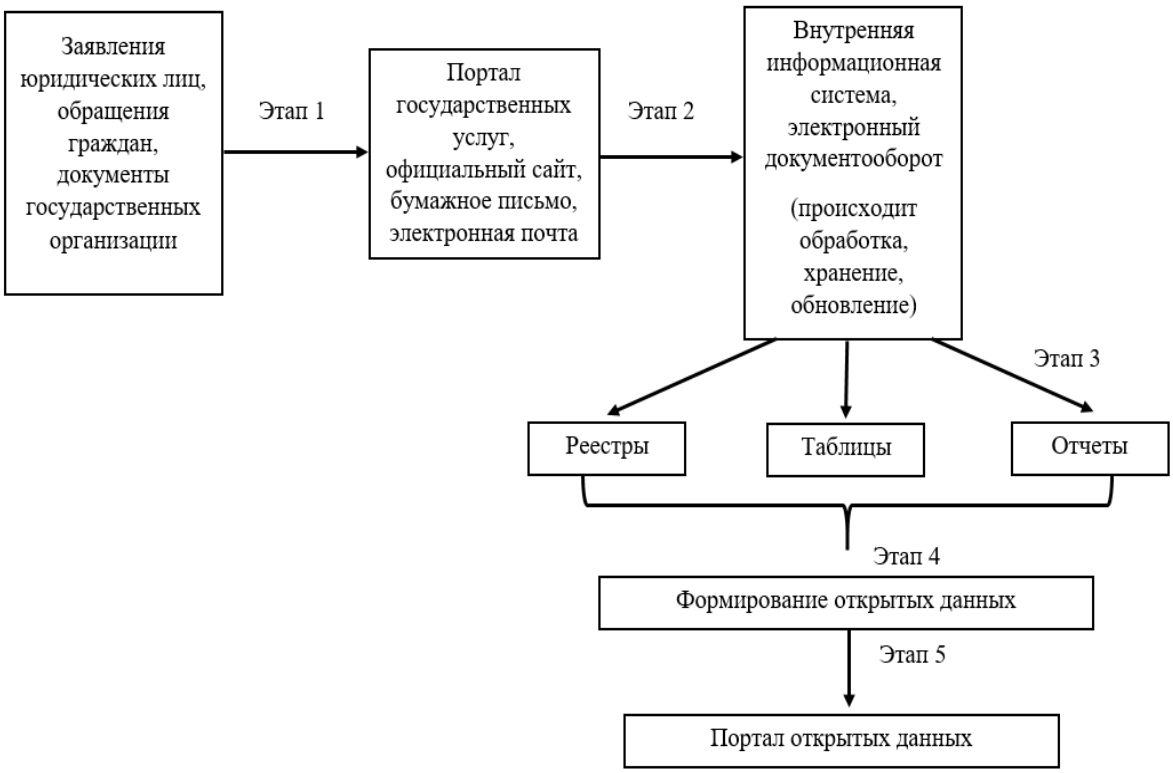


Рис. 2. Формирование ОД в органах власти

На каждом этапе обработки информации и формирования наборов ОД возможно возникновение угрозы безопасности информации. Они могут быть разделены на две большие группы: преднамеренные и не преднамеренные угрозы (рис. 3).

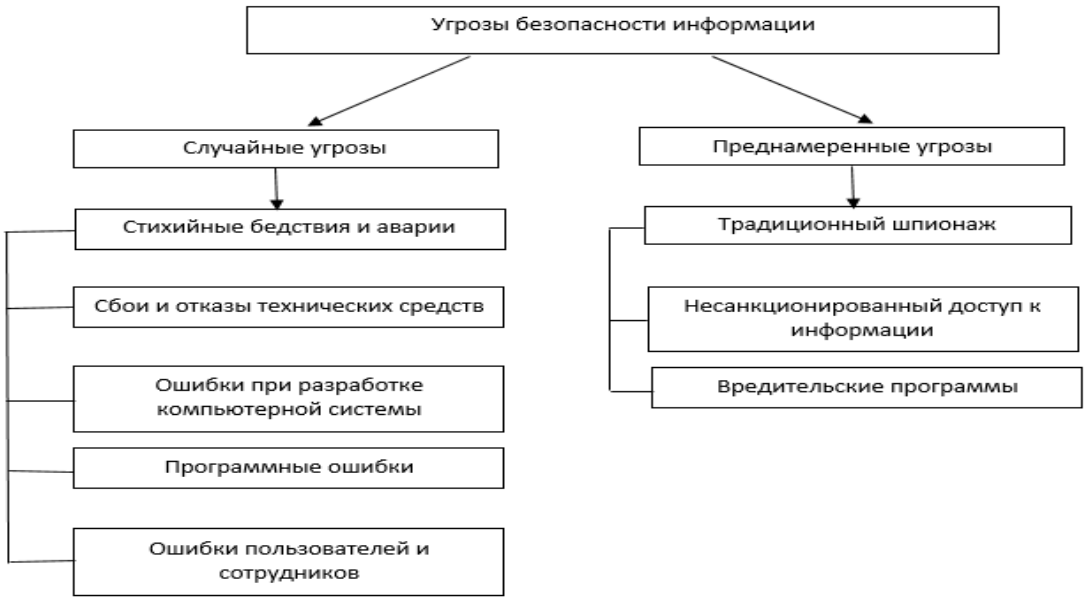


Рис. 3. Виды угроз

Возникновение первой группы угроз чаще всего наблюдается на 1, 2, 3 и 4 этапах формирования ОД. При этом степень защиты информации на этапах 2, 3 и 4 достаточно высокая и регулируется большим количеством нормативной и технической документации, контроль соблюдения требований осуществляется ФСТЭК. Этапы 1 и 5, а также дальнейшее распространение данных с сети Интернет наиболее подвержены угрозам из второй группы. Средства и методы защиты информации на 1 и 5 этапах создания ОД постоянно совершенствуются. Для автоматизации процесса сбора и анализа информации о событиях информационной безопасности используются специализированные системы мониторинга информации о событиях безопасности, поступающих из различных источников. В качестве таких источников могут выступать средства защиты информации, общесистемное и прикладное ПО [4].

Самый слабый и плохо исследованный аспект безопасного использования проектов на основе ОД можно условно назвать этапом 6 – распространение наборов и приложений на их основе в сети Интернет. При агрегации массивов информации, доступной для машинной обработки, возможно не только создание социально полезных продуктов, но и инструментов анализа, которые могут быть использованы такими видами нарушителей, как специальные службы иностранных государств, террористические, экстремистские группировки, конкурирующие организации.

Эти аспекты отражены в новой Доктрине информационной безопасности, принятой 5 декабря 2016 г. Доктрина создала политическую основу согласования деятельности органов государственной власти по реализации

национальных интересов в информационной сфере и защите их от внешних и внутренних угроз [5].

В качестве одного из инструментов контроля можно использовать широко применяемые для создания вирусов исполняемые файлы Loader.exe. В базовом понятии под словом «лоадер» понимается некое программное обеспечение, выполняющее функции доставки файлов на компьютер пользователя. Форматы, определенные для публикации открытых данных – CSV, XML, JSON, ODS, допускают использование подобных структур. Загрузчики позволяют предварительно обрабатывать файлы, содержащие пошаговые инструкции, которым компьютер следует, чтобы выполнить ту или иную функцию. Loader.exe способен манипулировать другими программами, записывать ввод данных и спрятать себя. Таким образом, можно получить информацию о распространении и использовании наборов открытых данных.

Исследования в области информационной безопасности при использовании ОД позволит обеспечить эффективное достижение основной цели размещения открытых данных – создание условий для получения максимального международного, политического, социального и экономического эффекта от их использования гражданами России, бизнес-сообществом и другими представителями российского общества, при этом не нарушая интересов физических лиц, государственных учреждений и бизнеса [6].

Список используемых источников

1. Совет по открытым данным обсудил раскрытие статистики и публикацию отчётности компаний [Электронный ресурс] // Открытое Правительство. URL: http://open.gov.ru/gov_commission/news/5515680/ (дата обращения 06.03.2017).

2. Пресс-выпуск № 3259 [Электронный ресурс]. URL: https://wciom.ru/index.php?id=236&uid=115980 (дата обращения 06.03.2017).

3. Береснева Е. Е. opendata: зачем они нужны и что это такое [Электронный ресурс] // Портал «Научная Россия». URL: https://scientificrussia.ru/articles/opendata-zachem-nam-nuzhny-otkrytye-dannye (дата обращения 06.03.2017).

4. Проект Постановления Правительства Российской Федерации «О федеральной государственной информационной системе» [Электронный ресурс] // Минэкономразвития России 20.07.2016. URL: http://www.garant.ru/products/ipo/prime/doc/56577108/#ixzz4cBHkTXm4 (дата обращения 06.03.2017).

5. Малков П. В. Реализация концепции ОД в РФ 15.12.2014 [Электронный ресурс] // Внедрение и использование ОД для экономического развития. URL: http://ac.gov.ru/events/04338.html (дата обращения 06.03.2017).

6. Доктрина информационной безопасности РФ от 5 декабря 2016 г. [Электронный ресурс] // Информационная безопасность РФ. URL: http://www.femida.info/ 14/19002.htm (дата обращения 06.03.2017).

УДК 004.056.53

ФОРМАТЫ ОПИСАНИЯ ПРАВИЛ ДЛЯ КОРРЕЛЯЦИИ СОБЫТИЙ БЕЗОПАСНОСТИ В КИБЕРФИЗИЧЕСКИХ СИСТЕМАХ

М. Н. Вихров[1], А. В. Федорченко[2], А. А. Чечулин[1]

[1]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
[2]Санкт-Петербургский институт информатики и автоматизации Российской академии наук

В настоящее время информационные технологии имеют широкое применение в различных сферах жизни человека, а уровень их распространения продолжает расти. С учетом появления киберфизичеких систем, задача обеспечения их безопасности становится особенно актуальной. Данная работа посвящена изучению реализаций правило-ориентированного подхода в процессе корреляции информации, как одного из ключевых этапов обработки данных, в средствах обеспечения безопасности разных классов. Описываются форматы правил, виды их представления и примеры для конкретных систем безопасности. Также приводится сравнение кибернетических (информационных) и физических средств защиты для выявления особенностей построения механизмов обеспечения безопасности киберфизических систем.

корреляция событий безопасности, правило-ориентированный подход, средства защиты информации, СЗИ, киберфизические системы.

На сегодняшний день развитие компьютерных систем и сетей передачи информации все больше используется как в бытовой технике и устройствах личного потребления, так и для обеспечения работоспособности критически важных объектов. Значительные перспективы применения киберфизических систем, как систем следующего поколения, в промышленных, военных и других критически важных отраслях обуславливают актуальность задачи обеспечения безопасности инфраструктур, в которых они применяются. Несмотря на то, что на данный момент существует множество классов средств защиты информации (СЗИ), ни один из них в полной мере не в состоянии обеспечивать должный уровень защищенности. Данная проблема является следствием разнородности СЗИ, их независимой разработки и отсутствия общепринятых стандартов при использовании различных методов. Между тем, во многих решениях используются схожие методы, модели и этапы обработки данных. Корреляция событий и информации безопасности является одним из таких этапов, основная цель которого заключается в преобразовании данных к высокоуровневому представлению, а также выявлении инци-

дентов и предупреждений безопасности. Однако, в СЗИ разных классов выполнение п роцесса корреляции значительно отличается по возлагаемым задачам и способам реализации.

В существующей литературе приводится множество методов корреляции данных, среди которых можно выделить: метод на основе моделирования (*model-based reasoning,* MBR); правило-ориентированный метод (*rule-based reasoning,* RBR); метод на основе кодовой книги (*codebook*); метод рассуждений на основе прецедентов (*case-based reasoning*, CBR); метод активного исследования (*active probing*), а также различные интеллектуальные методы [1, 2, 3]. В статье рассматривается правило-ориентированный метод, поскольку он используется в процессе корреляции большинства систем безопасности. Преимуществом данного метода является строгое соблюдение условий при принятии решений, а недостатками – большие трудозатраты на создание правил и сложность их составления.

В общем виде процесс корреляции можно представить как «черный ящик» – где на входе имеется определенный набор «сырых» событий, полученных от различных источников, а на выходе – результат их обработки. Как правило, процесс корреляции событий безопасности рассматривается в виде многоуровневой иерархии этапов: (1) нормализации; (2) предобработки; (3) анонимизации; (4) агрегации и фильтрации; (5) восстановления хода атаки; (6) восстановления сессии атаки; (7) определения источника и цели атаки; (8) многошаговой корреляции; (9) анализа ущерба; (10) приоритезации; (11) фильтрации на основе ранжирования [4]. Однако, присутствие каждого из этапов в конечном решении зависит от его реализации. Цель каждого из этапов заключается в выполнении определенных операций над обрабатываемыми данными безопасности.

Правила корреляции – самостоятельная оперативная единица правило-ориентированного метода корреляции, за счет которого изменяется входная информация. В составе правила всегда присутствует как минимум три компонента – источник данных, условие и реакция. Правила бывают простыми и сложными. Простое правило имеет одно условие, сопоставленное одному действию над входными данными. Сложное правило является совокупностью простых правил, связанных друг с другом. В статье выделяют четыре основных формата представления правил корреляции – (1) табличный, (2) граф-ориентирован-ный (матричный), (3) шаблонный, (4) конечный автомат (на основе машины конечных состояний).

Далее более подробно будут рассмотрены реализации правило-ориентированного метода корреляции данных в различных системах обеспечения безопасности, а именно: (1) системы обнаружения вторжений (*Intrusion Detection System*, IDS), (2) системы контроля и управления доступом (СКУД) и (3) системы управления событиями и информацией безопасности (*Security Information & Event Management*, SIEM).

Средства класса IDS разделяются на статические и динамические. Статические решения делают «снимки» (*snapshot*) среды и осуществляют их анализ. Типовая структура правила рассмотрена на примере IDS с открытым кодом Snort [4, 5] и представлена на рис. 1.

```
<действие_правила><протокол><порт><оператор_направления><порт>
([метаданные];[даные_о_содержимом_пакета];[данные_в_заголовке];[действие_после_обнаружения])
```

Рис. 1. Структура правила IDS Snort

Поле «действие правила» характеризует вариант обработки информации, которое может быть активным или пассивным. Например, данный параметр может принимать следующие значения: создание предупреждения (*alert*), запись в лог (*log*), запрет или разрешение на передачу пакета (*drop/pass*) и другие. Поле «протокол» позволяет выбрать сетевой протокол для фильтрации, например, TCP или UDP. Поле «порт» позволяет назначить номер TCP/UDP порта для дальнейшего принятия решения об обработке пакета. Данное поле используется для: (1) обозначения порта источника; (2) обозначения порта назначения. Поле «оператор направления» характеризует выбор направления трафика – от отправителя к получателю или двустороннее. Опциональные параметры характеризуют специфические поля отбора пакетов: по известным метаданным, данным из заголовка и многим другим. Все правила имеют общую структуру и хранятся в базе данных, которая постоянно обновляется.

Системы контроля и управления доступом (СКУД) являются примером физических систем безопасности, в котором также используется правило-ориентированный метод корреляции событий. В качестве примера можно представить охраняемый объект, вход и выход в помещения которого производится только по электронным пропускам зарегистрированных в системе сотрудников. Пропускной режим при этом не позволяет проходить в помещения каждой следующей зоны доступа, не зарегистрировав ключ в предыдущей зоне (кроме нулевой зоны доступа) на объекте. При прохождении сотрудника в любую зону доступа без регистрации в предыдущей зоне (например, при прохождении двух сотрудников по одному пропуску, или перепрыгивании турникета) на штатном средстве контроля администратора безопасности сформируется оповещение об инциденте нарушении правила пропускного режима и предупреждение о попытке несанкционированного доступа.

Работа SIEM-систем подразумевает анализ в реальном времени событий (предупреждений, инцидентов) безопасности, исходящих от различных источников информации. Как правило, SIEM-системы имеют набор предустановленных правил корреляции, которые сопоставляют события от источников и могут оповестить администратора безопасности о возникшей

угрозе. На пример, в решении HP ArcSight [6] первичная обработка событий происходит на коннекторах SIEM-системы. Обработка включает в себя фильтрацию, категоризацию, приоритезацию, агрегирование и нормализацию информации. Далее события в формате CEF (*Common Event Format*) [7] отправляются в ядро системы, где производится их дальнейшая корреляция, принятие решения об угрозе и визуализация результатов. Существует несколько вариантов условий обнаружения подозрительного поведения из информации получаемых событий: (1) по определенному событию с источника; (2) по нескольким последовательным событиям с источников за определенный период; (3) по достижению порогового количества событий одного типа за определенный период; (4) по отклонению определенных показателей от эталонного (либо среднего) значения.

Таким образом, в результате анализа ряда СЗИ следует заключить, что для киберфизических систем, где оперативность и точность мониторинга угроз являются критичными характеристиками системы обеспечения безопасности, больше всего подходят SIEM-системы. На рис. 2 представлена общая схема процесса корреляции для киберфизических систем с использованием правил.

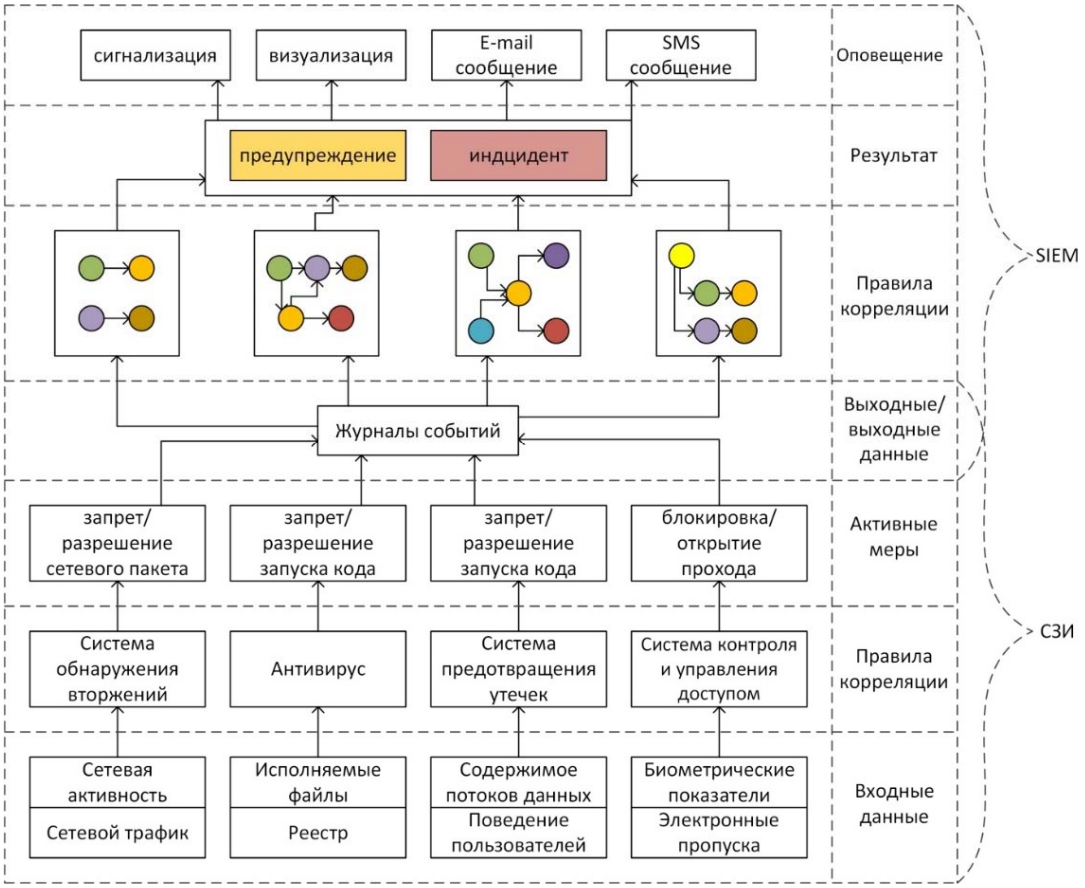


Рис. 2. Общая схема процесса корреляции на основе правило-ориентированного метода для киберфизических систем

Результатом данного процесса являются сгенерированные предупреждения и события об инцидентах, а также сгруппированные или отсеенные события на промежуточных этапах. На данном рисунке журналы событий являются выходными данными для всевозможных СЗИ и входными данными для SIEM-системы. Также стоит отметить, что СЗИ в ходе своей работы зачастую также используют правила для принятия решений. Однако на данный момент SIEM-системы не ориентированы на защиту киберфизических инфраструктур, а также имеет ряд общих проблем при реализации процесса корреляции событий безопасности.

Предполагается, что результаты данного исследования позволят построить обобщенную схему корреляции, которую можно было бы использовать как для информационных, так и для киберфизических систем. В дальнейшей работе планируется разработка программно-аппаратного прототипа и проведения исследований на экспериментальном стенде [8, 9].

Работа выполнена при финансовой поддержке РНФ грант № 15-11-30029 в СПИИРАН.

Список используемых источников

1. Федорченко А. В., Левшун Д. С., Чечулин А. А., Котенко И. В. Анализ методов корреляции событий безопасности в SIEM-системах. Часть 2 // Труды СПИИРАН. 2016. Вып. 6 (49). С. 208–225.

2. Muller A. Event Correlation Engine. Master`s Thesis. Swiss Federal Institute of Technology Zurich. 2009. 165 p.

3. Ghorbani A. A., Lu W., Tavallaee M. Network Intrusion Detection and Prevention. Springer, 2010. 224 p.

4. Федорченко А. В., Левшун Д. С., Чечулин А. А., Котенко И. В. Анализ методов корреляции событий безопасности в SIEM-системах. Часть 1 // Труды СПИИРАН. 2016. Вып. 47. С. 5–27.

5. Белоголовый В. Г., Ястребов В. А. Практика использования IDS Snort [Электронный ресурс]. СПбГУАП, Санкт-Петербург 2011. URL: http://pandia.ru/text/78/320/66161.php (дата обращения 26.02.2017).

6. Hewlett Packard Enterprise. ArcSight Express. [Электронный ресурс] URL: http://www8.hp.com/by/ru/software-solutions/arcsight-express-siem-appliance/index.html? (дата обращения 26.02.2017).

7. Common Event Format. ArcSight [Электронный ресурс]. URL: https://kc.mcafee.com/resources/sites/MCAFEE/content/live/CORP_KNOWLEDGEBASE/78000/KB78712/en_US/CEF_White_Paper_20100722.pdf (дата обращения 26.02.2017).

8. Kotenko I., Doynikova E., Chechulin A. Security metrics based on attack graphs for the Olympic Games scenario // 22th Euromicro International Conference on Parallel, Distributed, and Network-Based Processing (PDP 2014). IEEE Computer Society. 2014. PP. 561–568.

9. Котенко И. В., Десницкий В. А., Чечулин А. А. Исследование технологии проектирования безопасных встроенных систем в проекте Европейского сообщества SecFutur // Защита информации. Инсайд. 2011. № 3 (39). С. 68–75.

УДК 004.4'242

РАЗРАБОТКА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ АВТОМАТИЗАЦИИ ПОСТРОЕНИЯ УМНОЖИТЕЛЯ В ПОЛЕ ГАЛУА ПО СХЕМЕ РЕЙХАНИ-МАЗОЛЕХА

С. С. Владимиров, Д. Ф. Мухаметшина

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

В статье рассмотрены вопросы разработки программного обеспечения для решения задачи автоматизации формирования программного кода при построении умножителя элементов двоичного поля Галуа по схеме Рейхани-Мазолеха. Приведены требования к разрабатываемому программному обеспечению, показаны процедура и пример работы программы, а также предложены направления дальнейшего развития разрабатываемого программного обеспечения.

автоматизация разработки, автоматическое генерирование кода, поля Галуа, умножение элементов поля Галуа, умножитель Рейхани-Мазолеха, язык программирования Си.

При разработке современных систем передачи дискретных сообщений широко используются методы помехоустойчивого кодирования, направленные на повышение достоверности при передаче данных по каналам связи, подверженным помехам, и методы шифрования, предназначенные для обеспечения конфиденциальности передаваемых данных. Многие популярные методы помехоустойчивого кодирования, например, коды Рида-Соломона (РС) [1], и способы шифрования, такие как алгоритм симметричного шифрования AES [2], основаны на вычислениях в двоичных полях Галуа. Базовыми арифметическими операциями в полях Галуа являются сложение и умножение, из которых операция умножения имеет большую сложность, требуя большего количества логических элементов, что может приводить к задержкам при реализации алгоритмов помехоустойчивого кодирования и методов шифрования.

Основным методом реализации умножения является так называемый логарифмический умножитель, использующий операции логарифмирования и антилогарифмирования, для каждой из которых необходимо хранить в памяти отдельный массив элементов поля, что является существенным недостатком в случае ограничений на использование оперативной и постоянной памяти. Альтернативой являются алгоритмы умножения, не требующие операций логарифмирования и антилогарифмирования, например, алгоритм умножения длинных чисел Карацубы-Офмана [3, 4, 5] или алгоритм Мастровито, позволяющий реализовать эффективный умножитель на логических

элементах. В начале 2000-х членами IEEE А. Рейхани-Мазолехом и М. А. Хасаном был предложен эффективный вариант алгоритма Мастровито, так называемый алгоритм Рейхани-Мазолеха [5, 6]. Алгоритм Рейхани-Мазолеха, как и оригинальный алгоритм Мастровито, отличается большей сложностью построения аппаратной схемы умножителя и написания программного кода по сравнению с логарифмическим умножителем, имея при этом регулярную структуру, которая позволяет автоматизировать процедуры формирования аппаратной схемы и генерации программного кода.

На кафедре сетей связи и передачи данных СПбГУТ перед авторами была поставлена задача разработки программного обеспечения для автоматизации процесса разработки умножителя по схеме Рейхани-Мазолеха и, в перспективе, других типов умножителей.

Алгоритм Рейхани-Мазолеха для умножения элементов двоичного поля Галуа

Обозначим множители, являющиеся элементами поля Галуа GF(2^m), порождаемого неприводимым полиномом $p(x)$, как A и B и представим их в виде сумм $A = \sum_{i=0}^{m-1} a_i \varepsilon^i$ и $B = \sum_{i=0}^{m-1} b_i \varepsilon^i$, соответственно, где $a_i, b_i \in \{0,1\}$, а ε^i – элементы левого степенного базиса поля GF(2^m) [5, 6].

Элементы a_i можно представить в виде вектора $\mathbf{a} = [a_0, a_1, ..., a_{m-1}]^T$. В таком случае, множитель A можно представить как произведение векторов $\mathbf{A} = \boldsymbol{\varepsilon}^T\mathbf{a}$, где $\boldsymbol{\varepsilon} = [1, \varepsilon, ..., \varepsilon_{m-1}]^T$. Аналогично представляется и второй множитель B [5, 6].

Умножитель Рейхани-Мазолеха основан на понятии приведенной двоичной матрицы $\mathbf{Q}$ размера $(m - 1)\times m$, получаемой из тождества $\boldsymbol{\varepsilon}^{\uparrow} \equiv \mathbf{Q}\boldsymbol{\varepsilon} \left(\mathrm{mod}\left(p(\varepsilon)\right)\right)$, где $\boldsymbol{\varepsilon}^{\uparrow} = [\boldsymbol{\varepsilon}^m, \boldsymbol{\varepsilon}^{m-1}, \ldots, \boldsymbol{\varepsilon}^{2m-2}]^T$. Каждому неприводимому полиному $p(x)$ соответствует одна матрица $\mathbf{Q}$ [5, 6].

Дополнительно вводятся два вектора $\mathbf{d}$ и $\mathbf{e}$, являющиесятся функциями от A и B:

$$\mathbf{d} = \mathbf{L}\mathbf{b} \text{ и } \mathbf{e} = \mathbf{U}\mathbf{b}, \tag{1}$$

где $\mathbf{L}$ – нижнетреугольная матрица Теплица размера $m\times m$, а $\mathbf{U}$ – верхнетреугольная матрица Теплица размера $(m - 1)\times m$ [5, 6].

$$\mathbf{L} \triangleq \begin{bmatrix} a_0 & 0 & 0 & \cdots & 0 \\ a_1 & a_0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ a_{m-2} & a_{m-3} & \cdots & a_0 & 0 \\ a_{m-1} & a_{m-2} & \cdots & a_1 & a_0 \end{bmatrix}; \ \mathbf{U} \triangleq \begin{bmatrix} 0 & a_{m-1} & a_{m-2} & \cdots & a_1 \\ 0 & 0 & a_{m-1} & \cdots & a_2 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & a_{m-2} \\ 0 & 0 & \cdots & 0 & a_{m-1} \end{bmatrix}. \tag{2}$$

Вектор $\mathbf{c}$, соответствующий результату C произведения элементов поля A и B, вычисляется по формуле:

$$\mathbf{c} = \mathbf{d} + \mathbf{Q}^T\mathbf{e}, \quad (3)$$

где $\mathbf{c} = [c^0, c^1, ..., c^{m-1}]^T$ [5, 6].

Некоторые типы порождающих полиномов $p(x)$ имеют определенные формы матрицы **Q**, позволяющие построить ее, не прибегая к сложным расчетам [5, 6]:

1. Равномерно распределенные полиномы вида: $p(x) = x^{ns} + x^{(n-1)s} + \ldots + x^s + 1$, образующие поле Галуа GF(2^m) с $m = ns$.

2. Триномы: $p(x) = x^m + x^k + 1$, где $1 \le k \le m$.

3. Пентаномы: $p(x) = x^m + x^{k_3} + x^{k_2} + x^{k_1} + 1$, где $1 \le k_1 < k_2 < k_3 \le m - 1$.

Программа-генератор для автоматического формирования кода

Для автоматизации построения умножителя была написана программа-генератор, формирующая программный код умножителя для задаваемого пользователем порождающего полинома поля Галуа. Программа-генератор реализована на языке программирования JavaScript с использованием программной платформы Node.js [7], что позволило упростить разработку и обеспечить высокую переносимость кода для различных операционных систем, позволив в дальнейшем использовать ее в форме веб-приложения. В качестве интерфейса программы-генератора выбран консольный текстовый интерфейс.

При запуске программа-генератор рассчитывает приведенную матрицу **Q** для порождающего полинома поля $p(x)$, вводимого пользователем в двоичном виде в качестве параметра командной строки программы. Затем, на основе степени образующего полинома $p(x)$ и матрицы **Q** формируется программный код умножителя Рейхани-Мазолеха. В настоящее время программа-генератор формирует код умножителя на языке Си с использованием директив препроцессора #define, что, как показали ранее проведенные эксперименты, обеспечивает уменьшение размера программы по сравнению с логарифмическим умножителем при обеспечении максимального быстродействия [8].

Программный код умножителя состоит из трех блоков.

1. Блок директив препроцессора для преобразования входных значений – множителей A и B – в массив их элементов (двоичных коэффициентов).

2. Блок директив вычисления векторов **d** и **e** по формулам (1) на основе нижнетреугольной и верхнетреугольной матриц Теплица (2).

3. Блок расчета результата умножения на основе приведенной матрицы **Q** по формуле (3).

В функции main программы умножителя содержится код, преобразующий входные данные из строковых значений в беззнаковые целые, а также код для вывода результата умножения в консоль.

Пример программного кода для порождающего полинома $p(x) = x^6 + x + 1$ показан на рисунке.

```
#include <stdio.h>
#include <stdlib.h>

#define a0  ((A&1))
#define a1  ((A&2) >> 1)
#define a2  ((A&4) >> 2)
#define a3  ((A&8) >> 3)
#define a4  ((A&16) >> 4)
#define a5  ((A&32) >> 5)
#define b0  ((B&1))
#define b1  ((B&2) >> 1)
#define b2  ((B&4) >> 2)
#define b3  ((B&8) >> 3)
#define b4  ((B&16) >> 4)
#define b5  ((B&32) >> 5)

#define d0  (a0&b0)
#define d1  (a1&b0) ^ (a0&b1)
#define d2  (a2&b0) ^ (a1&b1) ^ (a0&b2)
#define d3  (a3&b0) ^ (a2&b1) ^ (a1&b2) ^ (a0&b3)
#define d4  (a4&b0) ^ (a3&b1) ^ (a2&b2) ^ (a1&b3) ^ (a0&b4)
#define d5  (a5&b0) ^ (a4&b1) ^ (a3&b2) ^ (a2&b3) ^ (a1&b4) ^ (a0&b5)
#define e0  (a5&b1) ^ (a4&b2) ^ (a3&b3) ^ (a2&b4) ^ (a1&b5)
#define e1  (a5&b2) ^ (a4&b3) ^ (a3&b4) ^ (a2&b5)
#define e2  (a5&b3) ^ (a4&b4) ^ (a3&b5)
#define e3  (a5&b4) ^ (a4&b5)
#define e4  (a5&b5)

#define c0  ((d0^e0))
#define c1  ((d1^e0^e1) << 1)
#define c2  ((d2^e1^e2) << 2)
#define c3  ((d3^e2^e3) << 3)
#define c4  ((d4^e3^e4) << 4)
#define c5  ((d5^e4) << 5)
#define cmul (c0^c1^c2^c3^c4^c5)

int main(int argc, char *argv[])
{
    char *pCh;
    unsigned int A = strtoul(argv[1], &pCh, 2);
    unsigned int B = strtoul(argv[2], &pCh, 2);
    unsigned int C;
    C = cmul;
    printf("%d\r\n", C);
    return C;
}
```

Рисунок. Пример программного кода преобразования входных значений для порождающего полинома $p(x) = x^6 + x + 1$

Корректность генерируемой программы была проверена с помощью сетевого калькулятора Галуа [9] и программы умножителя, написанной на JavaScript для полей Галуа со степенями $4 \leq m \leq 32$.

Направления развития программного обеспечения

В статье была рассмотрена часть задачи автоматизации процесса разработки систем кодирования и шифрования, основанных на операциях в конечных полях.

Дальнейшая разработка программного комплекса будет вестись по трем направлениям:

1. Расширение списка языков программирования, для которых формируется программный код умножителя. В первую очередь предполагается обеспечить поддержку популярных языков программирования Pascal, Python, Java, а также основных языков описания аппаратуры Verilog, VHDL и AHDL, что позволит быстро генерировать код для построения умножителя на основе ПЛИС.

2. Разработка графического интерфейса пользователя как отдельной программы (*front-end*), независимой от программы-генератора (*back-end*) и связанной с ней по методам межпроцессного взаимодействия. Это позволит использовать программу-генератор как в виде пользовательского приложения для персонального компьютера, так и в виде веб-приложения с отдельным веб-интерфейсом.

3. Расширение списка умножителей, которые могут быть сформированы с помощью программы-генератора, что позволит создать универсальную программу, которая позволит при разработке систем передачи данных сравнивать различные схемы умножителей, и выбирать наиболее подходящую.

Список используемых источников

1. Robert H. Morelos-Zaragoza The Art of Error Correcting Coding. Chichester : John Wiley & Sons, Ltd, 2002. 232 p. ISBN 0471-49581-6.

2. Баричев С. Г., Гончаров В. В., Серов Р. Е. Основы современной криптографии. М. : Горячая Линия – Телеком, 2011. 175 с. ISBN 978-5-9912-0182-7.

3. Карацуба А., Офман Ю. Умножение многозначных чисел на автоматах // Доклады Академии Наук СССР. 1962. Т. 145. С. 293–294.

4. Rodriguez-Henriquez F., Koc C.K. On fully parallel Karatsuba Multipliers for GF (2m) // Proceedings of the International Conference on Computer Science and Technology (CST), 2003. P. 405–410.

5. Владимиров С. С. Математические основы теории помехоустойчивого кодирования : учебное пособие. СПб. : СПбГУТ, 2016. 96 с.

6. Reyhani-Masoleh A., Hasan M. A. Low complexity bit parallel architectures for polynomial basis multiplication over GF(2m) // Computers, IEEE Transactions on. 2004. Aug. Vol. 53, no. 8. P. 945–959. ISSN: 0018-9340.

7. Node.js [Electronic resource] : [cite]. URL: https://nodejs.org/ (Accessed date: 03.03.2017).

8. Владимиров С. С. Эффективность умножителя Рейхани-Мазолеха элементов двоичного поля Галуа // Информационные технологии и телекоммуникации. 2015. № 3 (11). С. 84–92.

9. Владимиров С. С. Сетевой программируемый калькулятор Галуа // Инновационные процессы и технологии в современном мире. Международная научно-практическая конференция: материалы конференции. 2013. С. 147–150.

УДК 004.7

РАЗРАБОТКА МЕТОДА ТЕСТИРОВАНИЯ СИСТЕМЫ МЕНЕДЖМЕНТА ИНТЕРНЕТА ВЕЩЕЙ В КОНЦЕПЦИИ УМНОГО ГОРОДА НА БАЗЕ СЕТИ SDN

А. Н. Волков, А. С. Мутханна

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

Статья посвящена тестированию системы менеджмента Интернета Вещей на базе сети SDN. В качестве метода исследования поведения системы менеджмента и сетевой инфраструктуры проводилось тестирование трафиком Интернета вещей. В работе рассмотрена модель «Умного города» на примере Центрального района Санкт-Петербурга. В ходе тестирования были определены такие параметры как: RTT, задержка пакетов в сети. Сделан вывод по использованию SDN сети, как базовой сетевой инфраструктуры в условиях IoT трафика. С целью рассмотрения системы менеджмента IoTDM как сервиса для «Умного города», был проведен натурный эксперимент на разработанной модели, которая в свою очередь отражала возможную схему распределения определенной системы мониторинга и управления для Центрального района Санкт-Петербурга.

Интернет вещей, IoT, нагрузка, HTTP, SDN, ПКС, API, RTT, Smart City, Data Managment.

Введение

Умный город – футуристическая идея или неизбежное будущее? Умный город (*Smart City*) [1], он же «интеллектуальный город», «цифровой город» – понятие, у которого до сих пор нет однозначного определения. Можно сформулировать так, умный город – это город, который использует инфокоммуникационные технологии для эффективного использования ресурсов, что приводит к экономии затрат и энергии, повышению качества жизни жителей [2], улучшении экологической обстановки и т. п.

Такие сервисы, как: автоматический сбор показаний домовых счетчиков электроэнергии [3], автоматизация сервиса городского автотранспорта [4], которая позволяет наблюдать перемещение автобусов, троллейбусов и т. п., и знать приблизительное время их прибытия, городские многофункциональные центры с электронными очередями, электронное здравоохранение, геоинформационные системы и другие системы, облегчающие жизнь человека в большом городе. Но это естественно не все аспекты, которые содержит концепция «Умного города». Для полноценной реализации всех этих идей требуется новая сетевая инфраструктура, новые подходы к организации обработки данных, удовлетворяющая новым требованиям.

В результате развития этих вопросов появляется такое понятие, как Big Data. Можно сделать вывод, что для эффективной работы Smart City необходима глубоко интегрированная система, состоящая из многих подсистем, в которой будет учтены как текущие потребности различных городских служб, так и с учетом перспективы развития в условиях новых факторов.

Мониторинг различных параметров в умном городе производится на основе соответствующих сенсоров. В следствии чего, данную архитектуру можно представить в виде взаимодействия множества Интернет Вещей. Распространение IoT ввело новые комплексные требования к сетям и взаимодействию схем в текущих и будущих сетях. Чтобы сделать это реальным в текущих сетях, сети должны приветствовать неоднородность трафика Интернета Вещей [5].

В данной работе был поднят один из вопросов касающегося автоматизации мониторинга как температурного спектра города, так и значения влажности, для обеспечения наблюдения и выработки соответствующих методов оптимизации экологической обстановки в плотной городской застройке. Так же картина температурной обстановки может быть полезной не только с точки зрения экологических вопросов, но и для автоматизации контроля в сфере пожарной и газовой безопасности.

Также приходит подход программно-конфигуриремых сетей Software-Defined Networks (SDN) [6]. Данный концепция позволяет значительно автоматизировать и облегчить управление сетями за счет возможности их программирования. Данный подход подразумевает разделение уровней на передачу данных и управления, при этом операции по определению маршрута передачи пакета определяет контроллер («мозг» в данной концепции), который имеет информацию о топологии и о состоянии сети, для удобного мониторинга и управления сетью. Данный функционал определяется API контроллера.

Постановка задачи

В условиях большого количества Интернет Вещей, неоднородности трафика, множества пользователей, система менеджмента должна быть устойчива к большим нагрузкам, иметь свойство быстрого восстановления при критических перегрузках. Реализация вопроса безопасности системы так же должна быть проработана на высоком уровне для обеспечения корректного функционирования тех систем «Умного города», за которые отвечает IoTDM. Также сетевая инфраструктура должна удовлетворять особенностям трафика IoT.

В рамках исследования системы IoTDM на базе SDN сети была сформулирована основная задача – провести тестирование сервиса с учетом реальной возможной нагрузки трафиком Интернет Вещей при использовании

протокола HTTP, на основе модели реального района города Санкт-Петербурга. Тестирование по сути сводится к проверке взаимодействия между IoT – устройствами, сетевой инфраструктурой и сервисом IoTDM. В качестве сетевой инфраструктуры была построена сеть SDN, основанная на коммутаторах Mikrotik с поддержкой протокола openflow v.1.0. и контроллере OpenDayLight Berillium SR4.

Тестирование сервиса IoTDM, как системы менеджмента «Умного города»

Для тестирования сервиса IoTDM была построена модель, отображающая возможную архитектуру взаимодействия Интернет Вещей, цель которых – мониторинг таких показателей, как: температура, влажность. Также каждая Интернет Вещь имеет датчик GPS.

Для исследования был выбран Центральный район Санкт-Петербурга, так как для моделирования он более удобен своей формой имеет разделение на 6 муниципальных образований: Дворцовый округ, Литейный округ, Смоленское, Лиговка-Ямское, Владимирский округ, округ № 78, что позволяет равномерно распределить датчики при построении модели.

Лабораторный стенд

В роли сетевой инфраструктуры выступает SDN ядро, построенное на основе контроллера Opendaylight Berillium SR4 и коммутаторах Mikrotik RB 201 1UI AS-RM с поддержкой протокола Openflow v.1.0. В качестве агрегаторов трафика Интернета вещей на каждом openflow – коммутаторе выступают:

– один коммутатор SuperStack 3COM
– два коммутатора Cisco Catalyst 3750G series PoE-24

Иерархическая модель умного города выглядит следующим образом:

– Для равномерного распределения нагрузки на сетевые элементы, за каждым openflow-коммутатором было привязано 2 муниципальных образования.

– В каждом муниципальном образовании было предложено задействовать около 40 перекрестков.

– Каждый перекресток имеет 4 светофора, которые играют роль Интернет Вещей.

– Каждая Интернет Вещь содержит 3 типа датчика: температуры, влажности, GPS.

Работа модели построена по следующему алгоритму:

1. Построение дерева ресурсов с учетом иерархического разделения на муниципалитеты, перекрестки, светофоры.

2. Инициализация Интернет Вещи. Каждая Интернет Вещь при инициализации к дереву ресурсов сервиса IoTDM отправляет запрос, который так же содержит информацию о готовности датчиков, при их корректном подключении. Информация с GPS датчика приходит единожды.

3. Генерация трафика Интерна Вещей. В процессе работы, каждая Интернет Вещь посылает запросы каждую секунду (*Contant Instance*, по спецификации oneM2M) к дереву ресурсов, содержащие данные датчиков, время их регистрации, номер значения и другие метаданные. Также была организована передача с каждого перекрестка последовательно каждой Интернет Вещью, при этом запросы к дереву ресурсов (сервис IoTDM) производились одновременно от каждого перекреста. В результате получилась модель, содержащая 960 Интернет Вещей, при этом одновременно работало с сервисом 240 Интернет Вещей.

Для построения дерева ресурсов был разработан соответствующий скрипт. Также для генерации трафика был разработан генератор трафика Интернета Вещей с учетом спецификации oneM2M и построенной архитектуры модели района «Умного города», на основе протокола HTTP, отправляющий запросы, содержащие в теле сообщения формата JSON. Генератор трафика Интернет Вещей был разработан на основе языка Python и API IoTDM.

Дерево ресурсов, которое получилось в результате построения, отображено на рис. 1.

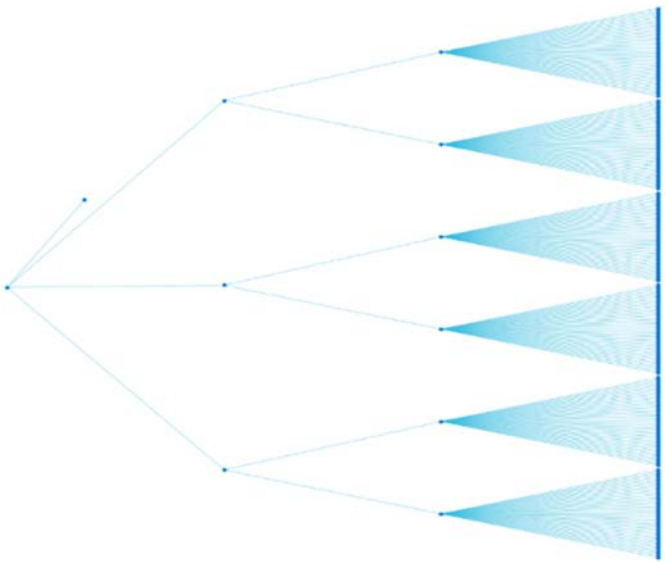


Рис. 1. Дерево ресурсов IoTDM

Множество конечных точек дерева на рис. 1, отображают все моделируемые перекрестки, при чем на каждом перекресте имеются 4 Интернет Вещи, которые не отображены на рис. 1, с целью корректного отображения масштаба дерева. В ходе эксперимента мы рассчитали параметр RTT (*Round Trip Time*) и задержку передачи пакетов IoT трафика в сети для протокола HTTP. Распределение значения RTT отображено на рис. 2.

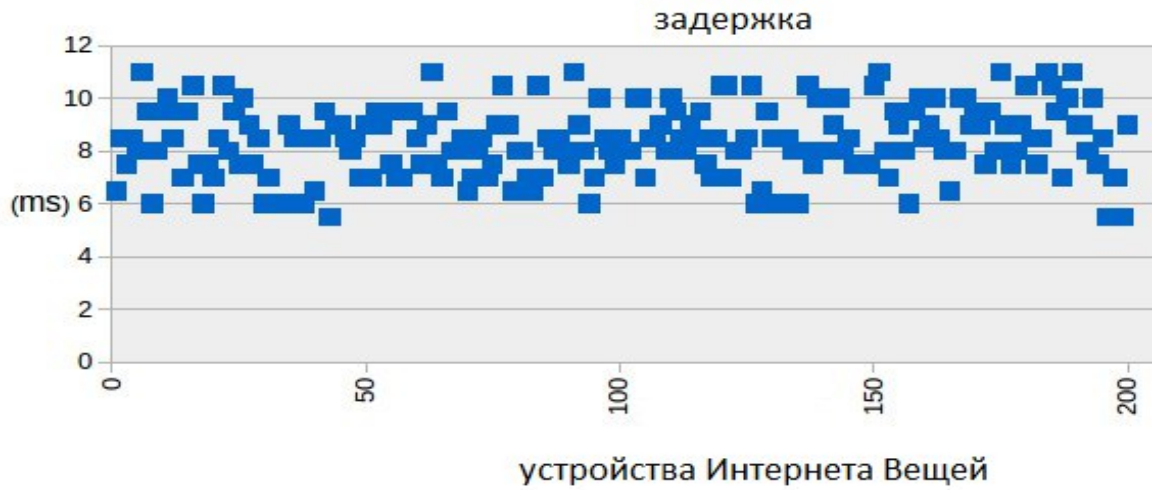


Рис. 2. Значение RTT протокола HTTP

Значения задержки пакетов IoT трафика в сети отображены на рис. 3.

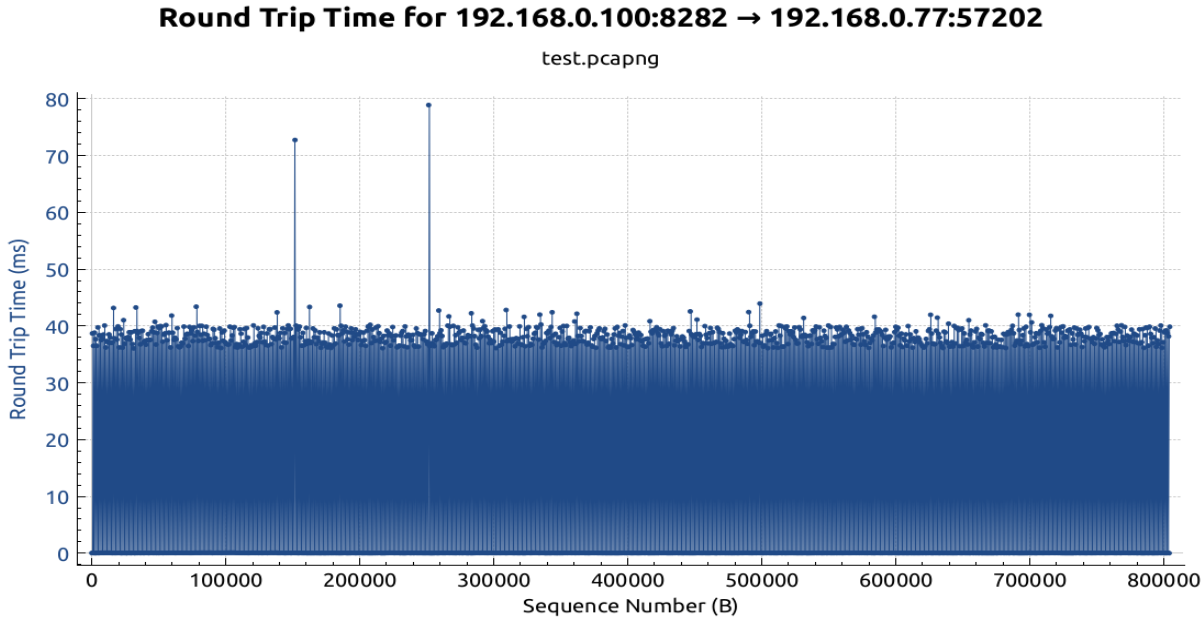


Рис. 3. Распределение задержки в сети в ходе эксперимента

Полученный результат значения RTT сравнили с ранее опубликованными данными из работы [7]. В итоге получили в несколько раз меньшее значение параметра RTT, что наглядно видно на рис. 3. Данный результат показывает эффективность использования сети SDN в условиях IoT трафика «Умного города», чем сетей классического типа.

Учитывая разнородность сетей ИВ, координация и оптимизация ресурсов в этих сетях является довольно сложной и трудоемкой задачей. Предполагается, что концепция SDN будет хорошим решением для удовлетворения потребностей в управлении ресурсами среды ИВ.

Заключение

Экспоненциальный рост устройств, подключенных к Интернету и управление сетью, в последнее время, стали одной из самых сложных задач. После возникновения технологии Интернета вещей (ИВ), объем трафика современных сетей будет увеличиваться. Подход программно-конфигурируемых сетей позволяют значительно автоматизировать и облегчить управление сетями за счёт возможности их программирования. В этой работе рассмотрено преимущество SDN для улучшения архитектур ИВ, где для системы менеджмента IoTDM как сервиса для «Умного города», был проведен натурный эксперимент на разработанной модели, которая в свою очередь отражала возможную схему распределения определенной системы мониторинга и управления для Центрального района Санкт-Петербурга. В результате получили в несколько раз меньшее значение параметра RTT. Данный результат показывает эффективность использования сети SDN в условиях IoT трафика «Умного города», чем сетей классического типа.

Список используемых источников

1. Naphade M. et al. Smarter Cities and Their Innovation Challenges // Computer. 2011. Vol. 44, No. 6. PP. 32–39.

2. Bowerman B., Braverman J., Taylor J., Todosow H., and U. Von Wimmersperg. The vision of a smart city // In 2nd International Life Extension Technology Workshop, Paris, volume 28, 2000.

3. Andrea Zanella, Nicola Bui, Angelo Castellani, Lorenzo Vangelista, and Michele Zorzi. Internet of things for smart cities // Internet of Things Journal, IEEE, 1 (1):22–32, 2014.

4. Radek Fujdiak, Pavel Masek, Petr Mlynek, Jiri Misurec, Ammar Muthanna: Advanced optimization method for improving the urban traffic management // FRUCT 2016: 48-53.

5. Jaeseok Yun. Interoperability between IoT Platforms // Workshop on the Future of IoT Standard Technology, Dec. 2015.

6. Vladyko A., Muthanna A., Kirichek R. Comprehensive sdn testing based on model network // Lecture notes in computer science. 2016. PP. 539–549.

7 Долгушев Р. А., Киричек Р. В., Кучерявый А. Е. Обзор возможных видов и методов тестирования Интернет вещей // Информационные технологии и телекоммуникации. 2016. Том 4. No 2. С. 1–11.

УДК 004.056.53

КАНАЛ УТЕЧКИ АКУСТИЧЕСКОЙ РЕЧЕВОЙ ИНФОРМАЦИИ, ВОЗНИКАЮЩИЙ ПРИ ЕЕ СОПУТСТВУЮЩЕЙ ПЕРЕДАЧЕ ПО ВОЛОКОННО-ОПТИЧЕСКИМ ЛИНИЯМ СВЯЗИ

И. А. Волков, С. А. Иванов

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

Волоконно-оптические линии связи становятся все более распространенными, а методы перехвата информации, по данному каналу связи, постоянно совершенствуются, поэтому необходимо постоянно улучшать методы и средства защиты информации от утечки по техническим каналам связи.

каналы утечки информации, защита акустической информации, волоконно-оптические линии связи.

Современные технологии волоконно-оптических линий связи имеют необходимые технические параметры для построения высокоскоростных и надежных информационных систем. В связи с этим в настоящие время происходит переход в информационных коммуникациях с электронных на волоконно-оптические технологии [1]. Поэтому волоконно-оптические линии связи становятся все более распространенными. Использование волоконно-оптических элементов в технических и выделенных помещениях, в которых находиться персонал, владеющий конфиденциальной информацией, создает новую угрозу информационно безопасности – несанкционированный съем акустической речевой информации при сопутствующей передачи по волоконно-оптическим линиям связи.

Согласно [2, 3] персонал, владеющий конфиденциальной информацией, является источником акустических волн. Акустическая волна, распространяясь в воздухе воздействует на волоконно-оптические элементы, находящиеся в технических и выделенных помещениях, модулируется на оптический несущий сигнал. Модулированный сигнал передается за пределы контролируемой зоны, где перехватывается злоумышленником при помощи устройства съема акустической речевой информации и дальнейшей его демодуляцией в восстановленный акустический сигнал. Схема съема акустической речевой информации при ее сопутствующей передаче по волоконно-оптической линии связи показана на рис. 1.

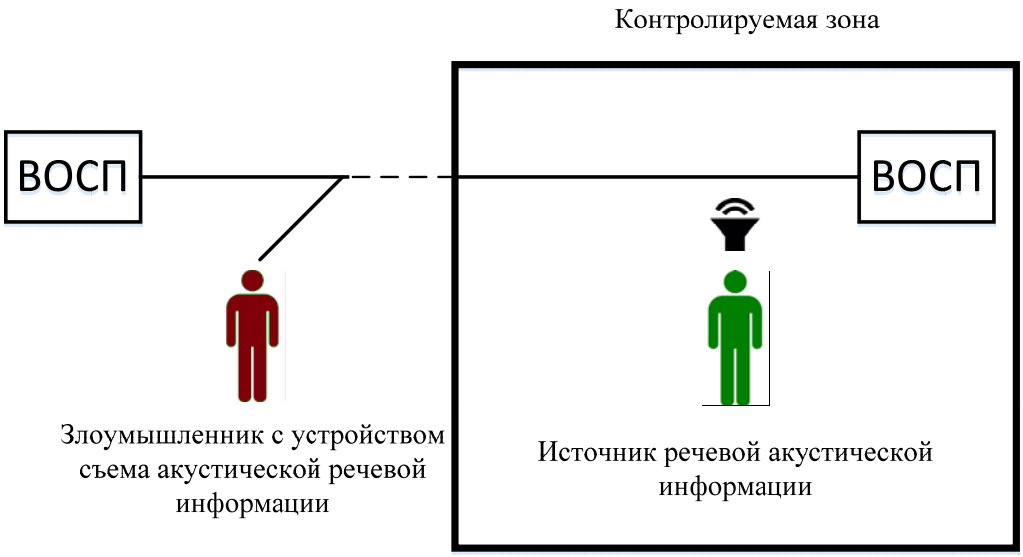


Рис. 1. Схема съема акустической речевой информации при ее сопутствующей передаче по волоконно-оптической линии связи

Физика процесса

Имеющиеся в волоконно-оптическом кабеле примеси и оптические неоднородности среды распространения, образуют границу раздела двух сред, для распространяющегося в нем оптического сигнала. Согласно [4] Акустическая речевая информация, падающая на границу раздела двух сред, вызывает отклонение поверхности от состояния покоя, происходит изменение оптической длины пути света отразившегося от колеблющейся поверхности, что приводит к изменению фазы световой волны. Величина модуляции, как правило, пропорциональна длине акустического взаимодействия и звуковому давлению. Использование данных эффектов и позволяет применять ВОЛС, как приемника акустических сигналов. Схема модуляции акустического сигнала на оптический сигнал показана на рис. 2.

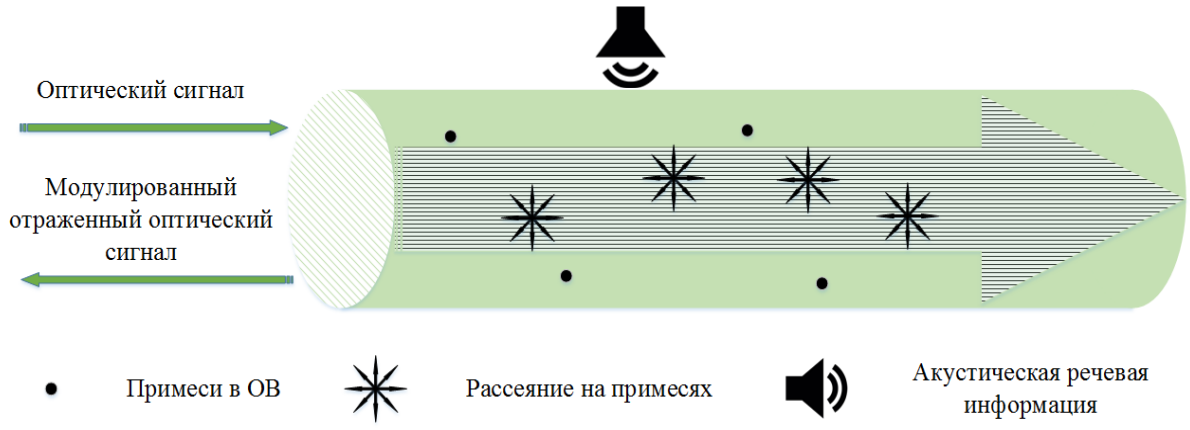


Рис. 2. Схема модуляции акустического сигнала на оптический сигнал

Основными каналами утечки являются световые потоки в оптическом кабеле линий связи. Каналы можно разделить на три типа:

– *контакты и соединения оптического волокна*. При воздействии акустической речевой информации на соединения волоконно-оптических элементов, необходимых для механического соединение оптических волокон, создает колебания, модулирующие оптический сигнал.

– *участки волоконно-оптического кабеля*. Оптоволокно обладает высокой чувствительностью к механическим воздействиям, даже небольшие колебания вызывают изменение условий прохождения света;

– *места крепления волоконно-оптического кабеля к элементам несущих конструкций здания*. Акустическая речевая информация передается на участки оптоволоконного кабеля через крепления оптического шнура с конструкцией здания, где в дальнейшем модулируется на несущий световой поток.

Обеспечить функционирование акусто-оптоволоконного канала утечки возможно при условиях, когда световой поток или уже существует, или специально создаётся в кабельной сети. Реализация каждого из способов зависит от режима работы активного оборудования и может быть разделена на два вида по состоянию сетевого оборудования.

1. Режим активного состояния сетевого оборудования, когда используются потоки оптического сигнала в волоконно-оптическом канале для переноса речевой информации. Формирование канала утечки возможно путём модуляции на звуковой частоте интенсивности света части трафика и последующим проведением акустической демодуляции за пределами систем защиты.

2. Режим пассивного состояния сетевого оборудования. При отключённом оборудовании возможно временное подключение внешнего источника света из незащищённых помещений, чтобы активировать канал утечки и по отраженному излучению произвести съём информации [5].

В связи с высокой вероятностью возникновения рассматриваемого канала утечки конфиденциальной акустической речевой информации при ее сопутствующей передаче по волоконно-оптическим линиям связи, требуется создание и внедрение новых средств защиты информации, направленных на уменьшение величины разборчивости речи. Так же необходимо учитывать данный канал утечки информации при проектировании сетей в контролируемой зоне и избегать прокладку волоконно-оптических элементов через выделенные помещения.

Список используемых источников

1. Семенов А. Б. Волоконно-оптические подсистемы современных СКС. М. : Академия АйТи: ДМКПресс, 2007. 632 с.

2. Гришачев В. В., Халяпин Д. Б., Шевченко Н. А. Опасности возникновения каналов утечки конфиденциальной речевой информации по волоконно-оптическим структурированным кабельным системам // Материалы X Международной научно-практической конференции «Информационная безопасность». Ч. 2. Таганрог : Изд-во ТТИЮФУ, 2008. С. 103–105.

3. Халяпин Д. Б. Защита информации. Вас подслушивают? Защищайтесь. М. : НОУ ШО «БАЯРД», 2004.

4. Яковлев А. В. Волоконно-оптическая система передачи конфиденциальной информации // Электросвязь. 1994. № 10.

5. Свинцов А. Г. Оптимизация параметров оптического рефлектометра для обнаружения неоднородности при попытке несанкционированного доступа в ВОСП // Фотон-Экспресс. 2006. № 6. С. 56–71.

УДК 004.056.53

ПРОБЛЕМА КРИПТОЗАЩИТЫ В УСТРОЙСТВАХ CISCO ПРИ ИСПОЛЬЗОВАНИИ АКТУАЛЬНЫХ ПРОШИВОК

В. Н. Волкогонов, В. С. Голубев, И. А. Ушаков

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

В данной статье рассматривается проблема шифрования данных на устройствах компании Cisco при использовании ключей шифрования с длиной ключа, предлагаемой по умолчанию.

В ходе работы будет рассмотрен популярный способ построения виртуальных частных сетей, а также определен нижний порог криптозащиты, при котором можно будет сказать, что сеть устойчива к атаке «человек посередине».

криптография, информационная безопасность, цифровой сертификат, открытый ключ, закрытый ключ, анализ трафика.

Объемы передаваемой по сети информации возрастают с каждым годом, так же не стоит на месте и развитие технологий виртуальных частных сетей [1]. Это, и тот факт, что 29 января 2017 г. стало известно, что доля HTTPS трафика в интернете превысила 50 % [2], говорит о том, что с каждым годом доля зашифрованного трафика только растет. Самый популярный способ организации VPN соединения – использовать стек протоколов IPsec [1]. Также на данный момент, подавляющее большинство сайтов, которые собирают, обрабатывают и передают пользовательскую информа-

цию, работают по протоколу https, что обеспечивает пользователям конфиденциальность и целостность передаваемой информации. Как в случае использования стека протоколов IPsec, так и протокола https может быть использован цифровой сертификат [1], в первом случае в качестве механизма идентификации, во втором в качестве гаранта, что ресурсу можно доверять.

Цифровой сертификат – выпущенный удостоверяющим центром электронный документ, подтверждающий принадлежность владельцу или ресурсу открытого ключа или каких-либо атрибутов. В основу сертификата заложена криптосистема с открытым ключом, одна из самых популярных криптосистем – RSA [1]. Разложив модуль N на простые два множителя можно решить задачу факторизации и подобрать закрытый ключ.

Форматы сертификатов:

– PEM – файл закодированный в Base64 и имеющие определенную структуру – начинается с строки "----- BEGIN CERTIFICATE -----", а заканчиваются строкой "----- END CERTIFICATE -----";

– DER – это бинарная форма PEM формата.

При создании новой пары ключей для сертификата операционная система CISCO IOS по умолчанию предлагает сгенерировать ключи с длиной в 512 бит [3], что не является безопасным решением в наши дни. Наибольшая длина ключа, для которого на данный момент была решена задача факторизации – 768 бит.

В данной статье проводится исследование безопасности использования ключа длиной в 768 бит. В качестве основных инструментов для проведения эксперимента были использованы следующие компоненты:

– ОС Linux;

– WireShark – достаточно популярных инструмент для анализа и захвата сетевого трафика. Он предоставляет возможность работы с подавляющим большинством известных протоколов [4];

– Openssl – криптографический пакет имеющий открытый исходный код для работы с TLS/SSL. Он позволяет создавать и анализировать сертификаты X.509 [5].

– Python – динамически типизированный высокоуровневый язык программирования, с минималистическим синтаксисом [6].

Библиотеки для Python

– Python-RSA – библиотека для позволяющая создавать ключи шифрования, шифровать и расшифровывать данные, а так же создавать цифровые сертификаты.

Для исследования имеется дамп трафика, в котором клиент обменивается информацией с сервером зашифрованной при помощи протокола TLS с длиной ключа шифрования 768 бит. Имея дамп при помощи WireShark из-

влекаем из него цифровой сертификат полученный от сервера, он извлекается в формате DER, для его дальнейшего анализа в таком формате используется инструмент OpenSSL.

Для анализа сертификата можно пойти двумя путями:

1. Анализировать сертификат непосредственно в DER формате.

2. Конвертация сертификата из DER формата в PEM, и уже анализировать его.

Выберем второй вариант, так как сертификат в формате PEM можно открывать, экспортировать и использовать.

Для конвертации необходимо ввести команду:

openssl x509 *-in cert -inform DER -out cert.pem -outform PEM*

Где в качестве ключей выступают:

– *in* – указывает на файл полученный программой на вход;

– *inform* – формат входного файла;

– *out* – имя файла полученного на выходе работы программы;

– *outform* – формат выходного файла.

Получив сертификат, необходимо его прочитать, это можно сделать командой:

openssl x509 *-in cert.pem -text*

Ключ *-text* выведет всю информацию о сертификате, нас же пока интересует лишь модуль *N*, по этому можно ввести команду:

openssl x509 *-in cert.pem –modulus*

Которая выведет только модуль *N*.

В нашем случае модуль равен:

Modulus=CAD984557C97E039431A226AD727F0C6D43EF3D418469F1B375049B229843EE9F83B1F97738AC274F5F61F401F21F1913E4B64BB31B55A38D398C0DFED00B1392F0889711C44B359E7976C617FCC734F06E3E95C26476091B52F462E79413DB5

Модуль – это число, представленное в 16-ой системе счисления, для дальнейшей работы нужно перевести его в 10 систему счисления, для этого можно использовать язык программирования Python. Переведя число в 10 систему счисления, надо разложить его на простые множители. Самый простой способ это сделать – воспользоваться базой данных с факторизованными числами, для этого можно обратиться к ресурсу [7].

Найдя коэффициенты p и q, можно написать программу на Python, с использованием библиотеки RSA, она позволяет создать сертификат открытого, закрытого ключей, а так же шифровать трафик. Воспользуемся возможностью создания сертификата закрытого ключа. Первым этапом необходимо описать расширенный алгоритм Евклида на языке программирования Python, он будет использоваться в функции вычисления обратного

числа. Эта функция необходима для вычисления секретного числа d, обратное к числу e по модулю $\varphi(n)$:

```
    def modinv(a, m):
        g, x, y = egcd(a, m)
        if g != 1:
            raise Exception('modular inverse does not
exist')
        else:
            return x % m

    def GCD(a, b):
       while b:
         a, b = b, a % b
       return a
```

При помощи библиотеки RSA собираем закрытый сертификат, сохраняем его и записываем его в файл.

```
priv_key = rsa.PrivateKey(N, e, d, p, q)
priv_key = priv_key.save_pkcs1(format='PEM')
f = open('private_b.pem', 'wb')
f.write(priv_key)
f.close()
```

WireShark умеет не только перехватывать траффик и выводить о нем информацию, но и анализировать его. В частности, он может расшифровать все пакеты, зашифрованные при помощи протокола TLS/SSL. Для этого необходимо взять сконфигурированный ранее сертификат закрытого ключа и в настройках программы указать с какого сервера необходимо расшифровывать траффик при помощи этого ключа.

Проанализируем полученный дамп (рис. 1) с исходным (рис. 2), в обоих случаях имеется 23-й пакет, указывающий на финишный этап в установлении соединения между источниками. В исходном дампе пакеты 24 и 25 находятся в зашифрованном виде. В полученном же дампе видно, что клиент отправляет на сервер GET запрос и получает на него ответ.

```
22 192.168.100.4 192.168.100.2 TLSv1   125 Change Cipher Spec, Finished
23 192.168.100.2 192.168.100.4 TCP      66 51695 → 443 [ACK] Seq=327 Ack=906 Win=524280 Len=0 TSval=890011170 TSecr=2106153
24 192.168.100.2 192.168.100.4 HTTP    471 GET /index.html HTTP/1.1
25 192.168.100.4 192.168.100.2 TLSv1   668 HTTP/1.1 200 OK , Application Data
26 192.168.100.2 192.168.100.4 TCP      66 51695 → 443 [ACK] Seq=732 Ack=1508 Win=524280 Len=0 TSval=890011170 TSecr=2106153
```

Рис. 1. Расшифрованные пакеты

```
22 192.168.100.4 192.168.100.2 TLSv1   125 Change Cipher Spec, Encrypted Handshake Message
23 192.168.100.2 192.168.100.4 TCP      66 51695→443 [ACK] Seq=327 Ack=906 Win=524280 Len=0 TSval=890011170 TSecr=2106153
24 192.168.100.2 192.168.100.4 TLSv1   471 Application Data
25 192.168.100.4 192.168.100.2 TLSv1   668 Application Data, Application Data
26 192.168.100.2 192.168.100.4 TCP      66 51695→443 [ACK] Seq=732 Ack=1508 Win=524280 Len=0 TSval=890011170 TSecr=2106153
```

Рис. 2. Зашифрованные данные

В ходе проделанной работы была продемонстрированная уязвимость сетей при использовании ключей шифрования с длиной ключа 768 бит. Данное исследование может лечь в основу образовательной методики при изучении построения защищенных локально-вычислительных сетей.

Список используемых источников

1. Коржик В. И., Просихин В. П., Яковлев В. А. Основы криптографии, СПбГУТ. СПб., 2014. 276 с.

2. Новостной портал Хабрахабр. URL: https://habrahabr.ru/post/321002/ (дата обращения 14.01.2017).

3. Официальный сайт компании Cisco. URL: http://www.cisco.com/ (дата обращения 14.01.2017).

4. Пользовательское руководство по WireShark. URL: https://www.wireshark.org/docs/wsug_html_chunked/ (дата обращения 14.01.2017).

5. 5Официальный сайт криптографического пакета с открытым исходным кодом OpenSSL. URL: https://www.openssl.org/ (дата обращения 14.01.2017).

6. Официальный сайт языка программирования Python. URL: https://www.python.org/ (дата обращения 14.01.2017).

7. Сайт с базой данных факторизованных модулей. URL: http://factordb.com/ (дата обращения 14.01.2017).

УДК 004.771

АНАЛИЗ ОСОБЕННОСТЕЙ УПРАВЛЕНИЯ ТРАФИКОМ В SDN

А. И. Ворожбитова, В. С. Елагин

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

В данном докладе рассматриваются особенности управления трафиком в программно-конфигурируемых сетях Software Defined Network. Управление происходит при помощи протокола OpenFlow через таблицы, характеризующие потоки (flow table, group table, meter table). Для их конфигурирования используются сообщения, которые бывают нескольких типов в зависимости от инициатора (контроллер или коммутатор). Произведен анализ сообщений, как с их помощью можно изменить таблицы в коммутаторах с целью управления трафиком.

SDN, OpenFlow, flow table, OpenFlow message, traffic control.

Традиционная архитектура сетей изначально не подразумевала нынешние объемы трафика, в связи с чем ее администрирование на данный момент стало очень сложным. Чтобы решить эту, а также ряд других проблем, связанных с традиционными сетями, в 2006 г. появился концепт нового подхода к архитектуре, а после начал активно внедряться в некоторые ведущие компании и получил название SDN – Software-Defined Network. Главная идея этого подхода – разделение плоскости управления и плоскости передачи данных за счет переноса функций управления на контроллер – некий сервер, а коммутаторам остается только следовать его указаниям [1, 2, 3, 4].

SDN реализуется протоколом OpenFlow, который обеспечивает взаимодействие контроллера с сетевым оборудованием. Именно благодаря протоколу OpenFlow и контроллеру, вся сеть, которая состоит из оборудования разных поставщиков, предстает для приложения управления сетью в виде одного логического коммутатора.

Протокол OpenFlow поддерживает три типа сообщений, а именно: контроллер-коммутатор, асинхронные и симметричные, у каждого из которых есть несколько подтипов. Назначение каждого из типов представлено в таблице 1.

ТАБЛИЦА 1. Типы сообщений

название	инициатор	назначение
контроллер-коммутатор	контроллер	управление, слежение за состоянием коммутатора, установка параметров, сбор статистики, модификация записей в flow table
асинхронные	коммутатор	оповещение контроллера о сетевых событиях (прибытие пакета, удаление записи из таблицы по истечению тайм-аута), об изменении состояния коммутатора или ошибках
симметричные	коммутатор или контроллер	установление соединения, измерение задержек, пропускной способности, проверка «живучести» соединения

Как можно увидеть из названия – при идентификации трафика ключевым понятием является «поток». Идея OpenFlow такова, что, несмотря на различия между оборудованием разных вендоров, у них имеется общая черта – они все содержат таблицу передачи данных. Эта таблица, в свою очередь, определяет базовую функцию передачи данных – каждый поступивший пакет как можно быстрее переправить на нужный интерфейс. И хоть формат этих таблиц различен, можно выделить сходства. Таким образом, основным элементом коммутатора, который поддерживает протокол OpenFlow, является таблица потоков Flow Table.

В таблице 2 указаны поля соответствий, по которым сравнивается входящий поток. Каждая запись содержит определенное значение, или ANY, что означает любое значение. Если коммутатор поддерживает произвольные битовые маски Ethernet полей источника и/или получателя, IP полей источника и/или получателя, эти маски могут более точно указать соответствия.

ТАБЛИЦА 2. Поля соответствий

Ingress Port	Metadata	Ether src	Ether dst	Ether type	VLAN id	VLAN priority	MPLS label	MPLS traffic data	IPv4 src	IPv4 dst	IPv4 proto/ARP opcode	IPv4 ToS bits	TCP/UDP/SCTP src port ICMP type	TCP/UDP/SCTP dst port ICMP type

Таким образом, одним их самых важных сообщений, передаваемых между контроллером и коммутатором, является FlowMod, которое позволяет контроллеру изменять состояния на OpenFlow коммутаторе. На рисунке, представлена структура этого сообщения.

В поле command (*cmd*) указывается, какое действие необходимо предпринять над потоком:

– OFPFC_ADD, создать новый поток;

– OFPFC_MODIFY, модифицировать все подходящие потоки;

– OFPFC_MODIFY_STRICT, модифицировать строго подходящие по шаблону потоки;

– OFPFC_DELETE, удалить все подходящие потоки;

– OFPFC_DELETE_STRICT, удалить строго подходящий по шаблону и приоритету потоки.

В поле flags указываются соответствующие флаги, которые уточняют необходимое действие:

Рисунок. Структура сообщения FlowMod

– SendFlowRem;
– CheckOverlap;
– ResetCounts;
– NoPacketCounts;
– NoByteCounts.

Для добавления новой записи, вся необходимая для него информация будет содержаться в полях match и instructions.

Это один из примеров, как происходит управление трафиком и поступающими потоками в протоколе OpenFlow. Помимо сообщения FlowMod, существуют сообщения GroupMod, TableMod и PortMod, которые также помогают вносить какие-либо изменения в работу коммутатора.

Список используемых источников

1. OpenFlow Specification 1.3. Open Networking Foundation. 2011.
2. Ворожбитова А. И. Выпускная квалификационная работа на тему «Анализ возможностей протокола Openflow в рамках Программно-конфигурируемых сетей (ПКС)». 2015 г.
3. Елагин В. С., Онуфриенко А. В. Технология глубокой инспекции пакетов в программно-конфигурируемой сети // Труды учебных заведений связи. 2016. Т. 2. № 2. С. 59–63.
4. Елагин В. С., Зобнин А. А. Аспекты реализации системы законного перехвата трафика в сетях SDN // Вестник связи. 2016. № 12. С. 11–14.

– SendFlowRem;
– CheckOverlap;
– ResetCounts;
– NoPacketCounts;
– NoByteCounts.

Для добавления новой записи, вся необходимая для него информация будет содержаться в полях match и instructions.

Это один из примеров, как происходит управление трафиком и поступающими потоками в протоколе OpenFlow. Помимо сообщения FlowMod, существуют сообщения GroupMod, TableMod и PortMod, которые также помогают вносить какие-либо изменения в работу коммутатора.

Список используемых источников

1. OpenFlow Specification 1.3. Open Networking Foundation. 2011.
2. Ворожбитова А. И. Выпускная квалификационная работа на тему «Анализ возможностей протокола Openflow в рамках Программно-конфигурируемых сетей (ПКС)». 2015 г.
3. Елагин В. С., Онуфриенко А. В. Технология глубокой инспекции пакетов в программно-конфигурируемой сети // Труды учебных заведений связи. 2016. Т. 2. № 2. С. 59–63.
4. Елагин В. С., Зобнин А. А. Аспекты реализации системы законного перехвата трафика в сетях SDN // Вестник связи. 2016. № 12. С. 11–14.

УДК 004.7

ВНЕДРЕНИЕ МЕХАНИЗМОВ ПРИОРИТИЗАЦИИ ПАКЕТНОГО ТРАФИКА В СЕТЯХ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

В. А. Воронцов, Д. Д. Корякин

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

Сети военного назначения обладают сложной структурой. Они включают в себя различные «конкурирующие» объекты – от сигналов, распоряжений до приказаний, команд. Пакеты информации в центрах коммутации разбиваются на приоритетные и не приоритетные по трафику. Обработка пакетов каждой очереди организуется по алгоритму обработки маршрутного процессора, и основной ресурс направляется на более приоритетную очередь. Из-за специфики организации сетей связи военного назначения возникает необходимость решать задачи с определением приоритетов

в множестве альтернатив в целях выбора предпочтительного варианта. Поэтому требуются приоритетные модели с учётом важности, скорости, объёмов передаваемой информации, класса каждого отдельного приоритетного потока, а также времени прибытия пакета в очередь.

приоритизация трафика, QOS, TOS.

Своевременность информационных обменов в структуре абонентов сетей связи военного назначения – актуальная и достаточно сложная задача, учитывая потенциальную опасность воздействия на цифровые системы связи специального назначения со стороны противника. В современном мире успешность выполнения задач в мирное и военное время находится в прямой зависимости от используемых средств телекоммуникации, которые применяются в процессе организации взаимодействия командиров и подчинённых.

Технологии стремительно развиваются, что позволяет повышать производительность сетей и расширять спектр интегральных услуг для пользователей. Число пользователей растёт, возникают новые приложения и разновидности типов трафиков в пределах одной мультисервисной сети. Но при этом производительность центров коммутации снижается, в результате чего может теряться полезная информация. Поэтому возникает необходимость реализации механизмов приоритизации пакетного трафика. Сети военного назначения обладают сложной структурой. Они включают в себя различные «конкурирующие» объекты – от сигналов, распоряжений до приказаний, команд. Пакеты информации в центрах коммутации разбиваются на приоритетные и не приоритетные по трафику. Обработка пакетов каждой очереди организуется по алгоритму обработки маршрутного процессора, и основной ресурс направляется на более приоритетную очередь. Из-за специфики организации сетей связи военного назначения возникает необходимость решать задачи с определением приоритетов в множестве альтернатив в целях выбора предпочтительного варианта. Поэтому требуются приоритетные модели с учётом важности, скорости, объёмов передаваемой информации, класса каждого отдельного приоритетного потока, а также времени прибытия пакета в очередь.

Создание сети, гарантированно пропускающей весь исходящий трафик при условии активной сетевой работы всех имеющихся пользователей, – задача практически нереальная. Дело в том, что у параметров пропускной способности есть некие усреднённые показатели, учитывая и предположения о характере использования сети (от типов задач, наличия голосового и мультимедийного трафика и др.). По данным параметрам и производятся расчёты. Большинство сетей у малых и средних предприятий имеет пропускную способность, которая используется гораздо меньше, чем на 100 %,

поэтому маловероятны ограничения передачи данных по причине исчерпания «полосы пропускания». Но в случае увеличения интенсивности применения сетевых приложений вероятность кратковременных перегрузок сети сразу повышается, что прямо влияет на всю работу с доставкой информации. В том случае, если пакет, содержащий данные, не передаётся, он может быть удалён и потерян. В большинстве случаев приложения корректно обработают факты с потерей части передаваемых данных и запросят их вторично. Но, с другой стороны, существуют задачи, для которых потеря пакетов является недопустимой. Проблему можно решить с помощью предоставления информации привилегированных условий. Тогда и встаёт вопрос о приоритизации трафика.

Для приоритизации трафика передаваемым по сети пакетам присваиваются определённые классы обслуживания/обеспечения. Такие технологии называют QoS – Quality of Service. Они по-разному внедряются в локальных и магистральных сетях. На уровне кадров Ethernet (второй уровень модели OSI) существует возможность включения поля TAG, значение которого определяет требуемый уровень обслуживания. Поскольку протокол IP работает не только в сетях Ethernet, но и в сетях WAN, которые не обязательно основаны на кадре Ethernet, то и в IP-пакете было предусмотрено специальное поле ToS (*Type of Service* – тип обслуживания), принимающее данные о требуемом уровне обслуживания. Впоследствии был разработан новый протокол Differtiated Services (DS или *DiffServ*), который и используется в настоящее время для маркировки IP-пакетов в соответствии с уровнем обслуживания [1]. Коммутаторы, используемые на малых и средних предприятиях, а также коммутаторы уровня доступа в больших сетях обычно используются для приоритизации только поле QoS Ethernet-кадра. Коммутаторы уровня предприятия могут приоритизировать трафик с учётом всех действующих стандартов [2].

Для настройки приоритизации трафика (рис.) создаются правила, позволяющие выделять часть трафика, которая требует при её передаче особых условий. Данный процесс называют классификацией, в ходе которого каждый пакет оказывается промаркированным. Когда выполнена классификация трафика, нужно начать процесс применения правил приоритизации. Стандарт включает восемь уровней приоритета, и к каждому из них существуют только общие рекомендации. А правила приоритизации формируются самостоятельно. Для приоритизированной передачи пакетов на коммутаторе создаются буферы для временного хранения пакетов на каждом порте. Это и есть очередь. Количество буферов соответствует количеству очередей, поддерживаемых коммутатором (по числу уровней приоритизации их должно быть восемь). Меньшее количество не позволит использовать все возможности протокола. Обычно размеры буфера не являются одинаковыми для разных очередей, потому что чем выше приоритет очереди,

тем больше памяти предназначается для хранения её пакетов. Затем трафик маркируется и если канал связи свободен, то пакет сразу передаётся по назначению, если занят – коммутатор помещает данный пакет в очередь на временное хранение. Очередь определяется по заданным правилам. Линия связи освобождается, и коммутатор начинает передавать пакеты из очередей. Существует несколько алгоритмов для передачи таких данных с настраиваемыми параметрами: Strict Priority Queuing (SPQ) и Weighted Round Robin (WRR).

Рисунок. Процесс приоритизации трафика

Суть каждого алгоритма заключается в том, что происходит обработка информационных пакетов с функцией предпочтения для рассматриваемого класса объектов на основе использования принципа их идентификации. Каждый вид сравниваемых объектов получает единую количественную характеристику, которая используется как основа для упорядочивания объектов. Это зависит от распределения ресурсов центра коммутации военного назначения по его приоритетам, а также классам и временным показателям. Данный метод позволяет усовершенствовать используемые алгоритмы обработки пакетных трафиков в центрах коммутации военных сетей связи и снижать процент потерь пакетов с высоким весом приоритета абонентов.

Список используемых источников

1. Битнер В. И., Попов Г. Н. Нормирование качества телекоммуникационных услуг: учебное пособие / под ред. профессора В. П. Шувалова. М. : Горячая линия – Телеком, 2004. 312 с.

2. ITU-T E.800. Telephone network and ISDN quality of service, network management and traffic engineering. Terms and definitions related to quality of service and network performance including dependability. 08/94 sector.

Статья представлена сотрудником НИЦ ВАС, кандидатом технических наук, доцентом Д. О. Федосеевым.

УДК 004.72

ТЕХНИЧЕСКИЕ АСПЕКТЫ РЕАЛИЗАЦИИ DPI НА СЕТЯХ SDN

С. А. Высоцкий, В. С. Елагин, В. А. Пряжников

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

В данной статье описываются сети SDN. Ввиду недостаточного развития сети отсутствуют многие услуги на данной сети. В статье описывается возможность применения технологии DPI для расширения функционала сети.

программно-конфигурируемые сети, трафик, глубокий анализ пакетов.

За последние несколько лет такая технология, как DPI (*Deep Packet Inspection*) стала очень востребованной среди операторов. Помимо основных функций технологии, таких как управление политикой доступа к сети и анализ данных, постоянно появляются новые варианты ее использования. Главное причина развертывания DPI и связанных с ним методик – необходимость среди операторов связи получать более точные данные об использовании трафика, поведении пользователей. На основе полученной информации предпринимаются действия для повышения производительности сети, более рационального использования полосы пропускания, контроля за нагрузкой на сети и повышения качества восприятия (*Quality of Experience*, QoE). DPI позволяет операторам полностью вернуть контроль над сетью благодаря точной идентификации сторонних приложений в режиме реального времени.

Новое, стремительно развивающиеся направление в архитектуре сетей – программно-конфигурируемые сети (*Software Defined Network*, SDN). Суть SDN состоит в отделении «плоскости управления» от «плоскости передачи данных», централизации управления и программирования сети, изменении архитектуры сети в целом [1, 2].

Традиционная сеть IP (рис. 1) представляет собой набор функциональных блоков, причем в каждом ее узле выполняется обработка достаточно больших пакетов данных. Такая архитектура сложна, далеко не оптимальна и неизбежно вносит существенные задержки. В крупных сетях это становится серьезной проблемой. В случае SDN при построении сети используется стандартное недорогое оборудование, а процедуры управления и необходимые в каждом сетевом узле сервисы реализуются с помощью ПО. Преимущества SDN заключаются в стандартных открытых API для сетевых приложений и возможности создания операторами собственного ПО

для управления сетью. Это делает сеть более «умной» с возможностью самоанализа и принятия решений о форвардинге трафика, исходя из требований приложений и загрузки сети в режиме реального времени [3, 4].

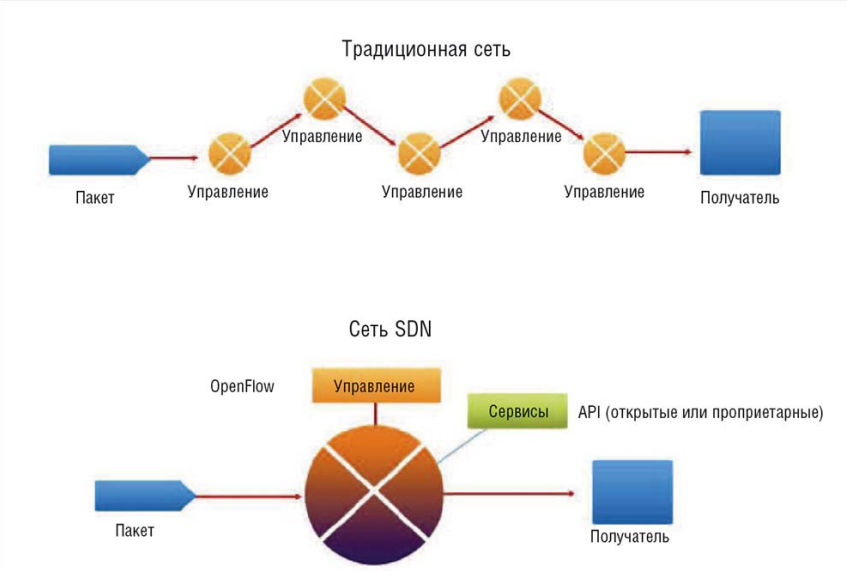


Рис. 1. Передача пакетов в традиционной сети и в сети SDN

Подход предоставляет и массу экономических выгод, включая сокращение затрат на оборудование. Т. к. «мозг» сетевого устройства вынесен на отдельное устройство, снижаются требования к функционалу сетевого оборудования, требуя от него лишь высокоскоростной обработки трафика и необходимого объема ресурсов для хранения записей потоков.

Благодаря максимальной автоматизации работы сети, снижаются и временные затраты на обслуживание инфраструктуры, позволяя инженерам сосредоточиться на разработке новых сервисов, сняв с себя множество рутинных задач.

Первичная архитектура SDN сосредоточена на L2-L4. В результате коммутаторы не могут различать трафик от приложений L7. Это приводит к неэффективному использованию полосы пропускания и вычислительных ресурсов. Например, медиа-серверу придется анализировать весь трафик, чтобы взять на обслуживание только соответствующие потоки данных, например, потоковое видео.

DPI на L4-L7 заполняет этот пробел, анализируя трафик и предоставляя информацию сетевого приложения и метаданные, необходимые для интеллектуальных систем принятия решений. Метаданные либо извлекаются из трафика, либо вычисляются, и затем используются для получения статистики или создания правил. Правила могут быть активными, то есть узел (например, коммутатор) принимает решение без участия контрол-

лера SDN (на основе предварительно настроенных политик), или возвратными, т. е. когда для решения проблемы контроллер вернет инструкции узлу.

Использование DPI широко распространено, а количество областей применения, в которых он используется постоянно растет. Тем не менее, основной функцией остается идентификация различных типов трафика в режиме реального времени, и связывание этой информации с другими данными, такими так абонент, устройство, местоположение и так далее.
Традиционным методом развертывания DPI является внедрение его в различные сетевые устройства, такие как пограничные контроллеры сессий (*Session Border Controller*, SBC), функцию обнаружения трафика (*Traffic Detection Function*, TDF), шлюзовой узел поддержки GPRS (*Gateway GPRS Support Node*, GGSN) и так далее. Главным недостатком такого подхода является высокая стоимость развертывания, связанная с внедрением DPI на многих различных устройствах в виде дополнительных опций. Кроме того, осуществить связь между приложениями будет достаточно трудно, ввиду того, что каждый вендор по-своему будет реализовать DPI и формируемый им результат. Например, один вендор определит трафик, как «Skype», другой же определить этот же трафик как «социальные сети».

В SDN данные проблемы достаточно легко решить переносом DPI со множества устройств на один сервер, сделав DPI одной общей функцией. Такой подход позволит снизить общие затраты на внедрение DPI в целом, поскольку он будет реализован на меньшем количестве оборудования, что, как следствие, вызовет снижение затрат на потребление энергии и экономии средств в будущем. Также, взаимодействие между функциями и приложениями, используемыми DPI, значительно упростится ввиду появления унифицированного формата данных, формируемых им.

DPI в SDN, в принципе, может быть интегрирован в сетевые устройства в качестве ПО, запущенного, например, на коммутаторах, или же может быть на управляющей уровне в контроллере, который является, в свою очередь, связующим между приложениями и коммутаторами (рис. 2). При подключении только к контроллеру DPI буду доступны только L2-L4, чего недостаточно для выполнения основных задач, поставленных перед DPI. Более продуктивным будет подключение DPI к коммутаторам. В таком случае появляется возможность полностью контролировать потоки трафика, с высокой точностью определять приложения, генерирующие эти потоки, следить за их источниками, а также, при необходимости, модифицировать отдельные пакеты или целые сессии.

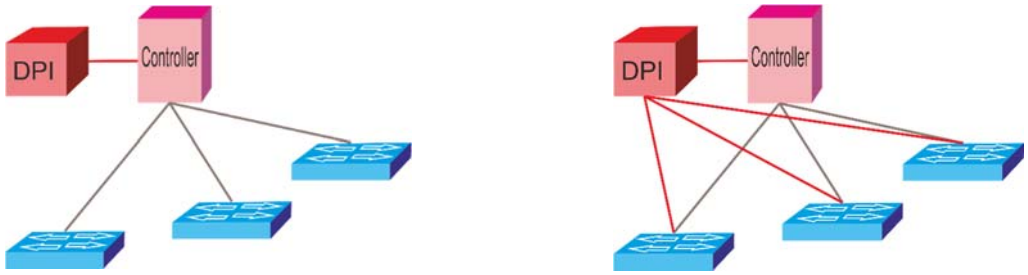


Рис. 2. Слева – установка DPI с подключением в контроллер,
справа – установка DPI в разрыв между контроллером и коммутаторами

Была развернута тестовая SDN зона с помощью эмулятора Mininet. Так же был написан скрипт на ЯП Python с применением библиотеки Scapy, реализующий функционал DPI. Данный скрипт реализовал удаление рекламных блоков с запрашиваемых HTML страниц по протоколу HTTP. В ходе его многократного тестирования было выявлено среднее время обработки запроса (между отправкой запроса и получением ответа) и среднее время выполнения скрипта.

На графике (рис. 3) видно, что основной объем HTTP пакетов обрабатывается в промежутке от 51 до 88 микросекунд. Среднее же время выполнения скрипта практически равно времени обработки пакетов. Это означает, что использование DPI на сети повлечет за собой появление, хоть и не значительных, но задержек.

Рис. 3. График времени
обработки пакетов HTTP

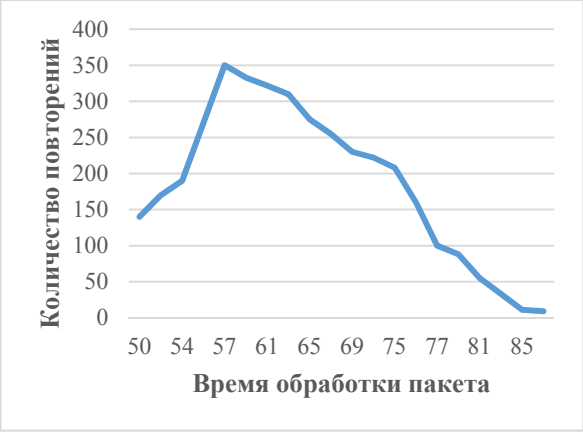


Рис. 4. График времени
обработки пакетов SIP

Для полноты картины дополнительно были проведены испытания с протоколом SIP (рис. 4) и получением полей To (адрес отправителя) и From (адрес получателя). Время обработки пакетов лежит в диапазоне от 50 до 90 микросекунд.

Основной пик в обоих случаях приходится на промежуток от 54 до 63 микросекунд. То есть можно с уверенностью сказать, что это и есть размер

задержки, вносимой DPI. Но не стоит забыть, что алгоритм работы данного DPI не является панацеей, вследствие чего данные задержки возможно уменьшить в разы.

В ходе данной статьи были освещены некоторые технические аспекты реализации DPI на сетях SDN, написан тестовый алгоритм глубокого исследования пакетов протоколов SIP и HTTP, выявлены задержки, вносимые работой данного алгоритма. В дальнейшей планируется оптимизация работы данного алгоритма для достижения лучших результатов.

Благодаря бурному развитию SDN уже не просто предмет исследований. Теперь это полностью работоспособное готовое решение для организации сети. Использование DPI позволяет реализовать новые функции, позволяющие в дальнейшем реализовывать новые сервисы и услуги, а также поможет оптимизировать расходы на построение и содержание сетей SDN.

Список используемых источников

1. Сетевые технологии SDN – Software Defined Networking. URL: https://habrahabr.ru/company/muk/blog/251959/ (дата обращения 30.04.2017).

2. Software-Defined Networking (SDN) Definition. URL: https://www.opennetworking.org/sdn-resources/sdn-definition (дата обращения 30.04.2017).

3. Высоцкий С. А., Матвеев П. С., Пряжников В. С., Сорокин В. А. Исследование систем для мониторинга и анализа сетевого трафика NTOPNG и NDPI // Студенческая весна – 2015. 69 региональная научно-техническая конференция студентов, аспирантов и молодых ученых: сб. науч. ст. 2015. С. 105–108.

4. Высоцкий С. А., Пряжников В. С., Сорокин В. А. Исследование возможности реализации и дальнейшего применения DPI на SDN сетях // Студенческая весна – 2016. 70-я региональная научно-техническая конференция студентов, аспирантов и молодых ученых: сб. науч. ст. С. 100–104.

УДК 621.39

ВЛИЯНИЕ ПОЛЯРИЗАЦИОННОЙ МОДОВОЙ ДИСПЕРСИИ НА ХАРАКТЕРИСТИКИ ОПТИЧЕСКОЙ СИСТЕМЫ С ВЯЗИ

С. А. Гагарина, А. С. Дюбов, Д. С. Микутавичайте

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

В статье рассмотрены физические процессы в оптических волокнах, приводящие к поляризационной модовой дисперсии. Показаны характерные искажения, вызываемые

PMD при распространении импульсов по оптическим волокнам. В статье приведены результаты моделирования работы волоконно-оптической системы передачи с учетом влиянием поляризационной модовой дисперсии.

поляризационная модовая дисперсия, оптическое волокно, волоконно-оптическая система связи.

Поляризационной модовой дисперсией (ПМД, *Polarisation Mode Dispersion*, PMD) называют изменение формы, огибающей цифрового оптического сигнала, обусловленное различием скоростей распространения двух взаимоперпендикулярных поляризационных составляющих моды [1, 2].

Причиной появления ПМД являются неизбежные случайные нарушения круговой симметрии волокна, имеющиеся многочисленные внутренние и внешние механические напряжения, приводящие к анизотропии и поляризационной зависимости показателя преломления. Существует множество причин возникновения анизотропии: неидеальность технологии изготовления волокна, воздействия на волокно в процессе производства кабеля, при его прокладке и монтаже. Как следствие множества неизбежных и случайных факторов существует различие в задержках ортогональных поляризаций распространяющегося по волокну оптического сигнала. Эту задержку называют дифференциальной групповой задержкой (ДГЗ, *Differential Group Delay*, DGD). В настоящее время уже разработаны эффективные методы компенсации затухания и хроматической дисперсии оптических волокон. Однако случайный характер природы возникновения ПМД усложняет разработку методов ее компенсации. Поляризационная модовая дисперсия становится одним из ограничивающих факторов, особенно для волоконно-оптических систем связи со скоростями в канале 40 Гбит/с и более. [3, 4]

Для оценки влияния ПМД на характеристики оптической системы связи рассмотрим искажений одиночного импульса по результатам моделирования в программе Optisystem. На рис. 1 приведена схема моделирования. При моделировании устранено влияние затухания и хроматической дисперсии, заданный коэффициент ПМД характерен для некоторых типов одномодовых волокон.

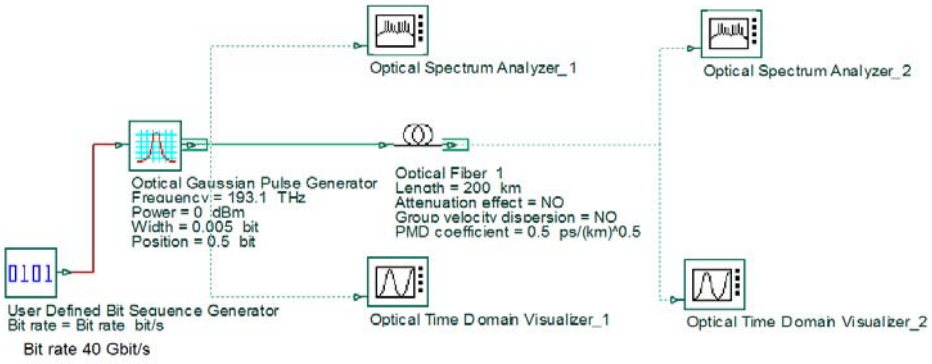


Рис. 1. Схема моделирования искажений одиночного импульса

На рис. 2 приведены формы импульсов после прохождения по волокну различной протяженности. Поляризационная модовая дисперсия проявляется подобно хроматической дисперсии, приводит к расширению оптических импульсов во временной области, следовательно, к ухудшению рабочих характеристик систем связи.

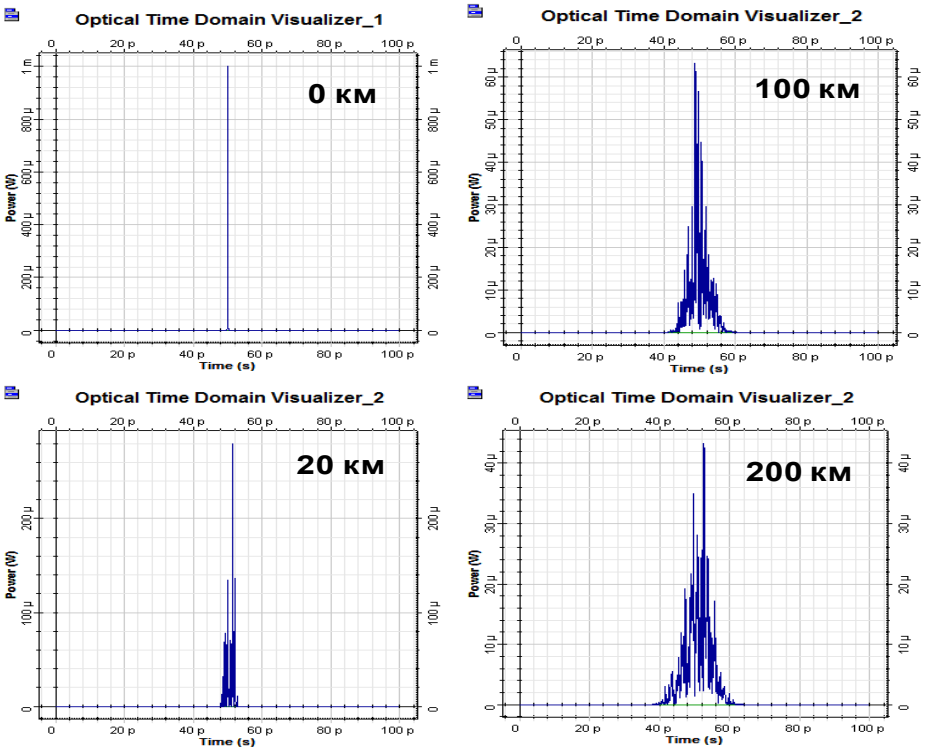


Рис. 2. Влияние ПМД на одиночный импульс

Для рассмотрения влияния ПМД на последовательность импульсов составим схему, приведенную на рис. 3. Аналогичная схема приведена в документации к программе и содержит компонент «PMD Emulator», реализующий математическую модель волокна с учетом ПМД первого и второго порядка [4].

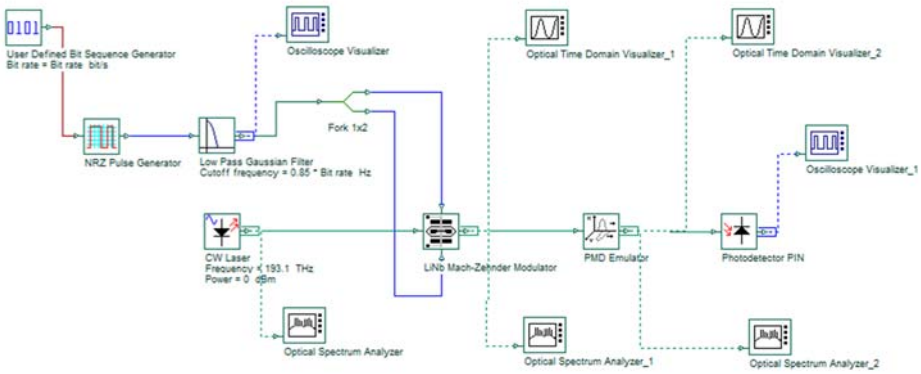


Рис. 3. Схема моделирования искажений последовательности импульсов

На рис. 4 представлены последовательности импульсов на входе и выходе компонента «PMD Emulator».

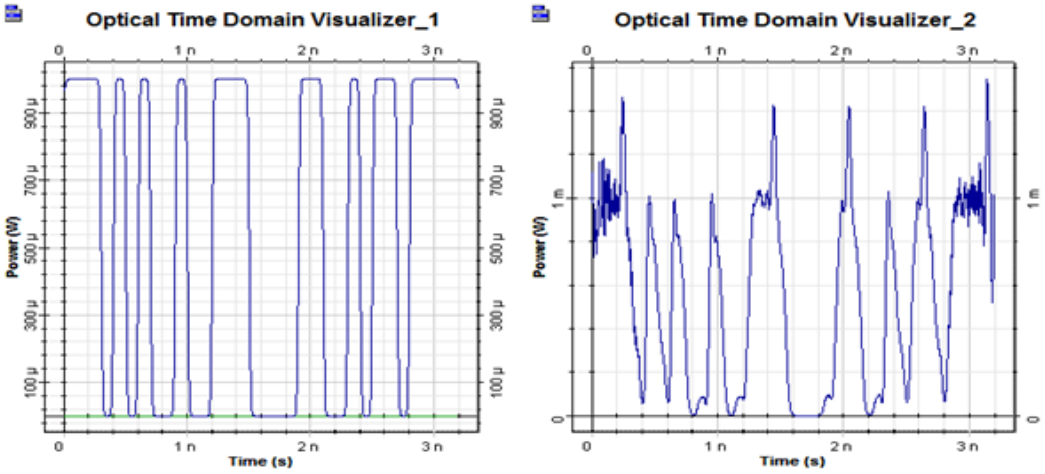


Рис. 4. Влияние ПМД на последовательность импульсов

В качестве тестового сигнала выбрана последовательность импульсов кода NRZ системы передачи со скоростью 10 Гбит/с. Компонент «PMD Emulator» воспроизводит волокно с высокой ПМД. При моделировании не учитывается хроматическая дисперсия и затухание. На выходной последовательности на фронтах импульсов заметны характерные искажения в форме выбросов. Полученные результаты хорошо согласуются и во многом повторяют результаты численного и экспериментального исследования ПМД представленного в работе [5].

Далее было выполнено моделирование с использованием компонента «PMD Emulator» и получены глаз-диаграммы и зависимость Q-фактор от ДГЗ для систем передачи с форматами модуляции RZ и NRZ. Схема моделирования приведена на рис. 5.

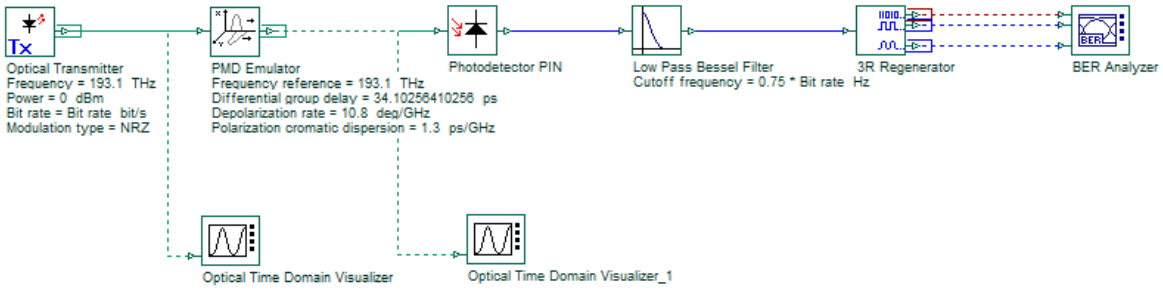


Рис. 5. Схема оценки влияния ПМД на Q-фактор

На рис. 6 приведены рассчитанные глаз-диаграммы для форматов модуляции RZ и NRZ при различных значениях дифференциальной групповой задержки.

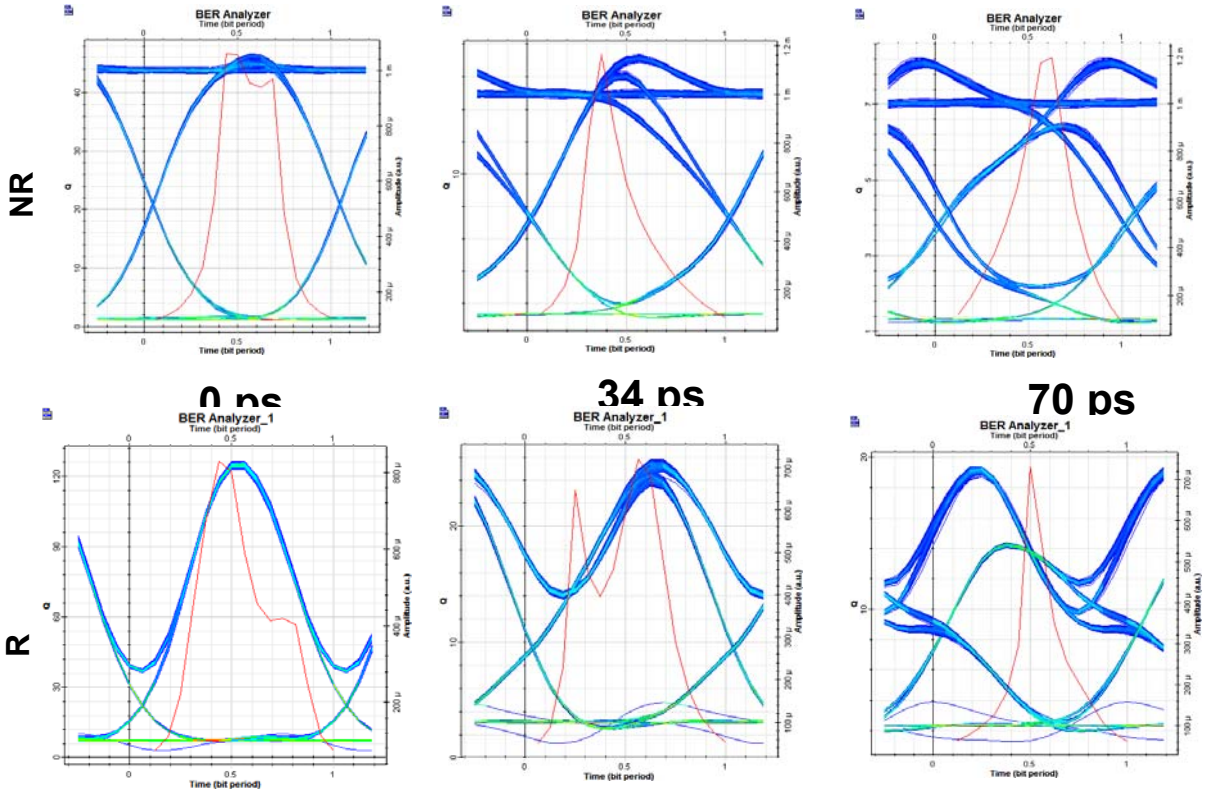


Рис. 6. Глаз-диаграммы при различном значении ДГЗ

На рис. 7 приведены зависимости Q-фактор от ДГЗ для форматов модуляции RZ и NRZ.

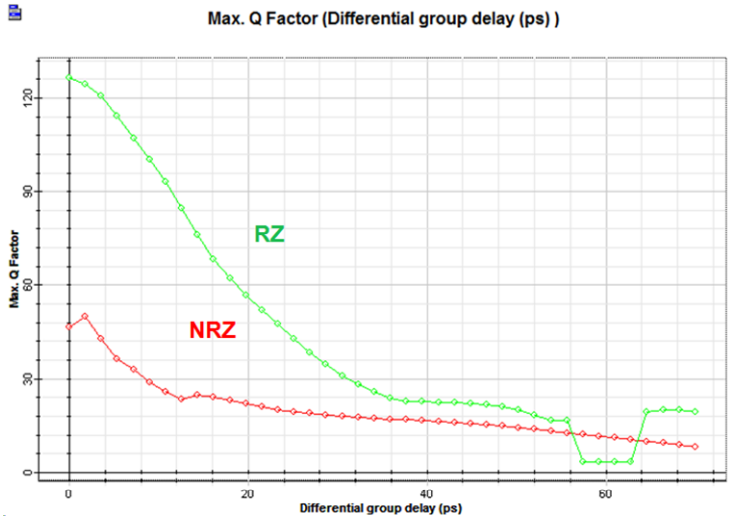


Рис. 7. Зависимость Q-фактор от значения ДГЗ

Список используемых источников

1. ОСТ 45.190-2001: Системы передачи волоконно-оптические. Стыки оптические. Термины и определения. М. : ЦНТИ «ИНФОРМСВЯЗЬ», 2002.

2. ГОСТ Р МЭК 60793-1-48-2014. Волокна оптические. Часть 1-48. Методы измерений и проведение испытаний. Поляризационная модовая дисперсия. М. : Стандартинформ, 2015. 47 с.

3. Agarkar A. M., Prajakta Joharapurkar. PMD & DGD Performance Analysis in SMF due to Fiber Irregularities // International Journal of Computer Applications, Vol. 12. No.6. December 2010.

4. OptiSystem Optical Communication System Design Software / Tutorials. 2016. Vol. 1. Optiwave, 2016.

5. Cristian Francia, Frank Bruyere, Denis Penninckx, and Michel Chbat. PMD Second-Order Effects on Pulse Propagation in Single-Model Optical Fibers // IEEE Photonics Technology Letters, December 1998. PP. 1739–1741.

УДК 004.056.53

МОДЕЛИ НАРУШИТЕЛЕЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Е. Ю. Герлинг, Е. И. Кулишкина

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

В данной статье произведен анализ вероятных нарушителей, определены типовые модели нарушителей, целью которых являлось хищение конфиденциальной информации путем атак на локальные вычислительные сети. На примере формулы расчета вероятности утечки информации произведена оценка вероятности утечки информации при атаке, направленной на персональный компьютер, оснащенный антивирусным программным обеспечением. На основе предложенной классификации нарушителей приведен ряд методов защиты информационной системы.

информационная безопасность, модель нарушителя, вероятность утечки информации, антивирусное программное обеспечение.

В настоящее время локальные вычислительные сети (ЛВС), совершив стремительный технологический прорыв, стали неотъемлемой частью производственно-технологической базы любого предприятия, от малого до крупного бизнеса, как в России, так и за рубежом. Появление новых технологий, внедряемых в ЛВС, не только расширили возможности функционирования, но и сделали их наиболее уязвимыми для вероятных нарушителей информационной безопасности. Именно поэтому основная перспектива состоит в создании и применении современной всесторонней системы защиты ЛВС. Знание угроз и уязвимых мест ЛВС способствует построению модели нарушителя информационной безопасности.

Прежде чем приступить к формированию модели нарушителя, необходимо иметь общее представление об актуальных угрозах на объекте. В основном, угрозы можно подразделить на две категории: технические и человеческий фактор. К первой категории относятся ошибки в программном обеспечении, ошибки типа отказа в обслуживании, внедрение компьютерных вирусов, червей, троянских коней, применение различных технических съемов информации и внедрение прослушивающих программ (например, снифферы) [1]. Ко второй непосредственно все деяния, связанные с человеческой деятельностью: промышленный шпионаж, низкая квалификация и халатность сотрудников.

Для построения комплексной модели защиты объекта связи, в первую очередь, необходимо определить несколько моделей нарушителя информационной системы (ИС). Эти модели предусматривают анализ потенциального нарушителя безопасности информационной системы. Целесообразно разработать несколько моделей злоумышленника, отличающихся типом нарушителей информационной безопасности объекта. Акцентируем внимание на те виды злоумышленников, которые обладают высокой профессиональной подготовкой и достаточными знаниями об информационной системе объекта и его системе безопасности.

Конкуренты. Основная преследуемая цель – незаконное получение, использование, разглашение коммерческой, служебной или иной тайны организации. Обладает значительными финансовыми возможностями и высокой квалификацией. Является одним из самых агрессивных типов нарушителей. С точки зрения методов и средств достижения результата – обладает современными технико-экономическим потенциалом.

Администраторы. Основной направленностью атак является присвоение полномочных прав, доступ к конфиденциальным, коммерческим и персональным данным. Высокая квалификация, имеют доступ к несанкционированному съему информации, блокированию отдельных пользователей, модификации пути маршрутизации и политик безопасности сети. Осуществляют действия, направленные на остановку или сбой сервера, модификацию или уничтожение ПО, создание ложных информационных сообщений, всеми доступными способами [2].

Хакеры. Атака направлена на получение информации о внутренней структуре сети, перехват сведений, проходящих по информационным потокам, создание условий, приводящих к выходу сети из строя (сбой северов, модификация/уничтожение программного обеспечения (ПО)) и внедрение «червяков» и «троянов», т. е. «прослушка» и съем информации [3]. Обладает значительными знаниями в области операционных систем и языков программирования. Совершение атак производят при помощи прослушивания коммутируемых сетей, перенаправление трафика, внедрение вирусных кодов в ПО, атак отказа в обслуживании.

Программисты. Преследуется личная коммерческая выгода. Направленность действий заключается во внедрении вирусных кодов в разрабатываемые продукты или внесении изменений в имеющиеся данные организации. Обладают высокой квалификацией в области программного обеспечения и знаний языков программирования. Атаки осуществляют посредством внесения неконтролируемых изменений в базы данных организации при помощи программного кода, встраивания в разрабатываемые продукты систем несанкционированного доступа или систем блокировки работы по условному ключу или команде.

Операторы. Не являются критичным типом злоумышленника. Выносят исключительно личную выгоду при имеющемся доступе к базам данных организации. В качестве используемых методов – осуществляют действия, направленные на остановку или сбой сервера.

Технический персонал. Основная цель: хищение конфиденциальной информации. Обладают специфическими возможностями по созданию незарегистрированных точек входа и выхода из локальной сети, модификации топологии сети. При имеющемся доступе в особо защищённые помещения (например, серверные) и легитимном имени и пароле входа в систему, могут выполнять действия, непосредственно направленные на хищение или уничтожение конфиденциальной информации организации.

Сотрудники, уволенные с работы. Цели носят исключительно личный и коммерческий мотив. Возраст не имеет значения. Квалификация зависит от бывших прав при работе в системе. Применяют существующие знания с целью уничтожения или же хищения конфиденциальной информации, для её дальнейшей передачи конкурентам и получения материальной выгоды.

Наиболее сложным этапом при построении моделей несанкционированного доступа к персональным компьютерам (ПК) и информационным системам (ИС) – является оценка вероятностей реализации каналов несанкционированного доступа. Элементарная оценка вероятности утечки информации может быть получена из рассмотрения конфликтной ситуации, содержание которой представляет ряд последовательных способов действий (стратегий) противоборствующих сторон – злоумышленника и атакуемого объекта:

$$q = (q_1, \ldots, q_n),\ s = (s_1, \ldots, s_n),$$

где q_i – вероятность применения злоумышленником i-й стратегии ($i = \{1, n\}$) для поиска интересующего его информативного сигнала; s_i – вероятность применения объектом (в целях уравновешивания указанной стратегии) j-го способа (средства) защиты сигнала ($j = \{1, m\}$).

Предполагается, что злоумышленнику априори известна логическая связь между информативным сигналом и характером отображаемой им информации, а также что соблюдается равенство, показывающее, что для объекта обязательно будет применен какой-либо способ защиты, а злоумышленник обязательно применит какой-либо способ атаки:

$$\sum_{i=1}^{n} q_i = \sum_{j=1}^{m} s_i = 1.$$

Примем r_{ij} – элементарная вероятность обнаружения искомого информативного сигнала с помощью соответствующего специального технического средства (СТС). Тогда, обращаясь к аппарату теории вероятностей, искомая вероятность утечки информации:

$$P_{\text{УТ}} = q_i \cdot \left(1 - s_i r_{ij}\right). \quad (1)$$

Формула (1) позволяет сделать следующий вывод: основным резервом обеспечения заданного уровня скрытия информации от злоумышленника в условиях производственного объекта является выбор приемлемого значения r_{ij} из условия минимизации $P_{\text{УТ}}$.

Установка антивирусного программного обеспечения сегодня обязательна для всех пользователей ПК, обеспокоенных проблемой безопасности данных. Исследование надежности антивирусов в основном сводится к проверке эффективности ПО в реальных условиях [4]. Для выбора оптимального антивирусного ПО проведем сравнительную характеристику выбранных продуктов (табл.). Статистические данные взяты из отчета о результатах тестирования файлового обнаружения антивирусов, проводимого в марте 2016 г., опубликованным AV-Comparatives в сотрудничестве с Microsoft [5].

ТАБЛИЦА. Сводка данных по рассматриваемым антивирусам

Наименование	Производитель	Вероятность обнаружения атаки, r_i (%)	Вероятность утечки информации, $P_{\text{ут}}$ (%)
Kasrepsky	Лаборатория Касперского (Россия)	88	6
Avira	Avira GmbH & Co. KG (Германия)	76	12
AVG	AVG Technologies (Чехия)	74	13
Sophos Anti-Virus	Sophos (Великобритания)	56	22

Представим вычисления на примере оценки эффективности антивирусного ПО Kaspersky. Примем в качестве q_i значение равное 0,5, при этом, считая, что почти все ПК оснащены антивирусными программами примем s_i равную 0,999. Вероятность обнаружения искомого информативного сигнала с помощью антивирусного программного обеспечения r_i примем равную 0,88, исходя из статистических данных об отражении атак антивирусами [5].

Далее вычислим вероятность утечки информации по формуле (1):

$$P_{\text{ут}} = 0{,}5 * (1 - \ 0{,}999 * 0{,}88),$$

$$P_{\text{ут}} = 0{,}06.$$

Приведя полученные данные в проценты, получаем, что вероятность утечки информации при осуществлении атак ПК, оснащенные антивирусным ПО приблизительно будет равна 6 %.

Аналогичным образом вычислим значения вероятности утечки информации для других предложенных антивирусов (табл.).

Полученные значения являются достаточно высокими, и можно сделать вывод, что сегодня ни один продукт не способен гарантировать 100 %-защиту от угроз, связанных с внедрением вредоносного кода.

Полное представление о существующей опасности и правильный выбор методов защиты способны свести возможность заражения к минимуму. Для снижения рисков компрометации информационных систем следует уделять особое внимание внешним ресурсам. При размещении и функционировании антивирусных программ необходима обязательная проверка файлов, вводимых с дисковых систем, устройств флеш-памяти во время загрузки. Вход в ИС должен осуществляться через систему паролей и аутентификационных процедур. Для контроля за ресурсами сети необходимо проводить сканирование ресурсов, доступных из внешних сетей [6]. Для защиты данных от угроз со стороны внутреннего злоумышленника следует прибегать к использованию шифрования информации и применения электронной цифровой подписи. Стоит так же предусмотрительно подходить к разграничению доступа сотрудников. Помимо программной защиты информационной системы необходимо разрабатывать ряд документаций, в которых будут отражены не только обязанности сотрудников, но также и ответственность за нарушение норм безопасности объекта (напр., должностная инструкция специалиста по защите информации) [7]. Кроме базовых мер защиты следует так же проводить аудит информационной безопасности и тест на проникновение внутреннего или внешнего нарушителя.

Список используемых источников

1. Андрианов В. И., Красов А. В., Липатников В. А. Инновационное управление рисками информационной безопасности: учеб. пособие. СПб. : СПбГУТ, 2012. 396 с. ISBN 978-5-91891-092-4.

2. Модель угроз и нарушителя безопасности персональных данных, обрабатываемых в типовых информационных системах персональных данных отрасли. Утверждена ФСТЭК России от 04.06.2010 г. № 240/2/2271. С. 33–39.

3. Мельников Ю. Н., Теренин А. А. Возможности нападения на информационные системы банка из Интернета и некоторые способы отражения этих атак [Электронный ресурс] // Сайт CITforum. 2004. URL: http://citforum.ru/security/articles/banks/ (дата обращения 26.02.2017).

4. Калашникова А. А., Калинин Д. А., Клеймёнов А. В., Стремоухов В. Д., Янковская А. А. Разработка методики сравнительного тестирования антивирусных продуктов // Научно-технический вестник ИТМО. 2008. № 52. С. 283–289.

5. Василий Бердников, Сергей Ильин. Сравнение антивирусов по эффективности защиты от новейших вредоносных программ [Электронный ресурс] // ЧОУ ДПО «Центр предпринимательских рисков» URL: http://www.cprspb.ru/bibl/computer/57.htm (дата обращения 26.02.2017).

6. Сборник исследований по практической безопасности «Positive Research». 2016 [Электронный ресурс]. URL: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Positive-Research-2016-rus.pdf (дата обращения 26.02.2017).

7. Должностная инструкция специалиста по защите информации [Электронный ресурс]. URL: http://www.it-rabota.ru/spec_zashita.phtml (дата обращения 26.02.2017).

УДК 535

ИССЛЕДОВАНИЕ ВЛИЯНИЯ НЕЛИНЕЙНЫХ ЭФФЕКТОВ НА ПРОЦЕССЫ ПЕРЕДАЧИ СИГНАЛОВ В ВОЛОКОННО-ОПТИЧЕСКИХ СИСТЕМАХ СВЯЗИ С DWDM

С. Ф. Глаголев, С. Э. Доценко, Л. Ю. Дуров, Т. Р. Ялунина

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

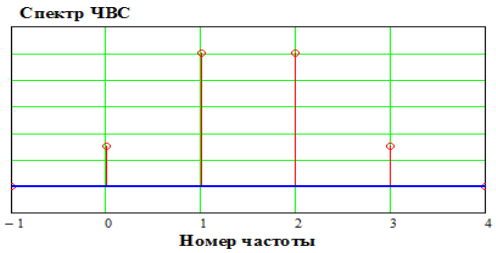
В одномодовых ОВ может возникать нелинейное взаимодействие нескольких оптических волн, в результате которого появляются комбинационные гармоники. Одним из таких эффектов является четырехволновое смешение ЧВС. Название эффекта связано с тем, что во взаимодействии участвуют четыре волны. Этот эффект играет важную роль в ВОСП с DWDM. Он сильно проявляется при совместном распространении по одномодовым ОВ нескольких квазимонохроматических волн с близкими частотами и поляризациями.

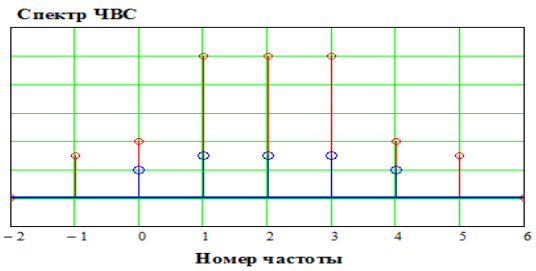
ВОЛС, DWDM, нелинейные эффекты, четырехволновое смешение.

При нелинейном взаимодействии излучений трех различных частот возникают комбинационные частоты [1, 2, 3, 4, 5]:

$$\nu_{ijk} = \nu_i + \nu_j - \nu_k. \quad (1)$$

Таких частот может быть много. Примем $i = 1, j = 2, k = 3$. В результате действия ЧВС происходит генерация девяти комбинационных частот, а именно: ν_{112}, ν_{113}, ν_{123}, ν_{132}, ν_{221}, ν_{223}, ν_{231}, ν_{331}, ν_{332}, а фактически семи частот, так как некоторые частоты совпадают: $\nu_{123} = \nu_{112}$, $\nu_{132} = \nu_{312}$, $\nu_{231} = \nu_{332}$ дают совпадающие частоты (рис. 1*б*).





Номер частоты	0	1	2	3
Значение частоты	$2\nu_1-\nu_2$	ν_1	ν_2	$2\nu_2-\nu_1$

Номер частоты	–1	0	1	2	3	4	5
Значение частоты	$\nu_1-2\Delta\nu$	$\nu_1-\Delta\nu$	ν_1	ν_2	ν_3	$\nu_3+\Delta\nu$	$\nu_3+2\Delta\nu$

Рис. 1. Спектр ЧВС при двух (слева) и трех (справа) несущих

Минимальное количество каналов DWDM равно двум (частоты ν_1 и ν_2). Этот случай относится к вырожденному варианту ЧВС и количество комбинационных частот будет равно двум. Полагаем, что интервал между частотами равен $\Delta\nu$. Введем обозначения для двух комбинационных частот и запишем для них выражения:

$$\nu_{ij} = 2\nu_i - \nu_j = \nu_i - \Delta\nu;$$

$$\nu_{jji} = 2\nu_j - \nu_i = \nu_j + \Delta\nu = \nu_i + 2\Delta\nu. \quad (2)$$

Если количество каналов в системе DWDM равно N, то количество комбинационных частот резко возрастает и составляет [4, 6]:

$$\mathrm{M} = \frac{N^2(N-1)}{2}. \quad (3)$$

На рис. 2 показана зависимость количества возникших комбинационных частот от количества каналов.

Для четного количества каналов N, расположенных через равные интервалы $\Delta\nu$ по ча-

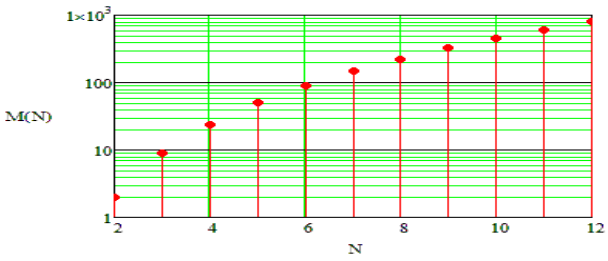


Рис. 2. Зависимость количества возникших комбинационных частот от количества каналов

стоте, можно определить количество помех за счет ЧВС, воздействующих на m-й канал WDM, по формуле [6]:

$$M_m = \frac{N^2}{2} + \frac{N \cdot m}{2} - \frac{m^2}{2} - N + \frac{m}{2}. \quad (4)$$

Для общего количества помех ЧВС, которые попадают в каналы N – канальной DWDM системы справедливо [6]:

$$M_N = \frac{1}{3}N^3 - \frac{3}{4}N^2 + \frac{1}{6}N. \quad (5)$$

Результаты расчетов по выражениям (3), (4) и (5) приведены в таблице 1.

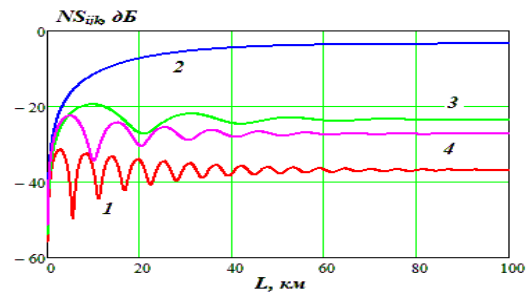
ТАБЛИЦА 1. Количество помех ЧВС в отдельных каналах WDM

N	2		4				6					
M	2		24				90					
M_N	0		10				46					
m	1	2	1	2	3	4	1	2	3	4	5	6
M_m	0	0	2	3	3	2	6	8	9	9	8	6

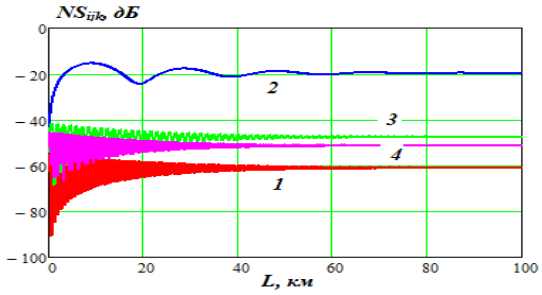
Отметим, что в DWDM системе с большим количеством каналов помеха в подверженном помехам конкретном канале складывается из большого количества отдельных помех. Из рис. 1 видно, что всего три действующих канала создают в других каналах до двух помех. При увеличении количества каналов количество помех в каждом канале быстро растет (табл. 1).

Проведены расчеты в среде MathCad зависимостей отношения NS_{ijk} мощности помех P_{ijk} к мощности сигнала на выходе ОВ от длины линии L для четырех ОМ ОВ: стандартного SMF-28e (1 кривая), со смещенной дисперсией DSF (G.653) (2 кривая), с ненулевой смещенной дисперсией +NZ DSF (LEAF) (3 кривая), с ненулевой смещенной дисперсией – NZ DSF (MetroCor) (4 кривая). Частота i – канала была выбрана равной ν_i = 194 ТГц (40 канал в частотной сетке МСЭ с интервалом между каналами $\Delta\nu$ = 100 ГГц). Частоты других каналов выбирались по выражениям.

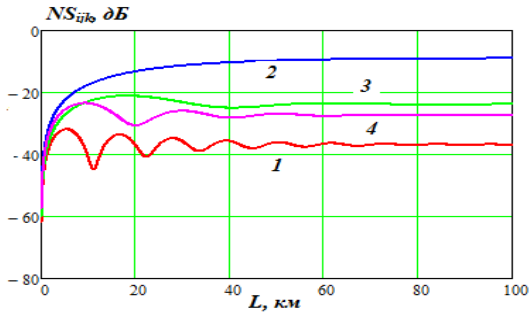
Расчеты проводились при значениях $\Delta\nu$ = 25 ГГц и 100 ГГц для вырожденного и невырожденного случаев для канальных мощностей P = 20 и 50 мВт. Результаты расчетов приведены на рис. 3.



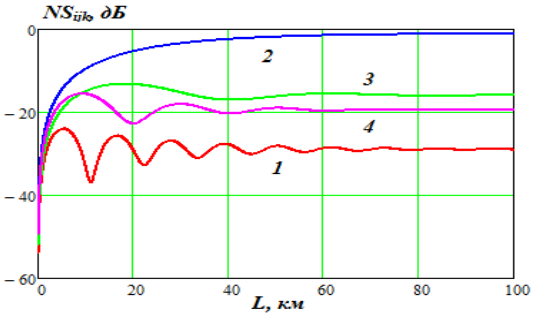
а) P = 20 мВт, $\Delta\nu$ = 25 ГГц, невырожд. случай



б) P = 20 мВт, $\Delta\nu$ = 100 ГГц, невырожд. случай



в) P = 20 мВт, $\Delta\nu$ = 25 ГГц, вырожд. случай



в) P = 50 мВт, $\Delta\nu$ = 25 ГГц, вырожд. случай

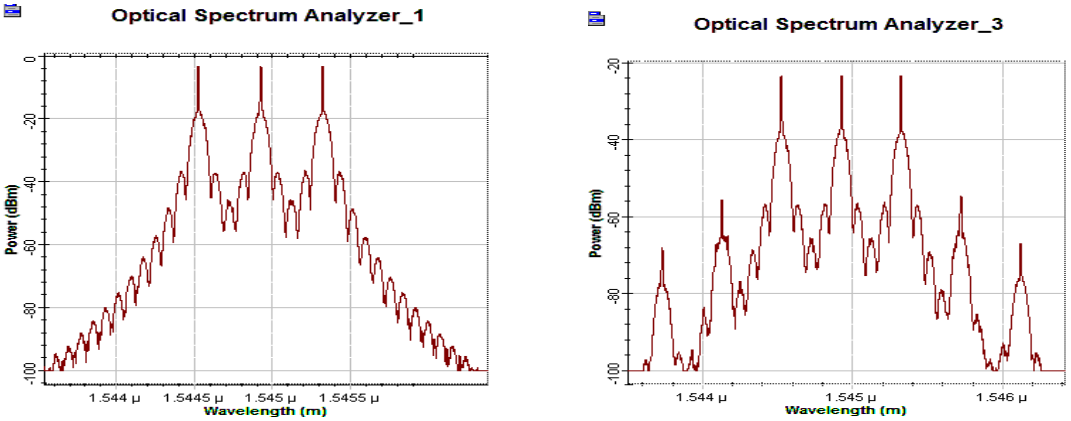
Рис. 3. Результаты расчетов отношения помехи к сигналу на выходе ОВ от его длины

Видно, что отношение помехи ЧВС к сигналу с увеличением длины ОВ при малых длинах быстро растет, испытывает затухающие колебания и стремится к установившемуся значению при больших длинах. Период колебаний уменьшается с увеличением интервала по частоте между каналами. Уровень помех от других каналов быстро уменьшается с увеличением частотного интервала между влияющими и подверженными влиянию каналами. Величина помехи ЧВС уменьшается при возрастании ХД и уменьшении мощности канальных сигналов. Особенно сильно эффект ЧВС проявляется на волнах, длина которых близка к длине волны нулевой дисперсии ОВ. Расчеты показывают, что ОВ со смещенной дисперсией DSF не пригодны для использования в ВОСС с технологией DWDM, работающих в диапазоне *C* (1530–1565 нм).

Было проведено исследование влияния эффекта ЧВС на процессы в линейном тракте ВОСС при использовании двух типов одномодовых ОВ: волокна со смещенной дисперсией DSF и стандартного волокна SF.

Спектр выходного сигнала после мультиплексора (на входе в ОВ DSF) показан на рис. 4*а* при уровне источников излучения 0 дБм. Видно, что из-за АМ в формате NRZ уровень сигналов на выходе мультиплексора примерно на 3 дБ меньше чем на источнике. На рис. 4*б* показан спектр сигнала на выходе ОВ. Видно, что эффект ЧВС уже проявляется, и на спектрограмме хорошо видны новые частотные составляющие – его продукты. В нашем

случае интервал между всеми частотами одинаковый, и соответствующий выбранной сетке частот DWDM $\Delta\nu$ = 50 ГГц ($\Delta\lambda$ = 0,4 нм)



а) б)

Рис. 4. Спектры входного (а) и выходного (б) сигналов при уровне мощности источника излучения 0 дБм

ТАБЛИЦА 2. Результаты моделирования ЧВС в ОВ DSF

№ частоты	–2	–1	0	1	2	3	4	5	6
p_0, дБм	–6								
p_l, дБм			–73/ –74,9	–30	–30	–30	–73/ –74,9		
Q				26	24	26			
p_0, дБм	0								
p_l, дБм		–68/ –65,2	–56/ –56,9	–24	–24	–24	–56/ –56,9	–68/ –65,2	
Q				26	16	26			
p_0, дБм	6								
p_l, дБм	–72/*	–50/ –47,2	–38/ –38/9	–18	–18	–18	–38/ –38/9	–50/ –47,2	–72/*
Q				8,5	4,8	8,4			
p_0, дБм	10								
p_l, дБм	–56/*	–39/ –35/2	–30/ –26/9	–14	–14	–14	–30/ –26/9	–39/ –35/2	–56/*
Q				4,3	2,6	4,3			
p_0, дБм	16								
p_l, дБм	–36/*	–28/ –17,2	–24/ –8,9	–15	–15	–15	–24/ –8,9	–28/ –17,2	–36/*
Q				2,7	2,3	2,7			

Примечания: В столбцах –2, –1, 0, 4, 5, 6 указаны уровней помех, первые, полученные в результате моделирования, а вторые после черточки, полученные в результате расчетов.

*означает, что соответствующие данные отсутствуют. В столбцах 1, 2, 3 указаны уровни сигналов, полученные в результате моделирования.

Из таблицы 2 следует, что при использовании ОВ DSF наихудшее качество связи (минимальная величина Q) реализуется в среднем из трех каналов DWDM, а допустимый уровень на входе ОВ не превышает 3 дБм ($Q > 7$).

Отметим, результаты моделирования проведенных расчетов хорошо совпадают с результатами моделирования вплоть до больших уровней входных сигналов (до 16 дБм).

В заключение отметим, что эффект ЧВС в основном ухудшает качество связи по ОВ. Однако он находит и полезные применения. Например, он может использоваться для преобразования частоты излучения в конвертерах, где для преобразования частоты сигнала с частотой ν_{c1} в другую частоту ν_{c2} используется излучение накачки с частотой ν_p в соответствии с выражениями (2):

$$\nu_{c2} = 2\nu_{c1} - \nu_{p1} \text{ или } \nu_{c2} = 2\nu_{p2} - \nu_{c1}.$$

Список используемых источников

1. Агравал Г. Нелинейная волоконная оптика: пер. с англ. М. : Мир, 1996. 323 с.

2. Иванов А. Б. Волоконная оптика: компоненты, системы передачи, измерения. М. : Компания Сайрус СИСТЕМС, 1999/ 672 с.: ил.

3. Листвин А. В., Листвин В. Н., Швырков Д. В. Оптические волокна для линий связи. М. : ЛЕСАРарт, 2003. 288 с.

4. Воронин В. Г., Наний О. Е. Основы нелинейной волоконной оптики: учебное пособие. М. : Университетская книга, 2011. 128 с.

5. Слепов Н. Н. Современные технологии цифровых оптоволоконных сетей связи. М. : Радио и связь, 2000. 468 с.: ил.

6. Jing Liang. Electrical Post-Compensation for Four-Wave Mixing Nonlinear Impairments Using Digital Coherent Detection in WDM Optical Communication Systems / A dissertation submitted to Kochi University of Technology in partial fulfillment of the requirements for the degree of Doctor of Philosophy Special Course for International Students Graduate School of Engineering Kochi University of Technology Kochi, Japan, August 2011.

УДК 535.92, 535.93, 531.717.53

РОЛЬ ФОТОНИКИ В ПЕРСПЕКТИВНЫХ ИНФОКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЯХ

С. Ф. Глаголев, Е. В. Полякова, Т. Р. Ялунина

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

На сегодняшний день многие перспективные инфокоммуникационные технологии строятся на принципах фотоники: от оптических дисков до создания сенсоров, регистрирующих световые потоки в соответствии с малейшим изменением окружающей среды. Фотоника охватывает множество наук и технологий, связанных с генерацией, управлением и обнаружением фотонов. В их число входят: оптика, лазерная физика, квантовая электроника, спектроскопия, оптоэлектроника, квантовые технологии, био-, нано- и радиофотоника и многое другое.

интегральная оптика, радио по волокну, RoF, перестраиваемые мультиплексоры, радиофотоника, ROADM, перспективные инфокоммуникационные технологии.

Фотоника – это область науки и техники, связанная с использованием светового излучения в оптических элементах, устройствах и системах, в которых генерируются, преобразуются и распространяются оптические сигналы.

Фотоника широко используется в инфокоммуникационных технологиях и позволяет создавать устройства для хранения огромных объемов информации, высокоскоростной передачи и обработки данных. На базе фотонных технологий и оптических волокон быстро развиваются новые методы измерений, создаются измерительные преобразователи (сенсоры) для контроля окружающей среды и технических устройств.

Одно из главных применений фотоника нашла в волоконно-оптических системах связи. Внедрение оптических волокон и оптических кабелей произвело революцию в телекоммуникационной отрасли, многократному увеличению трафика и резкому повышению эффективности использования направляющих систем связи. Прогресс в развития оптической связи обеспечивается развитием фотоники во многих областях.

На сегодняшний день в волоконно-оптических линиях связи перед фотоникой ставится ряд задач, к которым относятся:

– миниатюризация оптических элементов, устройств и систем;

– интеграция оптических элементов, устройств и систем на единой базе;

– сверхбыстродействие оптических систем;

– сверхскоростная передача больших массивов информации;
– низкий уровень энергии управляющих сигналов;
– полифункциональность оптических материалов.

Многие из этих задач решаются средствами интегральной оптики [1].

Интегральная оптика – это раздел фотоники, в котором разрабатываются принципы и методы объединения на единой подложке различных оптических и электронных элементов для создания сложных оптических и оптоэлектронных устройств. В таких устройствах используют оптические волноводы, электрические полосковые линии, источники и приемники излучения, оптические фильтры, усилители, модуляторы, интерферометры и т. п.

Необходимо отметить, что в отличие от интегральной электроники, интегральная оптика использует в качестве носителей заряда не электроны, а фотоны, что обеспечивает ряд преимуществ интегрально-оптических схем, к которым можно отнести широкую полосу пропускания, низкие оптические потери, нечувствительность к электромагнитным помехам, малые габариты, массу и более низкую стоимость. Но основным достоинством интегральной оптики является высокое быстродействие. Уже созданы интегрально-оптические переключатели со временем переключения меньше 100 фс. Такие показатели недостижимы для устройств обычной полупроводниковой электроники. Возможность передачи и обработки больших объемов информации определяет быстрое развитие интегральной оптики в настоящее время.

Еще одним перспективным направлением является технология передачи сверхвысокочастотных радиосигналов на большие расстояния по волокну RoF (*Radio over Fiber*).

Совместное использование беспроводной передачи данных и передачи по оптическому волокну было впервые продемонстрировано в начале 1980-х гг. в США для военного назначения. Оптические кабели были использованы для соединения центральной станции с удаленной антенной в радиолокационных системах. Низкий уровень потерь и большая полоса частот сделали оптическое волокно эффективным средством передачи высокочастотных радиосигналов.

В общем виде RoF можно представить следующим образом [2] (рис. 1).

Главное отличие этой технологии от традиционных волоконно-оптических систем передач заключается в том, что она решает радиотехнические задачи. Позволяет централизовать обработку радиосигналов в одном месте – на центральной станции. Далее радиосигналы передаются по оптическому волокну до модулей удаленного доступа. Такая организация системы позволяет максимально упростить модули удаленного доступа, так как они выполняют функции только оптоэлектронного преобразования, усиления и фильтрации.

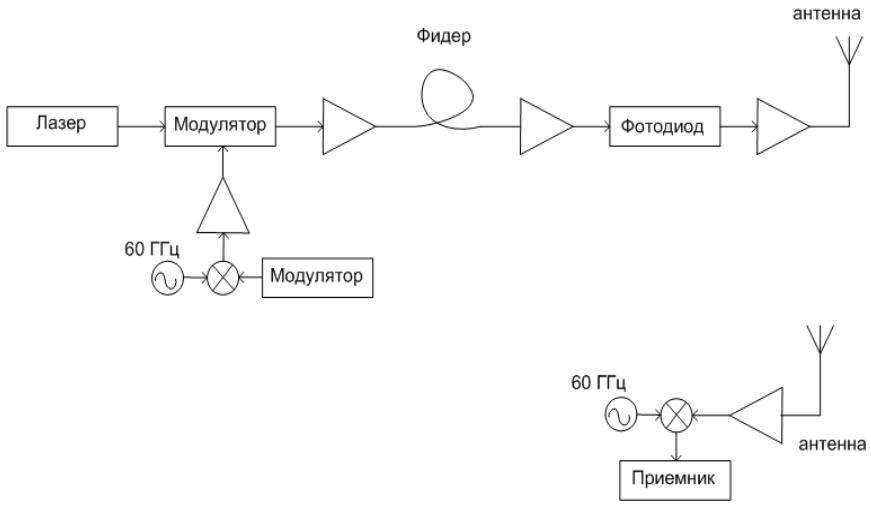


Рис. 1. Обобщенная модель системы передачи RoF

Формирование RoF-сигнала возможно тремя способами:

а) Классическая схема формирования RoF-сигнала (рис. 2);

б) Формирование RoF-сигнала с шириной спектра, равной промежуточной частоте радиосигнала (рис. 3);

в) Передача радиосигнала на оптической несущей (рис. 4).

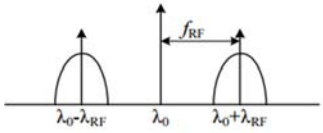


Рис. 2. Классическая схема формирования RoF-сигнала

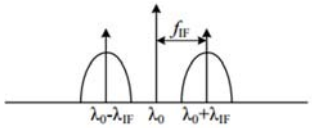


Рис. 3. Формирование RoF-сигнала с шириной спектра, равной промежуточной частоте радиосигнала

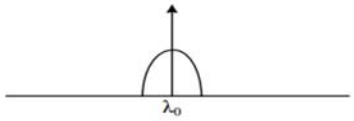


Рис. 4. Передача радиосигнала на оптической несущей

Использование одного из приведенных выше способов зависит от применимости систем и от элементной базы центральной станции.

В случае классической схемы формирования RoF-сигнала (см. рис. 2), радиосигнал с частотой f_{RF} передается по оптической линии на центральной длине волны источника оптического излучения (λ_0). Спектр оптического сигнала в результате модуляции имеет две боковые полосы. Преимуществом данного способа передачи является простота реализации базовой станции, так как формирование сигнала осуществляется на центральной станции. Однако такой способ передачи требует наличия высокоскоростных оптоэлектронных компонентов (фотодетекторов) для преобразования оптического сигнала в электрический сигнал. Также при данном способе передачи огромное влияние на сигнал оказывает хроматическая дисперсия.

Для уменьшения влияния хроматической дисперсии используется схема формирования RoF-сигнала с шириной спектра, равной промежуточной частоте радиосигнала (см. рис. 3). На центральной станции электрический сигнал преобразуется с понижением до промежуточной частоты, далее сформированный сигнал поступает в волоконно-оптическую линию связи. Преимуществом данной схемы является использование низкоскоростных оптоэлектронных компонентов. Однако на базовой станции требуются стабильный генератор колебаний и высокоскоростной смеситель для преобразования частоты.

Третий способ формирования характерен для сверхширокополосных (СШП) радиосигналов (см. рис. 4). На центральной станции происходит формирование СШП-сигнала, затем он передается в оптический тракт. При данном способе формирования RoF-сигнала хроматическая дисперсия практически не оказывает влияния на сигнал и не требуется использование высокоскоростных оптоэлектронных компонентов. Однако компонентная часть системы сильно усложняется, так как на базовой станции требуются компоненты для обработки сигналов.

Наиболее широкое применение технология RoF нашла в распределенных антенных системах (*Distributed Antenna System*, DAS) и в общегородских сетях (*Metropolitan Area Network*, MAN).

В настоящее время наблюдается большой интерес среди разработчиков базовых станций мобильной связи и радиолокационных станций к фазированным антенным решеткам, состоящим из множества элементарных излучателей [3]. С целью снижения габаритов и массы антенны, предлагается воспользоваться методами радиофотоники. Оптическое излучение лазера, расположенного на значительном расстоянии от антенны, в аппаратной, модулируется сверхвысокочастотным радиосигналом, и передается по оптическому волокну к своему достаточно мощному фотодиоду. Фотодиод выделяет высокочастотный модулирующий сигнал и передает его на свою элементарную антенну. Управляя фазами модулирующих сигналов элементарных антенн можно изменять диаграмму направленности фазированной антенной решетки (рис. 5). Для реализации этой конструкции нужны широкополосные высокочастотные модуляторы, фазовращатели, высокочувствительные быстродействующие фотодиоды. Возможна реализация данной конструкции в интегральном исполнении.

В настоящее время происходит бурное развитие полностью оптических сетей передачи данных, в которых добиться высокой пропускной способности возможно только с использованием оптических мультиплексоров и демультиплексоров светового потока. Промышленное внедрение технологий этих устройств связано с поиском путей совершенствования параметров преобразователей и преимуществ, которые скомпенсируют увеличение стоимости.

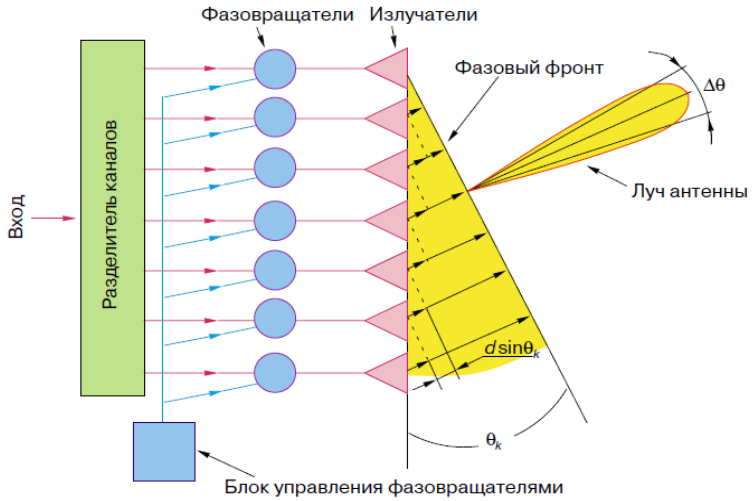


Рис. 5. Схема фазированных антенных решеток

Динамически изменяемые транспортные решения на основе перестраиваемых мультиплексоров (*Reconfigurable Optical Add-Drop Multiplexer*, ROADM) имеют огромное значение в первую очередь в сетевых приложениях, где постоянно изменяющиеся схемы движения трафика делают невозможным предварительное планирование, и традиционные статические решения становятся крайне неэффективными. Многонаправленные реконфигурируемые оптические мультиплексоры ввода/вывода увеличивают гибкость транспортных решений. Основная задача ROADM – позволить оператору изменять топологию сети в зависимости от текущих нужд без замены оборудования. В быстрорастущих сетях или при добавлении больших узлов или новых клиентов динамически изменяемые сети могут стать единственным решением, позволяющим быстро и без перерыва сервиса увеличить полосу пропускания в критичных направлениях. Используя ROADM, операторы связи, которым регулярно приходится перекидывать большие потоки данных с одного направления на другое, могут избежать огромных расходов, сопряженных с физическим перестроением сети.

Таким образом, сложно переоценить роль фотоники в перспективных инфокоммуникационных системах, так как в условиях их постоянного развития, необходимо появление все новых технологий, отвечающих высоким требованиям, которые вполне могут быть удовлетворены использованием принципов фотоники, что дает возможность стремительного развития систем связи.

Список используемых источников

1. Ханспердже р, Роберт. Интегральная оптика: Теория и технология ; пер. с англ.: В. Ш. Берикашвили, А. Б. Мещеряков ; ред. пер. с англ.: В. А.Сычугов. М. : Мир, 1985. 379 с.

2. Сперанский В. С., Кливцов О. И. Передача радио по волокну // T-Comm: телекоммуникации и транспорт. 2015. Т. 9. № 11. С. 38–40.

3. Вендик О. Г. Фазированная антенная решетка – глаза радиотехнической системы. Соросовский образовательный журнал. 1997.

УДК 004.6:378.862

ТЕХНОЛОГИЯ «БЛОКЧЕЙН»: ПЕРСПЕКТИВЫ РАЗВИТИЯ, СФЕРЫ ПРИМЕНЕНИЯ, ОБРАЗОВАТЕЛЬНЫЙ ВАКУУМ

А. П. Голубев

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

Дано общее описание и выделены свойства систем на базе технологии, существенные для определения сфер возможного применения. Показаны возможные сферы применения и отмечен огромный интерес со стороны государственных и бизнес структур. Отмечено практически полное отсутствие образовательных программ по технологии на базе высшего образования. Исследован набор ожидаемых компетенций разработчика блокчейн-систем.

блокчейн, распределённый реестр, децентрализованная база данных, цепочка блоков, образовательная программа высшего профессионального образования.

В последние годы интерес к технологии блокчейн растёт лавинообразно. Подпитывается он в том числе и очень «громкими» заявлениями со стороны людей, которые влияют на формирование инновационных направлений развития мировой экономики. Например, основатель и исполнительный председатель Всемирного экономического форума, Клаус Мартин Шваб, писал, что блокчейн-системы находятся в сердце четвёртой индустриальной революции, а Марк Андриссен, сооснователь Netscape Communications и Andreessen Horowitz, заявил, что блокчейн – одно из самых существенных изобретений в истории информационных технологий [1].

Революционный эффект от применения блокчейн-систем ожидают в тех областях, которые в настоящее время активно регулируются государством, поэтому важно отметить большой интерес и высокий уровень лояльности к технологии со стороны государства. Так, Алексей Кудрин, заместитель председателя Экономического совета при президенте РФ, глава фонда «Центр стратегических разработок», на Всемирном экономическом форуме

в Давосе в январе 2016 года заметил: «Для меня Blockchain, означает следующее: что каждый человек может войти в базу данных, выписать себе все необходимые документы для покупки участка, сформировать этот пакет за час, направить его в соответствующие органы, в течение часа, если все подтвердится, получить ответ. Это, безусловно, революция…» [2]. В марте 2017 года Председатель Правительства РФ Дмитрий Медведев поручил Минэкономразвития и Минкомсвязи проанализировать возможность применения технологии блокчейн в сфере государственного управления и управления экономикой в России [3].

Чтобы понять потенциал и возможные сферы применения, рассмотрим, в чём заключается сущность «блокчейн» (*blockchain*: *block* (англ.) – блок, *chain* (англ.) – цепь, цепочка).

Терминология в этой области пока ещё только формируется, но по сути блокчейн-системы являются распределёнными базами данных, записи в которых не подлежать изменению (рис.) и одновременно децентрализованными системами управления этими базами данных.

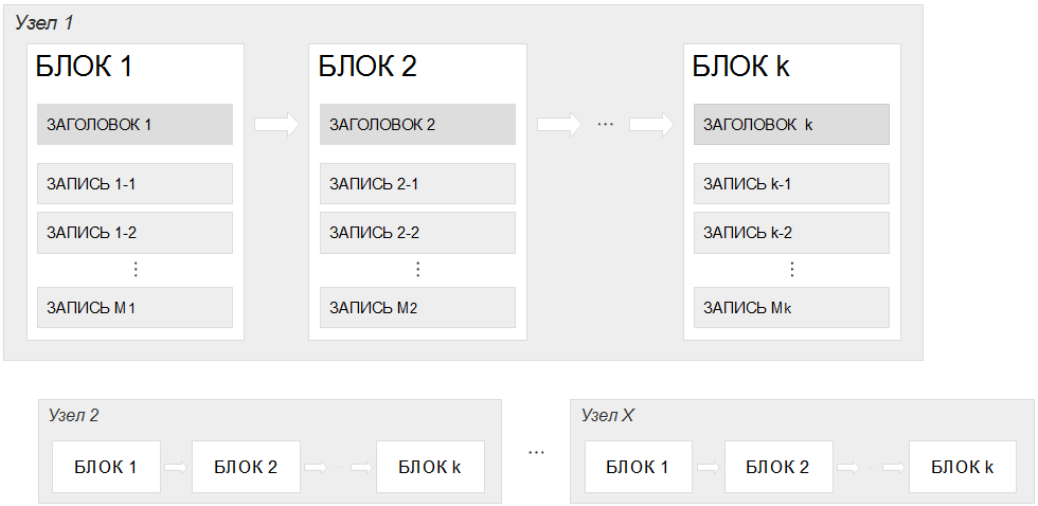


Рисунок. Упрощённая схема блокчейн-системы

Записи данных объединяют в блоки для повышения эффективности обработки и передачи (размер блока может также иметь особое значение для конкретной реализации, но не важен с точки зрения технологии в целом).

Формат записи (данных) с точки зрения блокчейн произвольный и определяется целями и задачами конкретной системы.

Чтобы обеспечить неизменность данных, в каждый блок включают результат вычисления криптографической хэш-функции [4] от данных из предыдущего. Поэтому по прошествии определённого времени невозможно изменить содержимое блока, сохранив целостность этих межблочных связей. Если блок изменится, изменится и его хэш-код (вероятность

получить тот же результат из допустимого множества входных данных ничтожно мала) – результат вычисления функции хэширования перестанет совпадать с контрольным хэш-кодом в следующем блоке, и попытка фальсификации будет обнаружена.

Каждый участник системы (узел) может хранить у себя копии всех блоков. На практике, некоторые узлы отказываются от этого (например, из-за ограниченного объёма доступной памяти). В последнем случае, информацию при необходимости запрашивают у «полных» узлов. Часто на основе записей данных формируют иерархические хэш-структуры (например, дерево Меркла [5]), что позволяет проверять наличие записи без загрузки всего блока целиком. Иногда, для оптимизации поиска, одни записи хранят ссылки на другие, ассоциированные с ней.

Активно используют электронную цифровую подпись. При этом, ключ проверки подписи или хэш-код от него используют в качестве идентификатора пользователя. Удостоверяющие центры противоречат принципу децентрализации, и в настоящее время их не используют (хотя технических препятствий этому нет).

Новые блоки формируются по мере накопления данных. Делать это может любой желающий – участники параллельно работают над формированием следующего блока, а системой выбирается один из них (например, первый сформированный). Как правило, за сформированный блок, принятый системой, участник получает вознаграждение.

Поскольку для распространения вновь созданных блоков требуется ненулевое время, обычная ситуация – когда в системе начинают формироваться несколько версий цепи. В таких случаях, в конечном итоге, пользователи выбирают цепь, сформировать которую было сложнее. На практике, это может быть выбор более длинной ветви.

Чтобы препятствовать злоупотреблениям в распределённых системах используют разные подходы.

Один из распространённых вариантов – Proof Of Work (англ. – доказательство работы) – требовать от составителя блока выполнения достаточно сложных вычислений. Например, вводят требования для получившегося хэш-кода блока, так, что участники вынуждены перебирать значение служебных полей пока не получат блок с хэш-кодом, удовлетворяющим условию.

Другой распространённый вариант – Proof Of Stake (англ. – доказательство владения/доли) – выбирать блок с учётом статуса в системе сформировавшего его участника. Например, в системах электронных денег – участник, готовый заблокировать на какое-то время большую сумму, имеет приоритет при формировании нового блока.

Во обоих вариантах существует некоторая вероятность, что недобросовестному участнику удастся сформировать «мошенническую ветвь», которая в итоге будет признана другими. Однако, считается, что для участников с небольшими долями всех ресурсов эта вероятность ничтожно мала, а участникам со значительной долей не выгодно подрывать доверие к системе. При дискредитации системы, последние либо теряют возможность получать вознаграждение за новые блоки (доказательство работы), либо обесценивают свои активы (доказательство владения).

По факту, электронные деньги (криптовалюта) является частью практически всех блокчейн-систем – даже тех, которые ориентированы на решение других задач – то есть, помимо алгоритмической защиты, в блокчейн-системах распространена и экономическая мотивация для сохранения достоверности данных.

В настоящее время активно ведутся разработки и апробация других вариантов достижения консенсуса по новым блокам. Разрабатываются также и многоуровневые системы (с привилегированными участниками).

Количество потенциальных сфер применения блокчейн-системы – огромно. Вот лишь некоторые из них: электронные деньги (криптовалюта), реестры (акционеров, учредителей, имущества, присвоенной квалификации, налоговый учёт, регистрация авторских и других прав, другие государственные услуги), протокольные записи (аудио, видео) с подтверждением времени, системы голосования, часть инфраструктуры Интернета вещей.

Мониторинг и анализ вакансий доступных посредством сети Интернет в течение февраля 2017 года, показал, что в настоящее время на рынке труда остро требуются специалисты, не только понимающие принципы работы таких систем, но и способные их разрабатывать и реализовывать. При этом образовательные проекты в области блокчейн-технологий в настоящее время активно действуют пока лишь в двух российских вузах (МФТИ и ВШЭ).

Подобные системы достаточно сложны в реализации, поэтому новые практически всегда создаются на базе уже имеющихся и/или с использованием специализированных программных библиотек. Блокчейн-системы, код и описание которых доступны посредством сети Интернет, в большей своей части реализованы на языке C++, в коде активно используются возможности стандарта 2011 г. и библиотека boost.

Таким образом, для качественной работы над блокчейн-системой в настоящее время требуются:

- понимание основ программирования;
- знание основ проектирования и архитектуры программных систем;
- владение языком программирования C++ на высоком уровне;
- понимание основ программирования в сетях связи;

– понимание основ криптографии и систем с открытым ключом;
– понимание непосредственно принципов работы блокчейн-систем.

Всё это делает обучение разработке блокчейн-систем в настоящее время доступным лишь студентам, владеющим навыками программирования на высоком уровне. Очень желательны предварительные знания в областях сетей связи и/или информационной безопасности.

Но с учётом интереса к технологии, в том числе и со стороны лидеров рынка информационных технологий, таких как Microsoft, IBM, Intel, в скором времени можно ожидать распространение инструментария, который позволит существенно снизить порог вхождения. Вероятно, требования к набору компетенций разработчика блокчейн-систем в ближайшем будущем необходимо будет регулярно пересматривать.

Следует отдельно отметить активное развитие так называемых «умных контрактов», реализуемых на базе блокчейн-технологий. Записью в таких системах является «код», который выполняется системой при наступлении определённых событий. В настоящее время активно набирают популярность платформы для «умных» контрактов, и языки их программирования (например, *Ethereum* и *Solidity*, соответственно). Уже заметен спрос на разработчиков, владеющих такими языками, и, судя по всему, в скором будущем курсы разработки умных контрактов станут очень актуальны.

Список используемых источников

1. Don Tapscott, Alex Tapscott. Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World [Электронный ресурс] // Интернет-портал amazon.com. URL: https://www.amazon.com/Blockchain-Revolution-Technology-Changing-Business/dp/1511357665 (дата обращения 30.03.2017).

2. Новости «Греф, Кудрин и Чубайс заглянули в будущее индустриальной революции» 22.01.16 (обновлено: 05.02.2016) [Электронный ресурс] // Сайт «РИА Новости». URL: https://ria.ru/economy/20160122/1363470152.html (дата обращения 30.03.2017).

3. Поручение Председателя Правительства Дмитрия Медведева по вопросу о возможности применения технологии блокчейн в системе государственного управления и экономике Российской Федерации [Электронный ресурс] // Официальный сайт Правительства РФ. 06.03.2017. URL: http://government.ru/orders/selection/401/26653/ (дата обращения 30.03.2017).

4. Коржик В., Яковлев В. Основы криптографии: учебное пособие. СПб. : Интермедия, 2016. 295 с. ISBN 978-5-89160-097-3.

5. Патент США US4309569 [Электронный ресурс] // Сайт Google, Inc. «Поиск по патентам». URL: https://www.google.com/patents/US4309569 (дата обращения 30.03.2017).

Статья представлена заведующим кафедрой, кандидатом технических наук, профессором Л. Б. Бузюковым.

УДК 621.3.052.9

ВЫБОР ЭЛЕМЕНТНОЙ БАЗЫ ДЛЯ РЕАЛИЗАЦИИ СИСТЕМ ПЕРЕДАЧИ ДАННЫХ ПРИ ПОМОЩИ ВИДИМОГО СВЕТА

И. В. Гришин, А. С. Дюбов, В. А. Хричков, Т. Р. Ялунина

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

В настоящее время технология передачи данных при помощи видимого света рассматривается как один из возможных способов решения надвигающейся проблемы дефицита спектра радиочастот, статье исследуются технические параметры основных функциональных элементов, входящих в состав систем передачи данных при помощи видимого света.

системы передачи при помощи видимого света, технология VLC, Li-Fi, RGB-светодиоды.

В настоящее время системы передачи данных при помощи видимого света (СПВС) являются перспективной технологией, позволяющей решить актуальную проблему кризиса спектра радиочастот. Однако, на сегодняшний день, СПВС нигде в мире не внедрены в эксплуатацию, а потому не имеют готовой элементной базы (ЭБ). Это порождает необходимость изучения рынка, исследования доступной ЭБ на возможность применения в СПВС и выбора подходящих образцов, что и является целью данной работы.

Рассмотрим блоки передачи и СПВС по отдельности.

Передатчики

В технологии СПВС роль источника оптического сигнала выполняют белые светодиоды (СИД).

На сегодняшний день существует два способа получения белого света с помощью светодиодов: RGB-СИД и люминофорные СИД.

Белые люминофорные СИД предпочтительны с т. з. цветопередачи и энергоэффективности, однако использование люминофора в конструкции сильно увеличивает его инерционность, из-за чего добиться высокого уровня быстродействия, не используя синий фильтр для подавления медленного желтого излучения, не представляется возможным. В связи с этим, в рамках технологии СПВС, преимущество за RGB-СИД. Физически это три

СИД (красный, зеленый, синий) под общей линзой. Принцип их работы основывается на том, что при одновременном излучении на трех длинах волн, соответствующих указанным выше цветам, человеческий глаз воспринимает излучение как белое (рис. 1).

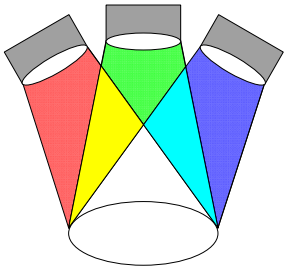


Рис. 1. Принцип действия RGB-СИД

При этом технология СПВС дает возможность передавать информацию параллельно на каждой несущей и таким образом увеличить полосу пропускания системы, которая будет складываться из ПП синего, зеленого и красного СИД.

Из многообразия СИД, представленных на рынке, для исследования были выбраны три образца RGB-СИД, характеристики которых указаны в таблице 12 [1, 2, 3].

ТАБЛИЦА 1. Основные характеристики исследуемых СИД

Название	λ, нм	V_f, В	Iv, мкд	FOV	I_f, мА
BetluxElectronics BL-L515RGBW-CC	630 (R)	2,10	500	±60°	30
	525 (G)	3,50	600		
	430 (B)	3,50	300		
Foryard Optoelectronics FYLS-5050RGBC	630 (R)	2,60	500	±60°	20
	525 (G)	3,60	1300		
	468 (B)	3,60	250		
Arlight ARPL-3W RGB/6-pin	630 (R)	2,60	83215	±45°	350
	520 (G)	3,40	125032		
	460 (B)	3,40	21326		

Первые два образца являются индикаторными, и для их применения в системах освещения требуется очень большое количество излучателей. К тому же, как выяснилось, первый СИД не позволяет передавать сигнал на трех длинах волн единовременно, что компенсирует преимущество от применения данного типа СИД.

Третий образец отличается от первых двух в первую очередь передаваемой мощностью, которая достигает 3 Вт в сравнение с 60 мВт предыдущих. В дополнение, он имеет наименьшее поле видимости, что является преимуществом для организации оптических точек доступа. По этим причинам данный СИД был принят подходящим для дальнейших исследований.

Частотные характеристики СИД определяются передаточной функцией, которая выглядит следующим образом [4]:

$$H_{\text{СИД}}(f) = (1 + j2\pi f\tau)^{-1}, \quad (1)$$

где $\tau = R_{\text{СИД}} \cdot C_{\text{СИД}}$ – постоянная времени; $R_{\text{СИД}}$ и $C_{\text{СИД}}$ – собственные сопротивление и емкость СИД; j – мнимая единица.

Исходя из (1), путем математических преобразований, полоса пропускания СИД рассчитывается по формуле [4]:

$$\Delta f = \frac{0,35}{\tau_{\text{н}}}, \quad (2)$$

где $\tau_н = \tau \cdot \ln 9$ – время нарастания импульса СИД.

В связи с тем, что СИД, которые рассматриваются в настоящей работе, изначально не имели отношения к системам связи, в технической документации на них отсутствуют необходимые параметры. Это породило необходимость их получения эмпирическим путем.

Таким образом, с помощью осциллографа были получены данные о времени нарастания импульса, среднее из которых для СИД Arlight ARPL-3W RGB/6-pin составило 8 нс, а полоса пропускания, согласно формуле (2) – 43 МГц.

Приемники

Возможная схема цепи приема представлена на рис. 2. В нее входят: 1 – фотодиод (ФД), 2 – трансимпедансный операционный усилитель (ТИОУ), 3 – фильтр верхних частот (ФВЧ), 4 – устройство восстановления сигнала AND 2807, состоящее из операционного усилителя с автоматической регулировкой уровня и блока восстановления данных, 5 – микроконтроллер для обработки сигнала.

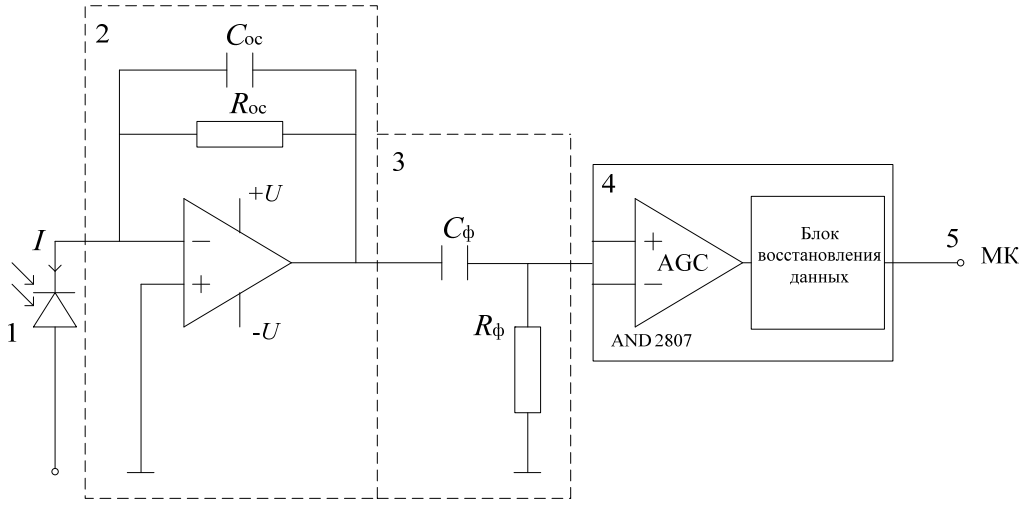


Рис. 2. Схема приема оптического сигнала

Приемниками оптического сигнала являются ФД, которые преобразуют попавший на его светочувствительную область свет в выходной электрический сигнал.

С этой целью, для исследования были выбраны датчики цвета двух разных фирм: TAOS TCS3200 и HAMAMATSU S9702. Основные их характеристики представлены в таблице 2 [5, 6].

ТАБЛИЦА 2. Характеристики исследуемых датчиков цвета

Название	λ, нм	*S*, А/Вт	T_{rise}, нс	Δ*f*, МГц
TAOSTCS3200	470 (R)	0,85	100	3,5
	524 (G)	0,5		
	640 (B)	0,48		
HAMAMATSUS9702	460 (R)	0,18	100	3,5
	540 (G)	0,23		
	620 (B)	0,16		

Первым исследуемым образцом был датчик цвета компании TAOS.

Это фотоприемное устройство (ФПУ) имеет массив ФД, встроенный ТИОУ и конвертер тока в частоту на монолитной интегральной схеме. Выходным сигналом является частота, прямо пропорциональная интенсивности падающего на светочувствительные площадки фотодиодов излучения.

Первым существенным недостатком этого ФПУ является отсутствие возможности использовать все три фильтра одновременно. К тому же, при проведении исследования было выявлено, что фильтры имеют слишком широкую полосу пропускания, что приводит к переходным помехам между соседними длинами волн. Эти два критерия и отсутствие возможности однозначного установления зависимости между выходным сигналом и входным, не позволяют использовать это ФПУ в исследуемых системах связи.

Второе ФПУ компании HAMAMATSU на данный момент не исследовано, в связи с невозможностью его использования без ТИОУ. Однако, это устройство обладает хорошими характеристиками и возможно является подходящим образцом для использования в СПВС.

После преобразования оптического сигнала в электрический необходимо произвести его усиление. С этой целью в цепи приема после фотодиода стоит ТИОУ. Это устройство позволяет усиливать сколь угодно маленький фототок.

В рамках настоящей работы было выбрано несколько ТИОУ, однако, в связи с малым коэффициентом прочих, подходящим был принят один ТИОУ – LTC 6268, характеристики которого представлены в таблице 3 [7]. К сожалению, на сегодняшний день, данный образец еще не исследован.

ТАБЛИЦА 3. Характеристики исследуемого ТИОУ

Название	Полоса пропускания, $\Delta f_{\text{ТИОУ}}$, МГц	Коэффициент усиления, $G_{\text{ТИОУ}}$, Ом	Спектральная плотность шумов, i_n, А/Гц$^{1/2}$
LTC 6268	350	∞	$5{,}3 \times 10^{-15}$ (B_{eff} = 100 кГц)

Следующим звеном в цепи приема является ФВЧ (см. рис. 2). Он необходим для отсечения всего немодулированного излучения. Посторонние источники света имеют относительно низкую частоту по сравнению с частотой, используемой передатчиком.

Чтобы избежать искажения переданных данных, фильтр разработан с относительно низкой частотой отсечки. В противном случае сигнал может быть искажен и его будет трудно обработать. Выбранные значения являются компромиссом между удалением шума и минимизацией искажений и составляют: для сопротивления, $R_{\text{ф}}$ – 10 кОм, для емкости, $C_{\text{ф}}$ – 100 мкФ. Частота отсечки на уровне –3 дБ определяется формулой [8]:

$$f_{\text{ср}} = \frac{1}{2\pi R_{\text{ф}} C_{\text{ф}}} = \frac{1}{2\pi \cdot 10 \cdot 10^{3} \cdot 100 \cdot 10^{-9}} = 159 \text{ Гц}.$$

После подавления низкочастотных составляющих сигнал поступает на устройство восстановления сигнала AND 2807, которое состоит из операционного усилителя с автоматической регулировкой уровня и блока восстановления данных, а далее – на микроконтроллер, где происходит цифровая обработка сигнала.

Таким образом, на сегодняшний день технология СПВС находится на стадии изучения. Пока что можно формулировать выводы только по исследованным нами образцам. В связи с тем, что приобрести ЭБ в России зачастую не получается, возникает необходимость заказывать из-за границы, что не позволяет проводить исследования в непрерывном режиме. Однако работы над этой темой активно ведутся и можно надеяться, что в скором времени будут получены существенные результаты.

Список используемых источников

1. Product Specification [Электронный ресурс] // Foryard Optoelectronics. URL: http://www.foryard-led.ru/pdf/fyls-5050rgbc.pdf (дата обращения 30.03.3017).

2. BL-L515RGBW-CC [Электронный ресурс] // Betlux Electronics. URL: https://lib.chipdip.ru/285/DOC000285587.pdf (дата обращения 30.03.3017).

3. ARPL-3W RGB/6-pin [Электронный ресурс] // Arlight. URL: http://www.platan.ru/pdf/datasheets/arlight/ARPL_Emitter_3W_RGB.pdf (дата обращения 30.03.3017).

4. Шуберт Ф. Светодиоды. 2-е изд. М. : ФИЗМАТЛИТ, 2008. 500 с.

5. TCS3200 [Электронный ресурс] // TAOS. URL: http://www.mouser.com/catalog/specsheets/TCS3200-E11.pdf. (дата обращения 30.03.3017).

6. S9702 [Электронный ресурс] // HAMAMATSU. URL: https://www.hamamatsu.com/resources/pdf/ssd/s9702_kspd1071e.pdf. (дата обращения 30.03.3017).

7. LTC6268/LTC6269 [Электронный ресурс] // Linear Technology. URL: http://cds.linear.com/docs/en/datasheet/62689f.pdf. (дата обращения 30.03.3017).

8. Arnon, Shlomi. Visible Light Communication. Negev : Cambridge University Press, 2015. ISBN: 978-1-31623-477-8.

УДК 004.021

ИССЛЕДОВАНИЕ ОСОБЕННОСТЕЙ АЛГОРИТМОВ РАСПОЗНАВАНИЯ ЛИЦ НА ПРИМЕРЕ БИБЛИОТЕКИ КОМПЬЮТЕРНОГО ЗРЕНИЯ

В. В. Громов, В. С. Елагин

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

В статье рассматриваются возможности алгоритмов распознавания лиц на основании существующих систем, которые включают в себя ПО, SDK и компьютерные библиотеки. На примере библиотеки компьютерного зрения OpenCV рассматриваются принципы работы четырех алгоритмов распознавания лиц, а также даются рекомендации для внедрения систем распознавания лиц.

распознавание лиц, MegaFace, OpenCV, Viola-Jones object detection, Eigenfaces, Fisherfaces, Local Binary Patterns Histograms.

Введение

В настоящее время происходит активное внедрение систем, использующих возможности компьютерного зрения. Широкое распространение получили разработки с функцией распознавания лиц для определенных задач, начиная с развлекательных сервисов и заканчивая системами для проведения розыскных мероприятий. Следует отметить, что двухмерные алгоритмы распознавания лиц по точности уступают другим биометрическим методам идентификации личности, такие как радужная оболочка глаза, рисунок вен и трехмерная идентификация лица. Однако методы распознавания лиц по двухмерному изображению получили широкое распространение в применении, поскольку изображения лиц являются наиболее распространенной информацией и стоимость систем распознавания лиц относительно невелика [1].

Возможность обрабатывать большие объемы данных с высокой точностью демонстрирует мировой чемпионат алгоритмов распознавания лиц MegaFace Benchmark [2]. Задача соревнования заключается в следующем: необходимо распознать 100 000 изображений с 530 различными лицами на наборе для обучения, который содержит 1 000 000 изображений с 690 000 различными лицами. Результаты 2016 г. представлены в таблице 1.

ТАБЛИЦА 1. Точность распознавания лиц по результатам MegaFace Benchmark

Место	Алгоритм	Точность, %	Страна
1	**Vocord-deepVo1.2**	**80,2**	**Россия**
5	Deepsense – Large	74,8	Америка
6	SIATMMLAB TencentVision	74,2	Китай
7	Shanghai Tech	74,0	Китай
8	**NTechLAB – facenx_large**	**73,3**	**Россия**
10	Google – FaceNet v8	70,5	Америка
18	**LBP OpenCV (*Small database*)**	**2,3**	**Америка**

Существующие российские системы с функцией распознавания лиц

Компания NTechLab (8 место) в 2016 г. представила сервис FindFace, который позволяет по сделанной фотографии снятого человека найти аккаунт в сети ВКонтакте. Компания Vocord (1 место) предоставляет системы компьютерного зрения для ЧОП и правоохранительных органов. Представленная разработка Vocord FaceControl применяется на железнодорожных вокзалах, частных учреждениях и внедряется в метрополитене. Компании 1С и NTechLab (8 место) и в 2017 г. представили систему Битрикс Face-Трекер, которая позволяет распознавать посетителей магазина и выводить о них информацию.

Выбор библиотеки компьютерного зрения

Множество SDK и компьютерных библиотек позволяют решить задачу распознавания лиц, в которую входит поиск (локализация) лица на изображении, и непосредственно идентификация лиц по найденному лицу. Это и коммерческие библиотеки, и SDK, например, Findface Cloud API, Vocord Face Control SDK и свободные (табл. 2), точность которых уступает коммерческим разработкам.

Отметим, что высокую точность можно получить при использовании совместно библиотек OpenFace + DLib Library [3]. В данной работе исследуется библиотека OpenCV, алгоритмы которой представлены ниже.

ТАБЛИЦА 2. Популярные Open Source библиотеки для распознавания лиц

Библиотека	Алгоритмы поиска лица (локализация)	Алгоритмы идентификации
OpenCV	Метод Виолы-Джонса	Eigenfaces, Fisherfaces, Local Binary Patterns Histograms
OpenFace	Отсутствуют	Google FaceNet – принцип работы
DLib C++ Library	Histogram of oriented gradient (HOG) object detector	Отсутствуют

Особенности алгоритмов распознавания лиц в библиотеке OpenCV

Рассмотрим принципы алгоритма Виолы-Джонса для поиска лица на изображении, описанный в 2001 г. Полом Виолой и Майклом Джонсом [4].

Интегральное представление изображения используется для быстрого расчета яркости прямоугольной фигуры.

Принцип скользящего окна: на изображении перемещается «окно» в разных масштабах. В случае нахождения лица в области алгоритм выдает координаты окна, в котором обнаружено лицо.

Примитивы Хаара: «форма», в которой вычисляется яркость изображения. Из яркости изображения, находящейся в белой части фигуры, вычитается яркость из черной части. По вычисленному числу и расположению примитива можно проанализировать наличие или отсутствие лица на изображении. При поиске лиц задействуется множество примитивов Хаара на разных позициях. Простейший пример с наложением примитивов (рис., *а*).

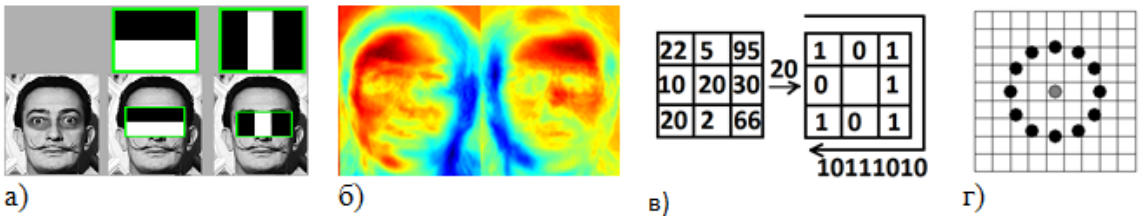


Рисунок. Иллюстрации к алгоритмам: а) наложение примитивов Хаара; б) кодировка изображения в Eigen Faces при различном освещении; в) двоичное представление окрестности пикселя в операторе ЛБШ; г) круговая окрестность пикселя в расширенном операторе ЛБШ

Слабый классификатор: функция, угадывающая присутствие объекта (лица) более чем в 50 % случаев по расположенным примитивам Хаара. Коэффициенты и позиции примитивов для слабого классификатора определяются в процессе машинного обучения алгоритма.

Сильный классификатор: функция, выдающая данные о присутствии объекта, которая состоит из *N* слабых классификаторов. Для создания сильных классификаторов используется процедура обучения AdaBoost. Метод AdaBoost позволяет из слабых классификаторов построить точный сильный классификатор, причем точность зависит от числа *N*. Каскад классификаторов: состоит из сильных классификаторов, которые используются в зависимости от масштаба скользящего окна.

Библиотека OpenCV предоставляет обученные каскады Хаара, которые позволяют обнаружить на изображении: анфас или профиль лица, глаза, фигуру человека (полностью, верхнюю или нижнюю часть тела), улыбку, автомобильные номера и т. д. Разработчик может использовать готовые каскады Хаара и тогда обучать алгоритм не требуется.

Преимущества алгоритма Виолы-Джонса: высокая точность и скорость работы, возможность обнаружения нескольких лиц под углом до 30 град., определяет лицо в разных профилях, применяется во встраиваемых системах. Недостатки: длительная процедура обучения каскадов Хаара (обычно не требуется обучение), может дублироваться одно лицо со смещением из-за масштаба и перемещения окна, алгоритм находит объекты только «одной природы», не обнаруживает раскрашенные лица.

Рассмотрим метод для идентификации найденных лиц **EigenFaces**, который использует метод анализа главных компонент – **P**rincipal **C**omponent **A**nalysis [5].

Обучение алгоритма **EigenFaces** происходит следующим образом.

Изображение с лицом с разрешением $K \times K$ пикселей преобразуется в вектор с длиной K^2 путем объединения строк картинки. *N* изображений для обучения алгоритма в виде вектора объединяются в матрицу A с размером $K^2 \times N$, где столбцами матрицы являются вектора изображений. В матрице A вычисляется «средний» вектор с длиной K^2, в котором хранятся схожие особенности векторов изображений. Далее из каждого столбца вычитается средний вектор для нормализации изображения и сохранения только уникальная информация для каждого изображения.

Следующим шагом является переход в новый базис B, в котором сохраняется информация по осям с большей дисперсией, т. е. с наибольшими различиями: вычисляется ковариационная матрица, находятся главные компоненты (они же собственные вектора) и считаются веса. На выходе получаются числа (веса) для каждого изображения в обучающей выборке, которые потребуются для идентификации.

Идентификация лица по изображению происходит следующим образом.

Входное изображение приводится к размерам $K \times K$. Затем переводится изображение в вектор с нормализацией изображения (вычет среднего вектора), проецируется изображение в пространство собственных векторов

В, определяются весы векторов входного изображения, и находится минимальное расстояние между полученными весами векторов входного изображения и ближайшими весами изображений из обучающей выборки. На основании минимального расстояния идентифицируется лицо, либо констатируется, что лицо не распознано.

Недостатком метода *EigenFaces*, когда анализируются различия между всеми изображениями, является то, что зачастую кодируются особенности освещения. На рисунке (*б*) показано, как алгоритм видит одно лицо при разном освещении. Таким образом, метод не устойчив к смене освещения.

Принцип работы алгоритма **Fisherfaces** (основан на методе линейного дискриминантного анализа ***L**inear **D**iscriminant **A**nalysis*) схож с EigenFaces.

Однако метод **Fisherfaces** сохраняет только схожую информацию среди изображений, которые относятся к одному лицу, а затем сохраняется информация только о различиях лиц. Данная особенность делает алгоритм *FisherFaces* более устойчивым к смене освещения [6].

Алгоритм идентификации обнаруженных лиц **Local Binary Patterns Histograms** (**LPBH**) использует оператор **Л**окальных **Б**инарных **Ш**аблонов (ЛБШ) и является устойчивым к смене освещения.

На рисунке (*в*) представлен оператор ЛБШ, представляющий собой описание окрестности пикселя в двоичном представлении. В пикселе, где интенсивность выше или равна интенсивности центрального пикселя – ставится 1, где меньше – 0. По окрестности пикселя можно составить бинарный код, который будет результатом применения ЛБШ. В OpenCV используются расширенные операторы ЛБШ, имеющие круговую окрестность с радиусом R (рис., *г*).

Алгоритм LBPH [7] делит входное изображение на N равных квадратных частей. Для каждой части изображения хранится *K*-значений, количество которых задается количеством возможных кодов оператора ЛБШ. Каждое значение хранит в себе информацию: сколько раз в области встречен определенный код. Внутри каждой области строится гистограмма по кодовым значениям. Далее полученные вектора гистограмм объединяются в один вектор, хранящий в себе все гистограммы областей. Для идентификации лица сравниваются полученные вектора, и находится наименьшее расстояние между гистограммами входного изображения и содержащихся изображений в обучающей выборке. На основании минимального расстояния идентифицируется лицо.

Заключение

С использованием библиотеки OpenCV для распознавания лиц рекомендуется использовать методы Виолы-Джонса и FisherFaces либо LPBH.

Для повышения точности можно использовать библиотеку OpenFace, принцип работы которой основан на нейронных сетях. В результате работы была исследована тематика распознавания лиц. Дальнейшим развитием работы является исследование алгоритмов распознавания лиц, основанных на нейронных сетях.

Список используемых источников

1. Современные методы идентификации [Электронный ресурс]. URL: https://habrahabr.ru/post/126144 (дата обращения 04.04.2017).

2. Сайт чемпионата MegaFace. URL: http://megaface.cs.washington.edu (дата обращения 20.01.2017).

3. Сайт OpenFace. URL: https://cmusatyalab.github.io/openface (дата обращения 20.01.2017).

4. Азаров Д. Метод распознавания лиц Виолы-Джонса (Viola-Jones) [Электронный ресурс]. URL: https://oxozle.com/2015/04/11/metod-raspoznavaniya-lic-violy-dzhonsa-viola-jones (дата обращения 04.04.2017).

5. Распознавание изображений. Алгоритм Eigenfaces [Электронный ресурс]. URL: https://geektimes.ru/post/68870 (дата обращения 04.04.2017).

6. Face Recognition with OpenCV. URL: http://docs.opencv.org (дата обращения 04.04.2017).

7. Петрук В. И., Самородов А. В., Спиридонов И. Н. Применение локальных бинарных шаблонов к решению задачи распознавания лиц // Вестник МГТУ им. Баумана. 2011. С. 58-63.

УДК. 621.396

МЕТОДЫ ОРГАНИЗАЦИИ СЕТИ СВЯЗИ НА БАЗЕ БЕСПИЛОТНОГО ЛЕТАТЕЛЬНОГО АППАРАТА

Ч. Н. Дао, А. И. Парамонов

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

В статье приводятся методы организации сети связи на базе беспилотных летательных аппаратов. Рассмотрены основные варианты выбора головного узла группы БПЛА для различных способов организации сети. В статье рассматривается применение алгоритма кластеризации Forel для решения задачи кластеризации. Так же в статье рассмотрены модели, разработанные в пакете Mathcad, и результаты их использования для выбора оптимального способа организации сети БПЛА.

беспилотные летающие аппараты, централизованные связи, децентрализованная сеть.

В последние годы интенсивно развиваются технологии построения беспилотных летательных аппаратов (БПЛА) и расширяется область их применения. БПЛА широко используются как в задачах военного характера, так и для решения задач гражданского назначения (разведчики, мишени, экология сельское хозяйство, управление транспортными потоками на автотрассах и т. д.). БПЛА может управляться дистанционно с помощью оператора или независимо друг от друга с помощью контроллера, установленного на нем. Иногда, чтобы решить поставленную задачу, необходимо использовать более одного БПЛА. При этом необходимо иметь возможность обеспечивать эффективную связь между БПЛА в группе. В общем случае БПЛА могут двигаться с разной скоростью и по различным траекториям. Поэтому выбор головного узла группы БПЛА для различных способов организации сети на базе БПЛА является важной задачей.

Сеть БПЛА, обычно, рассматривается как подвижная ad hoc сеть и называется FANET сетью, она является особой формой сетей MANET и VANET. Сеть FANET имеет отличные от упомянутых сетей характеристики с точки зрения подвижности узлов, их плотности, частоты изменения топологии, условий распространения радиоволн, потребляемой мощности, вычислительной мощности и локализации узлов, по сравнению с другими формами ad-hoc сетей. В связи с этим имеют отличия и задачи обеспечения связи в FANET. Сети FANET могут быть использованы для многих типов приложений, и могут осуществлять доставку различных типов данных, которые включают в себя данные о местоположении GPS, потоковое видео, звук, изображения, текстовые сообщения и т. д. В задачах обслуживания большой площади может потребоваться использование множества БПЛА, причем это количество может изменяться в процессе выполнения задачи. Поэтому необходимо использовать алгоритмы для координации группы БПЛА. Для FANET, как и для большинства сетей связи, важно поддерживать уровень качества услуг, таких параметров как задержка, пропускная способность, джиттер, потеря пакетов и т. д. Поэтому важной задачей является определение методов выбора общей структуры сети для обеспечения QoS, с учетом высокой мобильности и динамичной структуры FANET [1].

Специфические требования прикладных задач приводят к проблемам при проектировании сети и ограничении связи. Эти требования касаются типа трафика, его объема, частоте, задержке доставки, толерантности к задержке или потерям, дальности связи, эффекту мобильности, плотности сети, и энергетическим ограничениям [2]. В FANET, из-за высокой скорости движения БПЛА, качество связи и топология сети могут относительно быстро измениться. Степень подвижности узла является относительно высокой. В среднем, БПЛА имеет скорость 30–460 км/ч [1].

В связи с этим значительный интерес представляет задача обеспечения и поддержания эффективной связи между БПЛА в группе. В общем случае БПЛА могут двигаться с разной скоростью и по различным траекториям, что представляет очевидные сложности обеспечения непрерывной связи между ними. Топология сети БПЛА с числом узлов и связей, а также изменяющихся относительных положений узлов. Поэтому, обеспечения связи между узлами такой сети требуется выбора подходящей сетевой архитектуры.

Рассмотрим две основных архитектуры построения сети связи для группы БПЛА, такие как централизованная и децентрализованная сети и их комбинации [3]. На рис. 1. схематично изображены архитектуры сетей для централизованного способа построения рис. 1*а*, децентрализованного рис. 1*б* и комбинированного рис. 1*в* и рис. 1*г*.

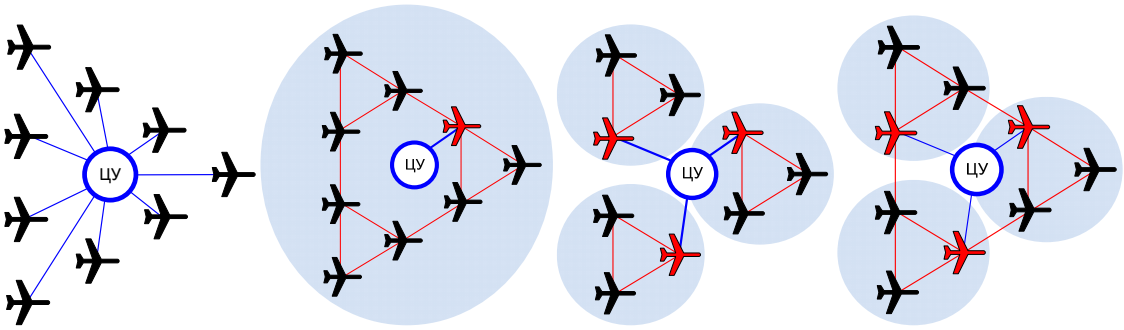


Рис. 1. Способы организации сети БПЛА: а) централизованный; б) децентрализованный (ad hoc сеть); в) и г) комбинированные способы (многогрупповой и многослойный способы)

Чтобы сделать выбор подходящей сетевой архитектуры и головного узла группы БПЛА, используются алгоритмы кластеризации Forel. Модель разработана в системе Mathcad. Рассмотрим пример, в котором используются 400 узлов сети, которые распределяются случайным образом на некоторой заданной территории. Для решения задачи кластеризации определяется радиус кластера, он будет радиусом поиска локальных сгущений узлов (в примере $R = 7$). Результатом выполнения алгоритма Forel, является выделение несколько кластеров.

В результаты моделирования приведены на рис. 2. Из данного рисунка видно, что использование алгоритма Forel позволило выделить в исходном множестве узлов (БПЛА) 14 групп БПЛА с разными плотностями узлов. Используя данное решение могут быть выбраны головные узлы кластеров в каждой из выделенных групп (рис. 3).

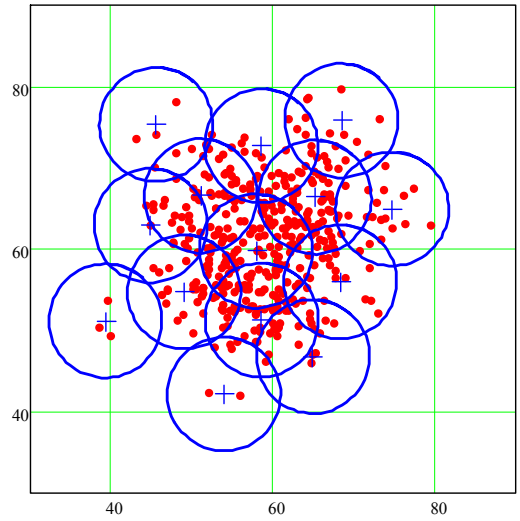


Рис. 2. БПЛА сформированы в 14 группы

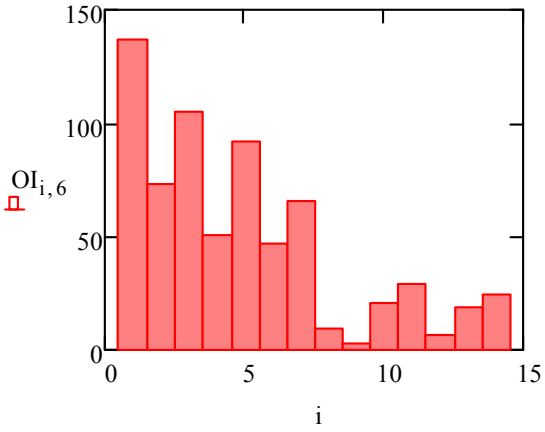


Рис. 3. Плотность БПЛА в каждой группе

Для групп с малым количеством БПЛА, если они расположены рядом с центром управления, можно применить централизованную архитектуру. В этом случае, все БПЛА подключаются непосредственно к центру управления и все связи между БПЛА организуются маршрутами через наземную станцию.

Для групп с большим количеством БПЛА, если они расположены далеко от центра управления, можно применить децентрализованную архитектуру. В этой сети, выделяется головной БПЛА (головной узел кластера), который служит шлюзом ad-hoc-сети. Через него передаются все данные между наземной станцией и другими БПЛА. Узлы, которые находятся в центре кластера, будут устанавливать связь с головным узлом и имеют возможность транзита трафика других узлов к центру управления по кратчайшему маршруту.

Надо отметить, что в реальной сети, кратчайший (наименее протяженный) маршрут может оказаться не оптимальным из-за условий распространения сигнала и нагрузки на каналы связи. В этом случае целесообразно рассматривать набор из нескольких альтернативных маршрутов. Длины кратчайшего маршрута в сети, образованной узлами, которые случайным образом распределены в трехмерном пространстве и образуют так называемое Пуассоновское поле.

Кратчайший маршрут определяется как маршрут с минимальной суммой длин каналов (участков) между образующими его узлами сети, с учетом радиуса связи узла. Полагаем, что радиус связи узла меньше размера области обслуживания $R < H$. В противном случае все кратчайшие маршруты будут равны расстоянию между узлами и будут состоять из одного хопа [4].

Таким образом, за счет использования алгоритмы кластеризации Forel с помощью программного обеспечения Mathcad полученные в работе результаты дают возможность выбирать оптимальный способ организации сети БПЛА.

Выводы

1. Для построения сети БПЛА, как правило, следует исходить из некоторого ограниченного количества способов размещения БПЛА в пространстве, т.е. организации группы.

2. С учетом наиболее распространенных способов размещения БПЛА в пространстве, для выбора структуры сети БПЛА могут быть использованы известные методы кластеризации, позволяющие выделять группы по плотности узлов, связности, расстоянию от центра и др.

3. Использование метода кластеризации Forel позволяет выделять кластеры по признаку расстояния от центра кластера до узлов сети. Алгоритм также позволяет находить головные узлы кластера (ближайший к центру масс кластера).

4. Приведенный пример моделирования кластеризации сети с помощью алгоритма Forel показал, что данный алгоритм формирует кластеры из локальных групп (сгущений) узлов. Размер кластера может быть задан параметром R (размер кластера), выбираемым исходя из соображений доступности и качества связи.

5. Формируемые с помощью алгоритма Forel кластеры имеют различную плотность (количество) узлов. Поэтому при его применении необходимо учитывать эту особенность.

Список используемых источников

1. Naveen and Sunil Maakar. Concept of Flying Ad-hoc Network: A Survey // National Conference on Innovative Trends in Computer Science Engineering (ITCSE-2015), pp. 178–182.

2. Hayat, Samira, Evşen Yanmaz, and Raheeb Muzaffar. Survey on unmanned aerial vehicle networks for civil applications: A communications viewpoint // IEEE Communications Surveys & Tutorials 18.4 (2016): 2624–2661.

3. Дао Ч. Н., Парамонов А. И. Анализ структуры сетей связи на базе беспилотных летательных аппаратов // DCCN-2016. Ноябрь 2016. С. 92–100.

4. Dao N., Andrey Koucheryavy, and Alexander Paramonov. Analysis of routes in the network based on a swarm of UAVs // Information Science and Applications (ICISA) 2016. Springer Singapore, 2016. PP. 1261–1271.

УДК 004.056

ПОДХОД К ОЦЕНКЕ КИБЕРУСТОЙЧИВОСТИ НА ОСНОВЕ ТОПОЛОГИЧЕСКОГО ПРЕОБРАЗОВАНИЯ СТОХАСТИЧЕСКИХ СЕТЕЙ

В. А. Десницкий[1,2], И. В. Котенко[2], О. С. Лаута[2], И. Б. Саенко[2]

[1]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
[2]Санкт-Петербургский институт информатики и автоматизации Российской академии наук

Предлагается метод оценки киберустойчивости компьютерных сетей, основанный на аналитическом моделировании компьютерных атак с помощью стохастических сетей и их последующем топологическом преобразовании. Предлагаются показатели и аналитические выражения для оценки киберустойчивости. Обсуждаются результаты экспериментальной оценки предложенных моделей и метода. Формулируются предложения по поиску мер противодействия компьютерным атакам, приводящие к повышению киберустойчивости компьютерных сетей.

кибербезопасность, моделирование атак, киберустойчивость компьютерной сети, компьютерные атаки, устойчивость, стохастические сети, преобразование Лапласа.

Современный период развития информационных и телекоммуникационных технологий характеризуется возрастанием угроз безопасности компьютерных сетей (КС), что обусловлено, с одной стороны, резким ростом количества компьютеров и сетевых элементов, задействованных в информационных системах различного назначения, а с другой – активизацией целевого воздействия (компьютерных атак) на эти системы со стороны злоумышленников.

Увеличение количества и важности задач, возлагаемых на компьютерные сети, обуславливает повышение требований, предъявляемых к сети по обеспечению устойчивости и ее элементов. Составляющими устойчивости являются живучесть, надежность и помехоустойчивость, которые не учитывают воздействие КА. Предлагается ввести четвертую самостоятельную составляющую устойчивости КС – *киберустойчивость*, под которой понимается свойство сети сохранять способность выполнять требуемые функции в условиях воздействия компьютерных атак.

Оценка киберустойчивости компьютерной сети является достаточно важной и сложной задачей. Решать эту задачу приходится достаточно часто как при проектировании компьютерной сети, так и при ее администрировании. Аналитическое моделирование компьютерных атак во многом помогает эффективному решению этой задачи [1, 2, 3].

В качестве показателя, характеризующего киберустойчивость сети, предлагается использовать коэффициент исправного действия по киберустойчивости. С целью определения этого коэффициента сначала находятся коэффициенты исправного действия для каждого j-го маршрута в условиях воздействия атак $K_{sa,j}$ и вероятность воздействия на эти маршруты $P_{act,j}$. Коэффициент $K_{sa,j}$ рассчитывается как отношение среднего времени исправной работы сети на маршруте к общему времени ее функционирования.

Так как маршрут передачи информации состоит из нескольких интервалов связи, то коэффициент исправного действия j-го составного маршрута равен:

$$K_{sa\_CM,j} = \prod_{j=1}^{O} K_{ca,j},$$

где O – общее количество интервалов связи на j-ом маршруте.

Совокупность маршрутов образуют направление связи, а совокупность направлений связи и средств вычислительной техники – компьютерную сеть. Коэффициент исправного действия i-го направления связи $K_{sa\_D,i}$ характеризуется вероятностью сохранения на этом направлении хотя бы одного маршрута и определяется по формулам:

$$K_{sa\_D,i} = K_{rel\_D,i} \cdot \left(1 - \prod_{j=1}^{N} \left(1 - K_{sa\_CM,j}\right) \cdot P_{act,j}\right), \quad K_{rel\_D,i} = \sum_{j=1}^{N} a_{ij} \cdot \left(\frac{H_j}{N-O} + \frac{O}{N}\right),$$

где $K_{rel\_D,i}$ – коэффициент связности i-го направления связи; N – число маршрутов в направлении связи; $\alpha_{ij} = \gamma_j / \gamma_{sum,j}$ – вес j-го маршрута в информационном обмене i-го НС.

Учитывая, что КС состоит из M направлений связи, коэффициент K_{sa} исправного действия КС в условиях КА определяется из следующих выражений:

$$K_{sa} = K_{rel} \cdot \left(1 - \prod_{i=1}^{M} \left(1 - K_{sa\_D,i}\right)\right), \quad K_{rel} = \sum_{i=1}^{M} a_i \cdot \left(\frac{G_i}{M-N} + \frac{N}{M}\right),$$

где K_{rel} – коэффициент связности сети; G_i – ранг i-го направления связи; M – количество направлений связи в КС.

Таким образом, для определения коэффициента исправного действия КС первоначально требуется определить среднее время воздействия системы атак и выработки мер противодействия, т. е. определить вероятностно-временные характеристики (ВВХ) атак. Для этого предлагается использовать эталонные модели атак и метод топологического преобразования стохастических сетей. Порядок построения эталонной модели атаки будет рассмотрен на примере атаки типа «Сканирование сети и ее уязвимостей».

Реализация этой атаки имеет следующие этапы:

– запуск программно-аппаратного комплекса (сетевого сканера) за среднее время $\overline{t_{start}}$ с функцией распределения времени $W(t)$;

– определение активных элементов атакуемой сети с вероятностью P_n за среднее время $\overline{t_{elem}}$ с функцией распределения времени $Q(t)$;

– определение типов операционных систем на активных элементах сети с вероятностью P_n за среднее время $\overline{t_{OS}}$ с функцией распределения времени $D(t)$;

– определение сервисов на элементах сети с вероятностью P_n за среднее время $\overline{t_{ser}}$ с функцией распределения времени $L(t)$;

– определение уязвимостей за среднее время $\overline{t_{vul}}$ с функцией распределения времени $O(t)$.

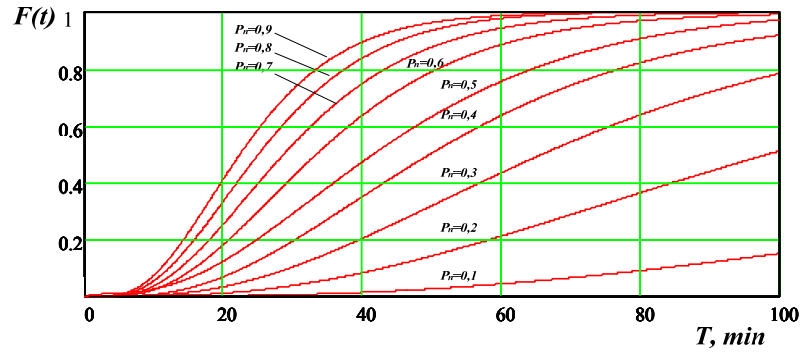
При этом если активные элементы сети, типы операционных систем и сервисы на них не будут определены, то с вероятностью $(1 – P_n)$ сетевой сканер будет запущен повторно за среднее время $\overline{t_{rep}}$ с функцией распределения времени $Z(t)$.

Порядок определения ВВХ с использованием метода топологического преобразования сетей подробно описан в [4, 5, 6], поэтому здесь будут приведены только результаты расчета, которые представлены в виде зависимостей на рис. 1.

В качестве исходных данных используются следующие значения средних времен реализации этапов атаки и вероятности перехода пользователя по ссылке: $\overline{t_{start}} = 3$ мин, $\overline{t_{elem}} = 7$ мин, $\overline{t_{OS}} = 4$ мин, $\overline{t_{ser}} = 5$ мин, $\overline{t_{vul}} = 7$ мин, $\overline{t_{rep}} = 3$ мин, $P_n = 0.1,\ldots,0.9$.

Анализ полученных на рис. 1*а* и 1*б* зависимостей позволяет сделать вывод о том, что для реализации атаки «Сканирование сети и ее уязвимостей» с вероятностью $P_n = 0.1$ требуется 280 минут и 33 минуты при $P_n = 0.9$. Полученные зависимости позволяют оценить влияние вероятности нахождения активных элементов сети, типов операционных систем и сервисов (за время не более заданного) на значения функции распределения времени реализации атаки. Видно, что увеличение вероятности P_n уменьшает среднее время реализации атаки. Однако по мере возрастания значения P_n степень влияния на интегральную функцию распределения $F(t)$ уменьшается.

а)



б)

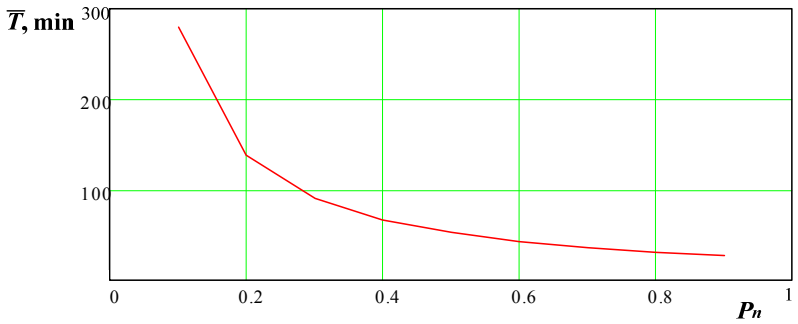


Рис. 1. Вероятностно-временные характеристики компьютерной атаки типа «Сканирование сети и ее уязвимостей»: а) зависимость интегральной функции распределения вероятности от времени реализации компьютерной атаки; б) зависимость среднего времени реализации компьютерной атаки от вероятности P_n

Используя эти вероятностно-временные характеристики, были получены зависимости коэффициента исправного действия от количества маршрутов, представленные на рис. 2 и 3.

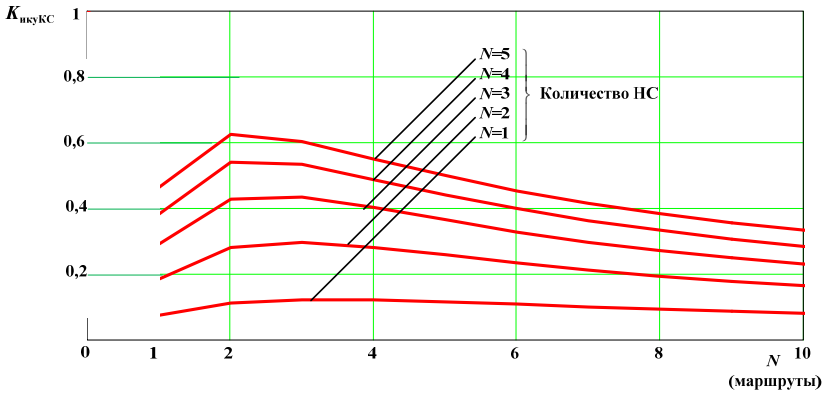


Рис. 2. Зависимость коэффициента исправного действия КС от количества маршрутов и НС

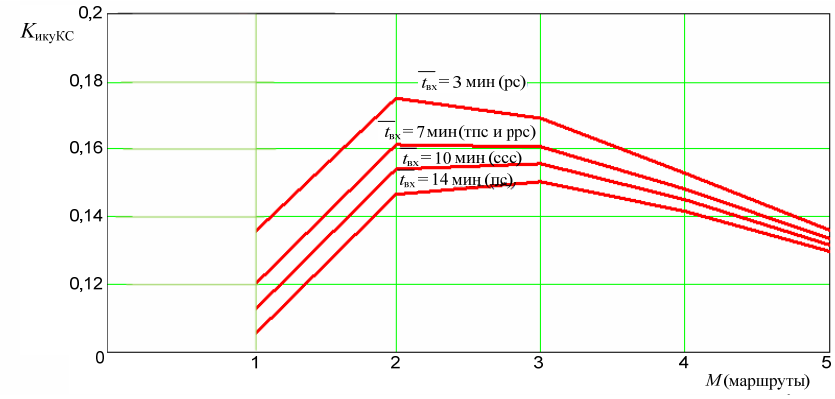


Рис. 3. Зависимость коэффициента исправного действия КС от количества маршрутов и времени вхождения в связь (реакции маршрутов)

В качестве исходных данных использовались следующие значения: $\alpha_i = 1$; $\overline{t_{ent}} = 3$ min; $\overline{t_{tr}} = 1$ min; $\overline{t_{de}} = 2$ min; $\overline{t_{re}} = 10$ min; $\overline{t_{CA}} = 13$ min.

Полученная зависимость коэффициента исправного действия от количества маршрутов позволяет определить рациональный диапазон количества потребных маршрутов при воздействии КА.

Анализ экспериментальных результатов показывает, что коэффициент исправного действия принимает оптимальное значение при использовании для передачи информации от 2 до 5 маршрутов в зависимости от количества направлений связи в КС, что свидетельствует о необходимости перехода от распределенной структуры КС к «звезде».

Таким образом, предлагаемая методика позволяет оценивать киберустойчивость КС. Результаты этой оценки обеспечивают формирование научно-обоснованных требований к топологии КС и к средствам и способам ее защиты от системы КА.

Работа выполнена при финансовой поддержке РФФИ (проекты 15-07-07451, 16-37-00338, 16-29-09482 офи_м) и при частичной поддержке бюджетных тем № 0073-2015-0004 и 0073-2015-0007.

Список используемых источников

1. Котенко Д. И., Котенко И. В., Саенко И. Б. Методы и средства моделирования атак в больших компьютерных сетях: состояние проблемы // Труды СПИИРАН. Вып. 3 (22). С. 5–30.

2. Kotenko I., Stepashkin M. Analyzing Vulnerabilities and Measuring Security Level at Design and Exploitation Stages of Computer Network Life Cycle // Lecture Notes in Computer Science, V. 3685. 2005. P. 317–330.

3. Авраменко В .С. Модели защищенности информации от несанкционированного доступа в многорежимных автоматизированных системах и методы ее контроля в условиях неопределенности угроз // Информация и космос. 2008. N 2. С. 87–94.

4. Саенко И. Б., Лаута О. С., Котенко И. В. Применение метода преобразования стохастических сетей для моделирования мобильных банковских атак // Известия высших учебных заведений. Приборостроение. 2016. Т. 9. N 11. С. 928–933.

5. Коцыняк М. А., Лаута О. С., Осадчий С. А. Вероятностно-временные характеристики компьютерной атаки типа «Анализ сетевого трафика» // Информация и космос. 2013. N 3–4. С. 25–27.

6. Привалов А. А. Метод топологического преобразования стохастических сетей и его использование для анализа систем связи ВМФ. СПб.: ВМА, 2000. 240 с.

УДК 004.77

МОДЕЛЬ ЗАЩИЩЕННОЙ МОБИЛЬНОЙ КОММУНИКАЦИОННОЙ СЕТИ ПОДДЕРЖКИ И ОПЕРАТИВНОГО УПРАВЛЕНИЯ В ЧРЕЗВЫЧАЙНЫХ СИТУАЦИЯХ

В. А. Десницкий[1,2], Н. А. Остроущенко[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 предложена модель защищенной мобильной коммуникационной сети поддержки и оперативного управления в чрезвычайных ситуациях. Модель строится на основе программно-аппаратных модулей XBee обеспечивающих работу протокола беспроводной связи ZigBee. Разработаны прототипы устройств сети, проведен анализ инцидентов киберфизической безопасности.

оперативное управление, XBee, самоорганизующиеся сети, модель нарушителя.

Сложность разработки модели защищенной мобильной коммуникационной сети поддержки и оперативного управления в чрезвычайных ситуациях состоит в необходимости одновременного вовлечения в целевые процессы различных служб управления, их совместной и согласованной работы. Под чрезвычайными ситуациями понимается обстановка на конкретной территории, которая сложилась из-за некоторой техногенной аварии, террористических актов, природного явления или иного бедствия, которая повлекла и может повлечь человеческие смерти, причинить ущерб здоровью людей и природе, или привести к значительным финансовым потерям [1].

Коммуникационные сети отдельных служб способны функционировать как в автономном режиме, так и совместно. К особенностям построения целевой мобильной коммуникационной сети можно отнести:

– сложность оперативного развертывания на местности, ситуативной защищенной интеграции (и дезинтеграции) отдельных подсетей, оперируемых различными службами реагирования в единую коммуникационную сеть без нарушения свойств доступности устройств и предоставляемых сервисов;

– сложность организации защищенного многостороннего обмена данными и событиями безопасности в режиме близком к режиму реального времени с возможностью обмена уже накопленными ранее данными.

Данные, которые приходят от устройств, обладают стихийным характером поступления, и как следствие, требуется изменение состава задействованных служб, необходимого их оснащения и персонала. Все это влечет необходимость гибкого подхода к формированию и обслуживанию подобных систем с возможностью подключения «на лету» новых устройств, и изменение конфигураций и сетевой топологии без необходимости приостановки ключевых бизнес-процессов системы.

Целевая система представляет собой мобильный командный технический комплекс для поддержки коммуникационных сервисов системы. В основе данной системы лежит мобильная самоорганизующаяся сеть, способная к перестроениям в процессе ее функционирования в зависимости от местоположения, количества и интенсивности использования пользователями узлов сети.

В общем случае, узлы сети могут быть смонтированы на транспортных средствах конкретных служб, в помещении оперативного штаба миссии, или они могут представлять собой мобильные персональные терминальные устройства. При этом мобильная коммуникационная сеть может работать в связке с другими мобильными сетями, в режиме коммуникации лишь с центральным штабом данной службы и в полностью автономном режиме работы.

Подобные системы, построенные на базе самоорганизующихся беспроводных сетей, могут иметь одну из следующих архитектур: (1) система с двумя непересекающимися множествами узлов-роутеров и оконечных устройств; (2) система, в которой множества роутеров и оконечных узлов совпадают; (3) гибридная схема, при которой данные два множества могут иметь пересечения, в зависимости от особенностей и ограничений конкретного сценария развертывания системы, делая систему более адаптивной. Предложенная типовая мобильная коммуникационная сеть оперативного управления и реагирования в чрезвычайных ситуациях имеет следующие элементы:

– узел мобильной сети – программно-аппаратный модуль, который встраивается непосредственно в конечное клиентское устройство или подключается к нему;

– шлюз мобильной сети – программно-аппаратный модуль, обеспечивающей иерархические соединения между несколькими мобильными подсетями системы;

– клиентские устройства – пользовательские терминалы, смартфоны, портативные компьютеры и др.;

– дополнительные сетевые элементы, позволяющие организовать связь с внешними по отношению к системе информационными сущностями, такими как серверы приложений, системы управления базами данных и пр.

За основу прототипа мобильной коммуникационной сети поддержки и оперативного управления в чрезвычайных ситуациях были выбраны встроенные устройства XBee серии 2, модификации XB24-ZB, позволяющие организовать беспроводные коммуникации по протоколу ZigBee [2]. Протокол ZigBee определяет правила работы программно-аппаратных комплексов, с помощью которых организуется беспроводный информационный обмен. Преимущества протокола ZigBee [3] – компактность устройств, низкое энергопотребление, а также возможность самовосстановления в случае обрыва связи между устройствами.

Средняя скорость информационного обмена в таких сетях составляет 250 кбит/с. При этом средняя скорость передачи полезных данных, в зависимости от загрузки сети и числа ретрансляций, составляет от 5 до 40 кбит/с. Встроенные средства защиты XB24-ZB включают лишь возможность шифрования с помощью алгоритма AES с длиной ключом 128 бит. При этом при помощи данного крипто примитива осуществляется шифрование только полезной нагрузки, тогда как структура пакета, в том числе идентификаторы PAN ID и MAC адрес оказываются незащищенными перед потенциальным нарушителем.

На рисунке приведен фрагмент верхнего уровня представления разработанной модели мобильной коммуникационной сети с тремя развернутыми службами. Двухуровневый характер системы позволяет организовать разграничения потоков данным и потоков управления между отдельным подсетями, узлами и пользователями системы [4].

На уровне 1 осуществляется передача потоков данных между группами устройств, где каждую отдельную группу составляют коммуникационные устройства определенной службы реагирования. Уровень 2 охватывает представления коммуникационных сетей каждой из задействованных служб системы. Так, коммуникационная сеть уровня 2 представляет собой три вида устройств: координирующий узел, маршрутизатор и оконечное устройство.

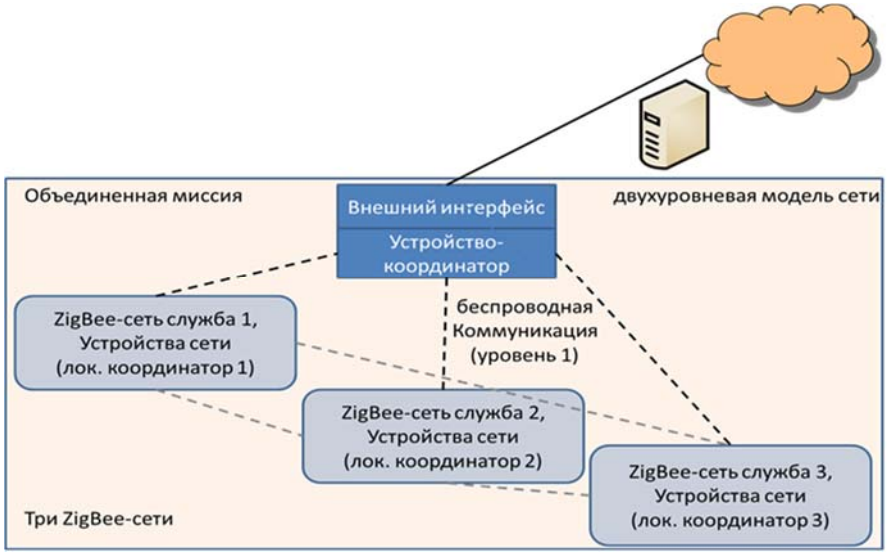


Рисунок. Двухуровневая модель коммуникационной сети

Рассмотрим устройства разработанной модели более детально. Терминальное устройство включает в себя управляющий контроллер Arduino, интегрируемый с ним модуль XBee, а также сенсор физической среды и программный модуль (прошивку), обеспечивающие работу бизнес-функций устройства. Локальный координатор (координатор уровня 2) базируемся на базе микроконтроллера Arduino Mega 2560 и включает в свой состав два модуля XBee – один для организации работы координируемой им подсети, второй – для связи устройств подсети с глобальным координатором. Координатор уровня 1 представляет собой центральное устройство, построенное на базе платы Arduino Yún с модулем XBee, координирующим коммуникационную ZigBee-сеть уровня 1 и предоставляющим Ethernet-интерфейс и встроенный модуль Wi-Fi для внешних коммуникаций системы.

Для анализа инцидентов киберфизической безопасности была построена модель нарушителя, позволяющая проанализировать возможности нарушителя, атакующие действия нарушителя и особенности защиты против данных определенных видов атак. Модель построена на базе классификаций нарушителя по уровням возможностям нарушителя (Rae A. J.) и по типу доступа нарушителя (Abraham D. G.) [5, 6].

Классификация по уровням возможностей нарушителя выделяет три уровня нарушителей. Нарушитель уровня 1 основывается только на ранее известных уязвимостях и использует готовые программные инструменты. Нарушитель уровня 2 обладает обширными знаниями и навыками в области уязвимостей и средств киберфизической безопасности, способен использовать специально разработанные атакующие средства и уязвимости нулевого дня. Уровень 3 представляет собой группу нарушителей уровня 2, обладающую неограниченным организационно-техническими ресурсами.

Классификация по типу доступа нарушителя описывает пять типов нарушителей. Нарушители типа 0 может использовать только атаки социальной инженерии. Нарушители типа 1 выполняют атаки на потоки данных удаленно, например, по средствам сети Интернет. Нарушитель типа 2 воздействует на беспроводные интерфейсы, например, Wi-Fi, Bluetooth, XBee и другие. У нарушителя типа 3 есть доступ к проводным и внешним интерфейсам, таким как USB, RS-232. Для нарушителя типа 4 устройство представляет собой набор микросхем, сенсоров и актуаторов, к которым нарушитель имеет полный доступ.

В работе проводится анализ инцидентов безопасности и возможных атакующих воздействий в рамках мобильной коммуникационной сети с использованием приведенной модели нарушителя. Примерами несанкционированных действий нарушителя являются: прослушивание пользовательских и служебных данных, передающихся по радиоканалам сети; создание конфликтных ситуаций в сети путем задания неправильных сетевых настроек модулей XBee и адресов пакетов данных, атаки имперсонализации и другие, относимые к третьему типу нарушителю уровня 2. В общем случае детектирование определенной разновидности атаки, вовлеченных в нее экземпляров сущностей, а также формирование конкретного инцидента безопасности осуществляются путем сбора и группового анализа событий безопасности, поступающих из нескольких источников информации, которые обрабатываются централизованно на стороне глобального координатора с привлечением вычислительных и коммуникационных ресурсов Arduino Yún.

В работе предложена модель системы оперативного управления в чрезвычайных ситуациях модель инцидентов безопасности. Модель имеет применение при следующих ограничениях: (1) ограниченная дальность действия (35–120 метров в зависимости от рельефа местности); (2) при количестве узлов больше 300 значительно снижается пропускная способность из-за возрастания служебного трафика в сети; (3) устройства XBee не пригодны для работы с быстродвижущимися объектами; (4) передача «живого» звука может быть осложнена задержками в сети.

Работа выполнена при финансовой поддержке РФФИ (проект № 15-07-07451) и при частичной поддержке бюджетных тем № 0073-2015-0004 и 0073-2015-0007.

Список используемых источников

1. Десницкий В. А., Котенко И. В. Проектирование защищенных встроенных устройств на основе конфигурирования // Проблемы информационной безопасности. Компьютерные системы. 2013. № 1. С. 44–54.

2. Документация на Digi XCTU Configuration & Test Utility Software, XCTU User Guide [Электронный ресурс] // 2016. URL: https://www.digi.com/resources/documentation/digidocs/90001458-13/default.htm#concept/c_90001458-13_start.htm%3FTocPath%3D_____1 (дата обращения 05.03.2017).

3. Лекнин В. Администрирование – Сети ZigBee. Зачем и почему? [Электронный ресурс] // 2012. URL: https://habrahabr.ru/post/155037, (дата обращения 27.02.2017).

4. Чечулин А. А., Котенко И. В., Десницкий В. А. Анализ информационных потоков для построения защищенных систем со встроенными устройствами // Системы высокой доступности. 2012. № 2. С. 116–122.

5. Desnitsky V. and Kotenko I. Expert Knowledge based Design and Verification of Secure Systems with Embedded Devices // Lecture Notes in Computer Science. Springer-Verlag. 2014. Vol. 8708. P. 194–210.

6. Котенко И. В., Десницкий В. А., Чечулин А. А. Исследование технологии проектирования безопасных встроенных систем в проекте Европейского сообщества SecFutur // Защита информации. Инсайд. 2011. № 3 (39). С. 68–75.

УДК 004.738

ПОДХОДЫ К ОРГАНИЗАЦИИ МОБИЛЬНЫХ ГЕТЕРОГЕННЫХ ШЛЮЗОВ НА БАЗЕ БЕСПИЛОТНЫХ ЛЕТАТЕЛЬНЫХ АППАРАТОВ

Ч. З. Динь, Р. В. Киричек

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

В последние несколько лет беспилотные летательные аппараты стали применяться во многих сферах жизнедеятельности. В связи с развитием технологий электропитания значительно увеличилось время автономной работы БПЛА и в настоящий момент составляет 2–3 часа. Согласно прогнозам Международного союза электросвязи в 2020 г. начнется повсеместная эксплуатация сетей пятого поколения (5G, IMT-2020). В рамках концепции 5G предполагается бесшовная связь между устройствами Интернета вещей, взаимодействующими на базе различных технологий. Для обеспечения такой связности необходимо полное покрытие участков местности с большим количеством устройств. Для этих целей предполагается использовать БПЛА с шлюзом на борту. Такой шлюз будет выполнять роль связующего звена между абонентами (устройствами, сотовыми телефонами и др.) и сетью связи общего пользования. В статьи рассматривается подходы к организации мобильных гетерогенных шлюзов на базе беспилотных летательных аппаратов, а также модели такого взаимодействия.

летающая сенсорная сеть, интернет вещей, 5G, БПЛА, шлюз.

В последние годы исследования в области всепроникающей сенсорной сети постепенно переходят от изучения характеристик на плоскости к моделям в трехмерном пространстве – это летающие сенсорные сети [1, 2, 3]. Летающая сенсорная сеть предполагается два сегмента: наземный и летающий. В качестве летающих узлов используются беспилотные летающие аппараты (БПЛА). В настоящим времени, БПЛА стали применяться во многих сферах жизнедеятельности. Например, мониторинг удаленных, труднодоступных или опасных объектов; картографирования; презентации, реклама, развлечения; ретрансляция сигналов; управление поведением живых объектов; доставка грузов и т. д. [4].

Согласно прогнозам Международного союза электросвязи, в 2020 г. начнется повсеместная эксплуатация сетей пятого поколения (5G, IMT-2020) [5, 6]. В рамках концепции 5G (рис. 1) предполагается бесшовная связь между устройствами Интернета вещей, взаимодействующими на базе различных технологий. Для обеспечения такой связности необходимо полное покрытие участков местности с большим количеством устройств [7].

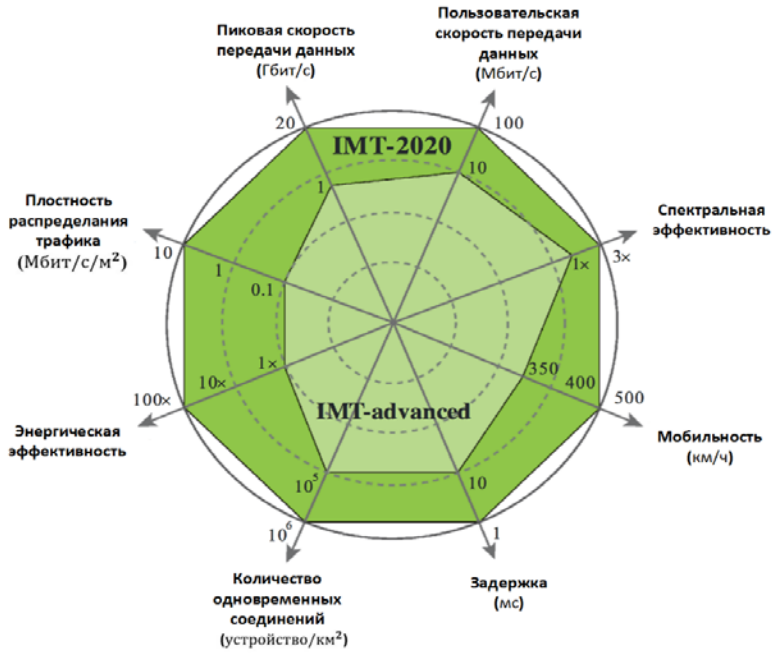


Рис. 1. Ключевые параметры для 5G

Для достижения этих целей и вместе с развитием технологий электропитания, БПЛА сможет работать до 2–3 часов [8], в этой связи, предполагается использовать БПЛА с шлюзом на борту как мобильный гетерогенный шлюз, который может поддержать многие технологии передачи данных. Такой шлюз будет выполнять роль связующего звена между абонентами (устройствами, сотовыми телефонами и др.) и сетью связи общего пользования.

Согласно с вышеописанными задачами, для БПЛА со шлюзом на борту, предполагается два подходы к организации мобильных гетерогенных шлюзов на базе беспилотных летательных аппаратов: Первый подход – для неподвижной наземной сети с сенсорными узлами и второй подход для подвижной наземной сети с мобильными устройствами.

Подход для неподвижной наземной сети с сенсорными узлами используется в случае что, когда БПЛА собирает данные с сенсорного поля далеко от базовых станций и обеспечивают канал связи с ССОП (рис. 2). Однако, в этом подходе, возможны следующие проблемы. Во-первых, необходимо рассчитать каким образом будут выбираться технологии передачи и протоколы, в зависимости от достаточной энергии аккумулятора у БПЛА. Во-вторых, БПЛА после сбора данных возвращается обратно на станцию подзарядки и передачи данных в ССОП. На его место прилетает новый БПЛА и в момент смены необходимо рассчитывать хэндовер [9]. В данном подходе, большинство БПЛА собирают только данных поэтому время хэндовера не так строго и рассматривать такую структуру сети, как DTN – сеть устойчивая к разрывам (DTN) [10].

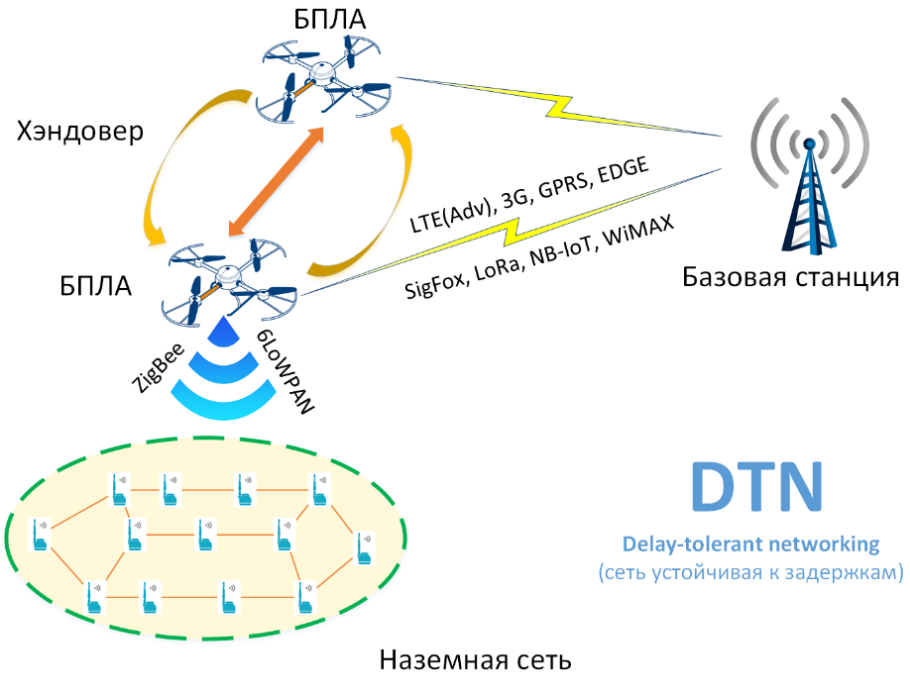


Рис. 2. Подход для неподвижной наземной сети с сенсорными узлами

Если в определенном месте большое скопление людей и у каждого есть сотовый телефон, планшет, ноутбук и т. д. Всем необходимо высокоскоростной доступ в Интернет. Допустим базовая станция рядом не может обслужить всех абонентов, поэтому подход для подвижной наземной сети

с мобильными устройствами предполагает присутствие БПЛА как временной базовой станции (рис. 3). В этом походе, абоненты потребляют большой обмен сетевого трафика, поэтому должны быть обеспечены оптимальные параметры качества обслуживания.

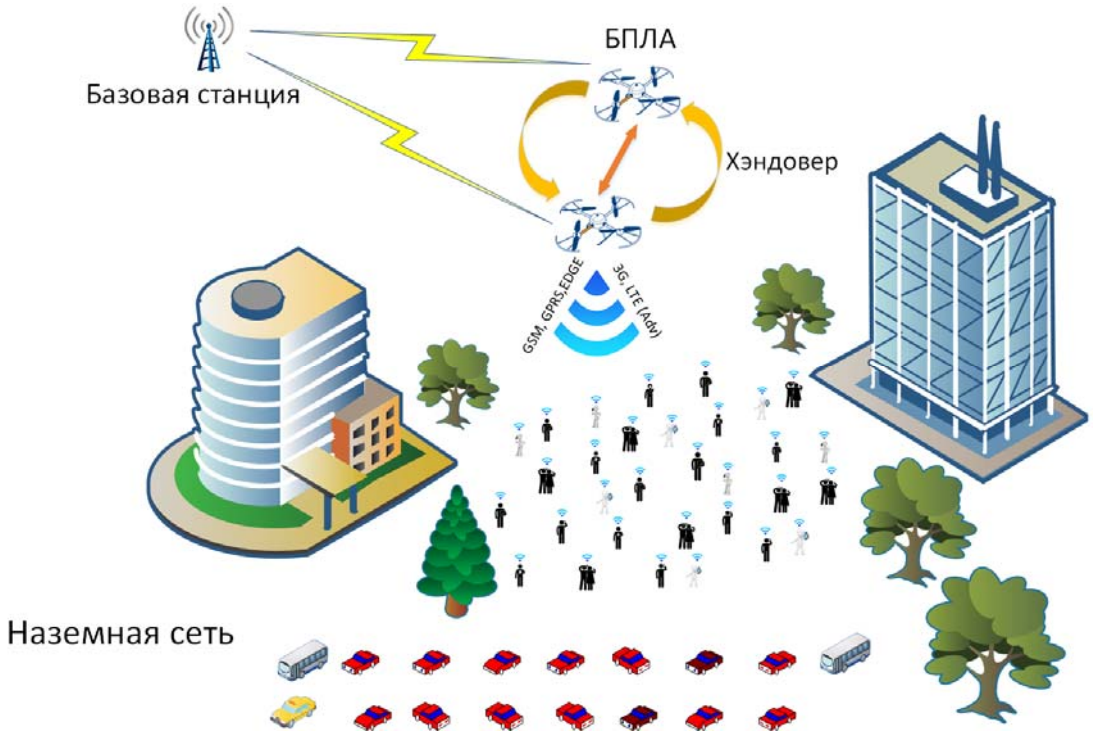


Рис. 3. Подход для подвижной наземной сети с мобильными устройствами

Аналогично как в первом подходе, возможно возникновение некоторых проблем. Во-первых, необходимо рассчитать каким образом будут выбираться технологии передачи и протоколы. В таблице рассматриваются технологии связи. Которые могут быть реализованы на базе летающего гетерогенного шлюза. В настоящий момент, не существует технологий беспроводной высокоскоростной передачи данных. Для этого будут использоваться технологии 5G, которые обеспечат скорость передачи до 10 Гбит/с. Во-вторых, когда базовая станция находится очень далеко от наземной сети, а нам необходимо передать данные - каждый дополнительный элемент вносит задержку. Чтобы избежать этого необходимо разработать модель системы массового обслуживания и провести расчеты. Во-третях, у БПЛА есть аккумулятор, который разряжается, когда он летит обратно на базу. В этот момент связь разрывается и критичным является то, что абоненты не должны потерять связь, они должны продолжать разговаривать и время хэндовера очень строгое.

ТАБЛИЦА. Сравнения различных технологий передачи данных

	LTE (Adv)	3G (UMTS)	EDGE	GPRS	SigFox	LoRa	NB-IoT	WiMAX (802.16m)
Мак. скорость передачи данных	1 Гбит/с	384 кбит/с	217,6 кбит/с	53,6 кбит/с	100 кбит/с	50 кбит/с	250 кбит/с	350 Мбит/с
Диапазон покрытия	100 км	100 км	100 км	35 км	50 км	15 км	35 км	50 км
Пропускная способность	100 МГц	5 МГц	200 кГц	200 кГц	100 Гц	125 кГц	180 кГц	40 МГц
Задержка	5 мс	150 мс	710 мс	320 мс	секунд	–	–	10 мс
Энергопо-требление	1 день	1 день	1 день	1 день	10 лет	10 лет	10 лет	7 дней

Таким образом, после рассмотрения подходов к организации мобильных гетерогенных шлюзов на базе беспилотных летательных аппаратов, получены некоторые задачи для проведения исследования:

– проанализировать технологии связи и протоколы для обеспечения бесперебойной связи;

– исследование энергопотребления БПЛА и шлюза, установленного на борту БПЛА;

– исследование хэндовера для различных конфигураций сетей;

– исследование возможности организации кластеров для сбора данных;

– оптимизация параметров шлюзов;

– разработка алгоритмов самоорганизации между группой БПЛА.

В дальнейшем планируется провести серию натурных экспериментов на базе летающей сенсорной сети, развернутой в Лаборатории Интернета вещей СПбГУТ [11, 12, 13].

Список используемых источников

1. Кучерявый А. Е., Киричек Р. В., Парамонов А. И., Прокопьев А. В. Эволюция исследований в области беспроводных сенсорных сетей // Информационные технологии и телекоммуникации. 2014. №4. С. 29–41. URL: https://www.sut.ru/doci/nauka/review/4-14.pdf

2. Кучерявый А. Е., Владыко А. Г., Киричек Р. В., Парамонов А. И., Прокопьев А. В., Богданов А. И., Дорг-Гольц А. А. Летающие сенсорные сети // Электросвязь. 2014. № 9. С. 2–5.

3. Кучерявый А. Е., Владыко А. Г., Киричек Р. В. Летающие сенсорные сети – новое приложение интернета вещей // Актуальные проблемы инфотелекоммуникаций в науке и образовании. IV международная научно-техническая и научно-методическая конференция: сборник научных статей в 2 томах. СПб. : СПбГУТ, 2015. С. 17–22.

4. Динь Ч. З., Киричек Р. В. Разработка и исследование методов инсталляции беспроводных сенсорных узлов с беспилотного летательного аппарата // Распределенные компьютерные и телекоммуникационные сети: управление, вычисление, связь (DCCN-2016). Москва, 2016. С. 114–121.

5. Andrews, J. G., Buzzi, S., Choi, W., Hanly, S. V., Lozano, A., Soong, A. C., & Zhang, J. C. What will 5G be? // IEEE Journal on selected areas in communications, 2014. 32 (6). PP. 1065–1082.

6. Agiwal, M., Roy, A., & Saxena, N. Next generation 5G wireless networks: A comprehensive survey // IEEE Communications Surveys & Tutorials. 2016. 18 (3). PP. 1617–1655.

7. Koucheruavy A., Vladyko A., kirichek R. State of the Art and Research Challenges for Public Flying Ubiquitous Sensor Networks // Lecrure Notes in Conputer Science. 2015. Vol. 9247. PP. 299–308.

8. Williams M. Fuel cell keeps drones in flight for hours, not minutes [Электронный ресурс]. URL:http://www.theverge.com/2015/12/15/10220456/intelligent-energy-hydrogen-fuel-cell-drone (дата обращения 15.03.2016).

9. Gupta, L., Jain, R., & Vaszkun, G. Survey of important issues in UAV communication networks // IEEE Communications Surveys & Tutorials. 2016. 18 (2). PP. 1123–1152.

10. Pöttner, W. B., Büsching, F., Von Zengen, G., & Wolf, L. Data elevators: Applying the bundle protocol in delay tolerant wireless sensor networks // In Mobile Adhoc and Sensor Systems (MASS). IEEE 9th International Conference on. 2012. PP. 218–226.

11. Kirichek R., Koucheryavy A. Internet of Things laboratory test bed//Lecture Notes in Electrical Engineering. 2016. Vol. 348. PP. 485–49, DOI: 10.1007/978-81-322-2580-5_44.

12. Kirichek, R., Vladyko, A. Zakharov, M., Koucheryavy, A.: Model Networks for Internet of Things and SDN // In 18th International Conference on Advanced Communication Technology (ICACT), pp. 76–79. IEEE (2016).

13. Kirichek, R., Vladyko, A., Paramonov, A., Koucheryavy, A.: Software-Defined Architecture for Flying Ubiquitous Sensor Networking. In: 19th International Conference on Advanced Communication Technology (ICACT), pp. 158–162 (2017).

УДК 4.056

РАЗРАБОТКА КОМПЛЕКСА ПРОГРАММНО-АППАРАТНОГО ОБЕСПЕЧЕНИЯ ДЛЯ ПЕРЕХВАТА БЕСПИЛОТНОГО ЛЕТАТЕЛЬНОГО АППАРАТА

Е.В. Дмитриева, А. В. Красов, О. Б. Филиппов

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

В данной работе рассматривается возможность и практическое применение обратного инжиниринга протокола передачи данных, между пультом дистанционного управления и квадрокоптером от компании WLtoys модели V686. Также, исследование радиочастотных каналов, потенциальные возможности атаки на отказ в управлении дрона, удаленный перехват контроля. Обратному инжинирингу подвергнется и приложение для Android устройств от производителя, с описанием обнаруженных уязвимостей, перехватом видеопотока, управления дроном.

беспилотники, RTL-SDR HackRF, риверс-инжиниринг, GNU Radio, Nmap.

Основная проблема заключается не только в операторах БПЛА, которые используются повсеместно, а еще в отсутствии защиты в канале передачи данных. Производители часто не уделяют должного внимания этому аспекту. В данной работе будет использован квадрокоптер производства компании WLtoys модели V686 (рис. 1), являющийся одним из примеров недостаточной защищенности канала передачи данных. В статье будут проведены исследования методом ручного анализа канала, реверсивного инжиниринга данных на предмет наличия уязвимостей, защит от атак на повтор, возможность перехвата управления. После анализа и описания этих данных, будут приведены примеры атак на перехват контроля и отказа в управлении, а также приведен алгоритм анализа радиочастотного канала, т. к. протокол передачи данных является закрытым [1].

Наибольший интерес представляет первые две функции. Реверс инжиниринг проводился с помощью RTL-SDR HackRF и комплекта открытого программного обеспечения GNU Radio [2]. Алгоритм реверс-инжиниринга представлен ниже:

– подключаем HackRF и запускаем граф исследования 2,4 ГГц диапазона;

– запускаем квадрокоптер и пульт ДУ;

– взаимодействует с любой функциональной кнопкой на пульте, записывая в блокнот время нажатия и кнопку;

– составляем описание сигнала, модуляцию и последовательность данных, записываем в блокнот пример сигнала для действия;

– повторяем действия для всех кнопок на пульте.

Рис. 1. Рисунок квадрокоптера (изображение)

Анализ полученных данных показал, что передача данных идет на частотах от 2,412 ГГц до 2,484 ГГц, что соответствует Wi-Fi сетям. Основываясь на том, что данные передаются с помощью сети стандарта 802.11 в установленных выше диапазонах, можно сделать частотное распределение по функциям управления (табл.).

ТАБЛИЦА. Результат риверс-инжиниринга радио-протокола

Центральная частота, ГГц	Номер канала Wi-Fi	Действие
2,412	CH 1	Крен по горизонтали
2,417	CH 2	Крен по вертикали
2,422	CH 3	Скорость вращения лопастей
2,427	CH 4	Рыскание

Использование Wi-Fi в качестве средства передачи данных между оператором и устройством не удивительно, т. к. поддержка такого метода проста, а реализация не составляет труда. В интернете можно найти множество

моделей на радиоуправлении, которые использует такой вариант. Однако, здесь появляются и крупные недостатки, связанные с уязвимостями точек доступа и их настройкой. В случае исследуемого дрона, то шифрование трафика внутри сети полностью отсутствует, а точка не запрашивает авторизацию при подключении, позволяя злоумышленнику удаленно подключится к квадрокоптеру и использовать атаки на отключение пульта ДУ (дистанционное управление) оператора, методом отправки на MAC адрес, специально сформированный пакетов типа deAUTH. Это приводит к полному отказу (к разрыву канала между пультом дистанционного управления и дрона) контроле за объектом и зависание в воздухе дрона на несколько секунд. По прошествии этого промежутка времени, дрон попытается вернутся к месту взлета, параллельно находясь в режиме поиска контролирующего пакета с данными для восстановления управления. Атакующий может в этот момент отправить пакет с данными на порт шлюза дрона, на котором запущен обработчик событий, и если полученные данные пройдут необходимую проверку, то возможно выполнение произвольной команды на целевом устройстве – дроне. Данный метом является приоритетным для перехвата управления, так как в момент принятия пакетов, не обрабатываются запросы с пульта оператора [3, 4].

В момент запуска дрона, на 6-ом канале Wi-Fi создается открытая точка доступа, без шифрования. Она позволяет подключать к себе до четырех клиентов, однако, она не маршрутизирует трафик внутри себя, и клиенты не могут друг друга видеть. То есть пакеты могут посылаться только от клиента к точке (*Gateway*). Это понижает коэффициент успешных попыток перехвата управления методом атаки типа человек посредине. С помощью утилиты Nmap были обнаружены два открытых порта на дроне: 80 и 8080. На 80 порту запущен Веб сервер, через который можно конфигурировать точку доступа, выполнять удаленную перезагрузку устройства. На другом – обработчик, отвечающий за обработку TCP пакетов и передачу их по шине – в контроллер дрона. Который, в свою очередь, передаст команды на винты, светодиоды и т. д. Недостатком является то, что на обоих портах отсутствует аутентификация, что в купе с отсутствием таковой на точке доступа, позволяет атакующему посылать произвольный пакеты обработчику, что способно вызвать перехват контроля. Еще большую опасность представляет 80 порт, т. к. он позволяет перезагрузить устройство [5]. Перед моментом перезагрузки системы не происходит проверка на то, что находится ли устройство в воздухе, и позволяет атакующему вывести устройство из строя, путем отключения его в процессе полета и физическому повреждению последнего об ударе о землю, либо о любой другой предмет.

В качестве рекомендации предлагается проделать следующие операции. Для перехвата управления, необходимо послать по TCP протоколу на порт 8080 специально сформированную последовательность, однако,

это коммерческий продукт с закрытым исходным кодом и протоколы передачи недоступны для публичного доступа. Но у компании производителя квадрокоптера существует мобильное приложение, благодаря которому существует возможность удаленного управления полетом. Проведя обратную разработку файла, была получена библиотека с описанием протокола данных для отправки на порт 8080. Так же, была замечена особенность, что после запуска приложения, пульт ДУ оператора, не участвовал в процессе полета.

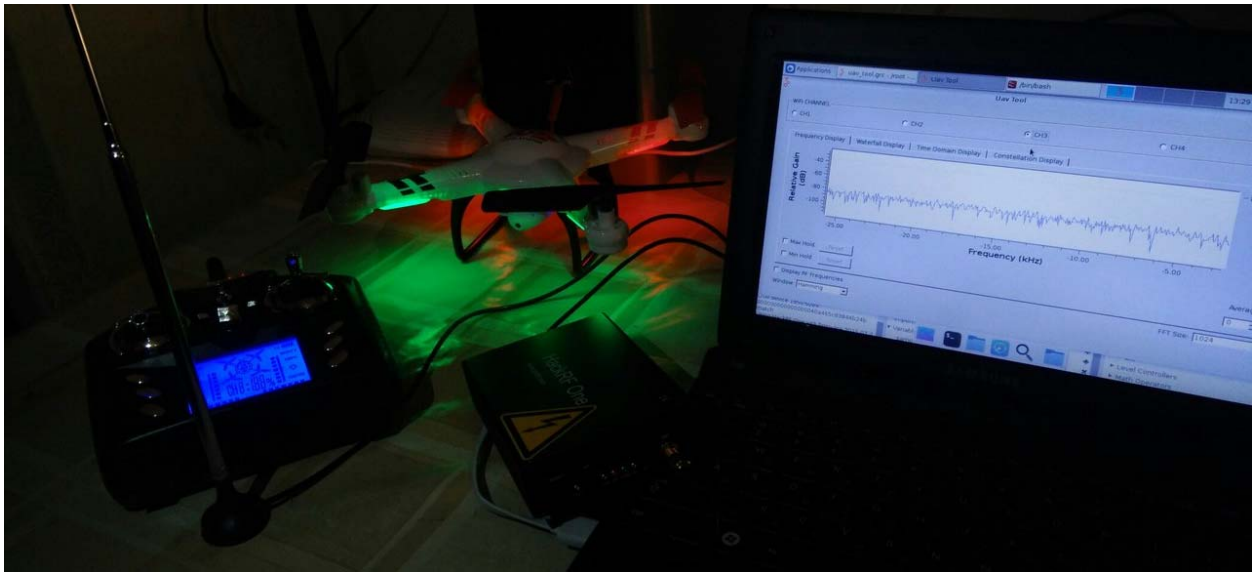


Рис. 2. Демонстрация работы программно-аппаратного комплекса

На основе проведенного исследования, можно сделать вывод о том, что контроллер отдавал приоритет на управление обработчику команд на порту 8080 (рис. 2). На основании всего вышеизложенного, был разработан комплекс ПО и направленных Wi-Fi антенн, позволяющий отключать, перехватывать управление за тестовым дроном. Что и являлось целью данной работы.

Список используемых источников

1. Штеренберг С. И. Методика применения в адаптивно системе локальных вычислительных сетей стеговложения в исполнимые файлы на основе самомодифицирующегося кода // Системы управления и информационные технологии. 2016. Т. 63. № 1. С. 51–54.

2. Андрианов В. И., Романов Г. Г., Штеренберг С. И. Экспертные системы в области информационной безопасности // Актуальные проблемы инфотелекоммуникаций в науке и образовании. IV Международной научно-технической и научно-методической конференции: сб. науч. ст. в 2 томах. 2015. С. 193–197.

3. Андрианов В. И., Красов А. В., Липатников В. А. Инновационное 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». СПб., 2012.

4. Душин С. Е., Красов А. В., Кузьмин Н. Н. Моделирование систем управления: учебное пособие для студентов высших учебных заведений, обучающихся по направлению 220400 «Управление в технических системах» / под ред. С. Е. Душина. М., 2012.

5. Жадан О. П., Стахеев И. Г., Штеренберг И. Г. Алгоритм формирования архитектуры системы технологического управления полевой транспортной сети связи специального назначения // Актуальные проблемы инфотелекоммуникаций в науке и образовании. III Международная научно-техническая и научно-методическая конференция: сб. науч. ст. 2014. С. 808–811.

УДК 004.732

РАДИООБСЛЕДОВАНИЕ И РАДИОПЛАНИРОВАНИЕ БЕСПРОВОДНЫХ ЛОКАЛЬНЫХ СЕТЕЙ WI-FI

Р. А. Дунайцев, К. Ф. Короткин

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

Сегодня сети Wi-Fi пользуются огромной популярностью из-за стремительного роста количества беспроводных пользовательских устройств. Данные сети строятся повсеместно: в офисах, магазинах, кафе, гостиницах, на складах, в парках, больницах и на транспорте. Поскольку на работу сетей Wi-Fi влияет множество факторов (планировка помещения, помехи в радиоканале, количество пользователей и т. д.), для обеспечения заданного качества обслуживания требуется тщательный их учет. В статье рассматривается важность проведения таких этапов проектирования беспроводной локальной сети как радиообследование и радиопланирование.

Wi-Fi, радиообследование, радиопланирование, беспроводная локальная сеть.

Для обеспечения высокого качества беспроводной связи необходимо проводить грамотное проектирование радиосети. Независимо от того, собираемся ли мы строить новую сеть или осуществлять модернизацию уже существующей, проект сети Wi-Fi всегда должен включать в себя такие важные этапы, как радиообследование и радиопланирование.

Первый этап при построении сети Wi-Fi – это проведение на территории заказчика детального радиообследования (*site survey*). Радиообследование позволяет изучить особенности помещения и территории, где планируется развертывание, определить присутствие интерференции, идущей от других источников электромагнитного излучения, которая может снизить

производительность сети Wi-Fi. Также радиообследование помогает определить наилучшее расположение устанавливаемого оборудования и систем кабельной связи, тип используемых антенн и каналы, на которых будет меньше помех.

Для радиообследования используется специализированное программное обеспечение, которое собирает и обрабатывает данные, создавая на их основе тепловые карты (*heatmaps*). Эти цветовые схемы отображают ряд важнейших показателей в соответствии с заданной легендой. Например, позволяют визуализировать мощность сигнала, соотношение сигнал/шум, обнаруженные точки доступа и т. д. [1, 2].

Радиообследование проводится в несколько этапов:

1) Сначала заказчик должен сформулировать требования к работе сети (необходимая зона покрытия, требуемая скорость передачи данных, емкость сети, планируемые к использованию сервисы и приложения).

2) Вместе с заказчиком определяются места установки точек доступа.

3) Затем устанавливаются тестовые точки доступа, и производится замер мощности сигнала в зоне действия данной точки.

4) Производится поиск источников помех, если таковые имеются.

5) По результатам замеров определяется необходимое количество точек доступа и тип антенн, места установки и рекомендации по снижению уровня выявленных помех.

Радиопланирование (*planning*) включает в себя комплекс действий, которые необходимо выполнить при построении новой сети. В его рамках проводится компьютерное моделирование того, как будет работать создаваемая сеть. С помощью специализированного программного обеспечения создается карта помещения или местности, где будет строиться сеть, со всеми присутствующими инженерно-техническими конструкциями, такими как стены, перегородки, двери, окна и перекрытия. Далее указывается материал, из которого состоят инженерно-технические конструкции, и соответствующий коэффициент затухания. Если планируется развернуть сеть Wi-Fi на открытой местности, то указывается наличие и взаимное расположение зданий, сооружений и других препятствий, задаются перепады высот. Карта составляется на основе существующих строительных планов, представленных заказчиком. Затем на карте в программе расставляются виртуальные точки доступа и указывается, какая будет мощность передатчика у этих точек, тип и количество антенн, в каком частотном диапазоне они будут работать. Учитывая всю эту информацию, программа создает план будущей сети Wi-Fi. Но этот программный расчет – ориентировочный. Далее необходимо выехать на объект и провести детальные замеры с помощью комплекта тестового оборудования. В месте, предложенном программой, на специальной штанге устанавливается тестовая точка доступа (AP-on-a-Stick) и проводятся измерения. Затем точка доступа переносится на следующее место

и процесс повторяется. Все это позволяет определить расхождение между реальной картиной и программными расчетами.

В зависимости от того, где и при каких условиях будет разворачиваться сеть Wi-Fi, а также условий эксплуатации и характеристик объекта, будет зависеть как сложность радиообследования и радиопланирования, так и выбор соответствующего программно-аппаратного комплекса. Небольшой офис может ограничиться проверкой интерференции, в то время как большие помещения, крупные офисы, аэропорты, ж/д вокзалы, жилые дома, больницы, ангары, и цеха требуют детального радиообследования и радиопланирования. Особую сложность представляет организация беспроводной сети Wi-Fi в условиях отсутствия развитой инфраструктуры связи, сложного рельефа, неблагоприятных природно-климатических условиях [3, 4]. Традиционные подходы к проектированию Wi-Fi здесь работают плохо. Ярким примером может служить применение технологий беспроводного доступа стандарта IEEE 802.11 на горных предприятиях при проведении открытых горных работ [5, 6]. Беспроводная сеть здесь необходима для организации системы видеонаблюдения, передачи диагностической информации и решения задач оперативного управления горнотранспортным комплексом (экскаваторы, самосвалы, бульдозеры, грейдеры, погрузчики и т. п.). Это обуславливает необходимость внедрения самых современных технологий беспроводной связи, характеризующихся возможностью высококачественной передачи значительных объемов оперативной информации при высокой надежности системы [7].

Создаваемая сеть Wi-Fi для открытых горных работ должна гарантировать надежное радиопокрытие, иметь высокую пропускную способность, обеспечивать передачу любого типа трафика с заданным качеством обслуживания. Для построения такой сети к радиообследованию и радиопланированию предъявляются повышенные требования. При выполнении данных этапов необходимо учитывать особенности работы беспроводной сети в условиях горнодобывающего предприятия, непрерывно меняющуюся конфигурацию карьера и мобильность основного технологического оборудования – клиентов создаваемой сети. Также необходимо учитывать наличие разнообразных препятствий на пути прохождения сигнала, радиопомехи, возникающие при работе электрических машин, а также помехи, связанные с переотражением сигнала в железорудных карьерах.

Радиообследование и радиопланирование помогают получить в полном объеме информацию о местах предпочтительного размещения точек доступа, возможности использовать их для видеонаблюдения, определить мертвые зоны и возможность использования мобильных точек доступа для обеспечения связи в тех местах, где по производственным причинам не могут располагаться фиксированные точки, либо возникает необходимость лишь временного радиопокрытия.

Для получения такого большого объема информации и для организации надежной сети передачи данных необходимо использовать специализированный программы, обеспечивающие:

1) возможность проведения радиообследования с использованием GPS;
2) расчет зон радиопокрытия с применением ГИС;
3) поддержку картографических сервисов Web, интернет-карт;
4) возможность импортировать векторные и растровые карты;
5) измерение мощности и определения местоположения источников помех;
6) измерение реальной скорости в восходящем и нисходящем каналах;
7) проверку готовности и оптимизации сети Wi-Fi для речевого трафика VoIP;
8) учет данных о трафике и количестве пользователей для расчета нагрузки на сеть;
9) отображение в каждой точке мощности сигнала, отношения сигнал/шум, интерференции, присвоенные точкам доступа каналы, скорости передачи, проблемные и работоспособные участки в целом;
10) возможность генерации отчетов в формате PDF/DOC/DOCX.

Такие программы, как Altair WinProp, ATDI ICS telecom и Forsk Atoll, обладают необходимым функционалом и являются лучшими решениями для радиообследования и радиопланирования сетей Wi-Fi на открытой и сильно пересеченной местности. [8, 9, 10].

Грамотно спроектированная и построенная сеть Wi-Fi обеспечит возможность автоматической диспетчеризации горной техники и динамической оптимизации транспортных потоков, повысит эффективность функционирования производства и снизит аварийность на горных предприятиях.

Список используемых источников

1. О важности радиоразведки и радиопланирования при развертывании Wi-Fi сетей [Электронный ресурс] // Издание PC Week Ukrainian Edition 21.01.2015. URL: http://www.pcweek.ua/themes/detail.php?ID=148474 (дата обращения 30.03.2017).

2. Наталенко А. Программное обеспечение для планирования беспроводных сетей [Электронный ресурс] // Журнал о беспроводной и мобильной связи WIRELESS UKRAINE, 2012. URL: http://www.wireless.ua/436-programmnoe-obespechenie-dlya-planirovaniya.html (дата обращения 30.03.2017).

3. 2010: Guidelines For Successful Large Scale Outdoor Wi-Fi Networks [Электронный ресурс] // Публикации на официальном сайте NOVARUM, December 2009. URL: http://www.novarum.com/publications.php (дата обращения 30.03.2017).

4. Mareco D., Wegner P. The Ultimate Guide to Planning a Successful Outdoor Wireless Network [Электронный ресурс] // Официальный сайт SecurEdge Networks. URL: http://www.securedgenetworks.com/blog/the-ultimate-guide-to-planning-a-successful-outdoor-wireless-network (дата обращения 30.03.2017).

5. Пахомов Г. И., Головин С. И., Калашников А. Д., Каширина Е. С., Тонких М. Ю. Технологии Wi-Fi и WiMAX в горной промышленности [Электронный ресурс] // Вестник ПНИПУ. Электротехника, информационные технологии, системы управления, № 5 / 2011. URL: http://cyberleninka.ru/article/n/tehnologii-wi-fi-i-wimax-v-gornoy-promyshlennosti (дата обращения 30.03.2017).

6. Клебанова И. В. Применение систем радиосвязи для оперативного управления горнотранспортными комплексами в карьерах [Электронный ресурс] // Труды МАИ, № 89. URL: http://www.mai.ru/science/trudy/published.php?ID=73353 (дата обращения 30.03.2017).

7. Аудит действующей беспроводной сети передачи данных в составе системы управления технологическими процессами в карьерах ГОК ОАО «Карельский окатыш». 16.05.2011 [Электронный ресурс] // Официальный сайт «Группа компаний Дэйтлайн». URL: http://www.dateline.ru (дата обращения 30.03.2017).

8. Altair Product [Электронный ресурс] // Официальный сайт Altair URL: http://www.altair.com/Default.aspx (дата обращения 30.03.2017).

9. ATDI Advanced Spectrum Software [Электронный ресурс] // Официальный сайт ATDI URL: http://www.atdi.co.uk/ (дата обращения 30.03.2017).

10. Forsk: Radio Planning and Optimization Software [Электронный ресурс] // Официальный сайт Forsk URL: http://www.forsk.com/ (дата обращения 30.03.2017).

УДК 004.72

ОБЗОР АРХИТЕКТУРЫ СОВРЕМЕННЫХ МНОГОЯДЕРНЫХ ПРОЦЕССОРОВ И ТЕХНОЛОГИИ NOC

Р. А. Дунайцев, О. Р. Кулебякина

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

В современном мире многоядерные процессоры являются одним из основных направлений развития компьютерной техники. Однако на данный момент прогресс в этом направлении приостановился, так как увеличивать тактовую частоту более не представляется возможным, а увеличение количества ядер процессора более восьми имеет больше отрицательных эффектов, чем положительных. В статье рассматриваются различные архитектуры многоядерных процессоров, анализируются их достоинства и недостатки, а также отмечаются возможные направления развития технологии сетей на кристалле.

SoC, NoC, WiNoC, многоядерный процессор, система на кристалле, сеть на кристалле.

Повышение производительности современных процессоров тесно связано с увеличением количества их ядер. В настоящее время для массового

использования доступны 2-, 4-, 6- и 8-ядерные процессоры. Однако стоит отметить, что простое увеличение числа ядер процессора не приводит к мгновенному росту его производительности, так как необходима еще реализация соответствующих алгоритмов, способных эффективно использовать эти ядра. Также для увеличения производительности процессора может применяться технология системы на кристалле (*System on Chip*, SoC) [1], подразумевающая размещение на кристалле не только ядра, но и других элементов обработки. Такая данная технология позволяет значительно уменьшить энергопотребление и размеры оборудования.

Вычислительная мощность процессоров мобильных устройств (ноутбуков, смартфонов, планшетов) стремительно растет, однако емкость их аккумуляторных батарей увеличилась лишь недавно, да и то незначительно. Конечно, предпринимаются попытки увеличить время жизни аккумуляторных батарей и уменьшить потребление электроэнергии процессором за счет использования энергоэффективных технологий, но параллельно с этим растет и нагрузка на процессор со стороны ресурсоемких приложений и задач.

Вычислительные мощности технологии SoC упираются в пропускную способность шины, связывающей между собой ядра и блоки обработки процессора. Шина представляет собой общую среду передачи данных, к которой подключено несколько блоков процессора. В каждый момент времени лишь один блок может успешно передавать данные, а все остальные – получать. Если нескольким блокам нужно передавать данные одновременно, то возникает коллизия, а значит растет задержка в их доставке. При числе ядер больше 8-ми задержки становятся неприемлемо большими, практически полностью перечеркивая преимущества параллельной работы нескольких ядер. Поэтому важным направлением развития архитектуры многоядерных процессоров стала технология сети на кристалле (*Network on Chip*, NoC) с коммутацией пакетов, которая позволяет объединять больше сотни блоков на одном чипе.

В технологии NoC каждое ядро или блок процессора соединен с коммутатором, через который происходит его общение с другими блоками. Сами коммутаторы объединены в сеть, по которой пакеты данных передаются от одного блока к другому, аналогично пакетам в обычной компьютерной сети. Это значительно упрощает топологию микросхемы и снимает ограничения по масштабированию, так как, в отличие от шины, множество блоков способно общаться одновременно, не мешая друг другу.

Однако для эффективной работы процессора нужно минимизировать задержки до наносекунд и снизить энергопотребление коммутаторов. Коммутаторы должны занимать мало места. Биты должны передаваться параллельно, а не последовательно. Для решения данных задач используются следующие технологии [2]:

1) Virtual bypassing. Позволяет передать пакет практически без задержек за счет того, что заголовок посылается заранее и коммутатор успевает сделать нужные переключения цепей к тому моменту, как придет тело пакета. Таким образом пакет идет без остановок, минуя буфер.

2) Low-swing signaling. Эта технология подразумевает уменьшение разницы между напряжениями 0 и 1, что существенно влияет на энергопотребление.

Эти технологии позволили приблизиться к теоретическим пределам пропускной способности и задержек, а также заметно снизить энергопотребление.

Используя технологию NoC, можно создавать сети со следующими топологиями [3]:

1) Топология shared-bus – самая простая в реализации, но имеет существенный недостаток в виде невысокой пропускной способности.

2) Топология ring – модификация топологии shared-bus – позволяет увеличить полосу пропускания, но, чтобы передать информацию от одного узла к другому, необходимо пройти все узлы сети, что увеличивает задержку.

3) Топология fat tree страдает от избыточного количества маршрутизаторов при увеличении числа узлов.

4) В топологии crossbar каждый узел соединен с другим, однако при применении такой топологии отсутствуют маршрутизаторы, что перекладывает задачи маршрутизации на сами узлы.

5) Топологии mesh и torus широко применяются в многопроцессорных архитектурах из-за простоты в реализации и хорошей масштабируемости. Топология torus показывает лучше результаты по производительности, чем mesh, однако топология mesh менее избыточна.

Следует отметить, что все перечисленные топологии имеют свои плюсы и минусы и, соответственно, топологию сети следует выбирать под требования конкретной задачи.

Одним из направлений развития технологии NoC с целью минимизации задержек является технология беспроводной сети на кристалле (*Wireless* NoC, WiNoC). Для реализации бесконтактных соединений между слоями микросхемы могут использоваться эффекты емкостной связи между миниатюрными контактными площадками или индуктивной – между спиральными катушками индуктивности. Среди возможных подходов к реализации WiNoC в первую очередь следует отметить использование в одном чипе и беспроводных, и традиционных проводных линий передачи сигналов. При этом вся сеть условно делится на подсети из групп ядер, внутри которых коммуникация осуществляется по проводным линиям. Каждая такая подсеть оборудована базовой станцией (БС), обеспечивающей передачу

и получение пакетов данных по радиоканалам от других подсетей. Все ядра в подсети связаны с их БС через проводные линии связи. Передача пакета данных между ядрами разных подсетей осуществляется сначала локально до соответствующей БС, затем беспроводным способом до БС подгруппы, в которой находится адресат и далее – по проводной линии к пункту назначения.

Список используемых источников

1. Jose L. Ayala. Communication Architectures for Systems-on-Chip. CRC Press, 2011, 449 p.

2. Сеть на кристалле – мини-интернет внутри процессора [Электронный ресурс]. URL: http://www.rusdoc.ru/articles/set_na_kristalle__mini-internet_vnutri_protsessora/20021/ (дата обращения 30.03.2017).

3. Sudeep Pasricha, Nikil Dutt. On-Chip Communication Architectures. Morgan Kaufmann, 2008, 544 p.

УДК 004.42

ОБЗОР ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ СБОРА И АНАЛИЗА ВЫСОКОСКОРОСТНОГО ТРАФИКА

Р. А. Дунайцев, А. А. Москалюк

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

В последнее время наблюдается существенный рост скоростей передачи данных, а каналы передачи данных со скоростью 1 Гбит/с и более получают все более широкое распространение. Соответственно, встает вопрос об эффективности сбора и анализа трафика, передающегося с такими высокими скоростями, так как те методы, которые применялись ранее, становятся малопригодными.

анализ трафика, сбор трафика, захват трафика, высокоскоростной трафик.

С учетом роста скоростей каналов связи и объемов, передаваемых по ним данных, те методы сбора и анализа трафика, которые успешно использовались ранее, сегодня оказываются непригодными или малоэффективными. Например, компанией Cisco был разработан протокол NetFlow, который позволяет не анализировать каждый пакет в отдельности, а транзакции и потоки целиком [1]. Таким образом намного проще и удобнее анализировать трафик.

Wireshark – это один из самых известных анализаторов трафика или снифферов, который используется повсеместно [2]. Его особенность в том, что он поддерживает практически все существующие протоколы, а также имеет большое количество возможностей для анализа трафика. Wireshark удобно использовать тогда, когда необходимо изучить отдельный пакет или отдельную транзакцию. Когда же объемы трафика очень велики, использование Wireshark оказывается неэффективным, а то и просто невозможным, так как программа не в состоянии оперировать столь большими объемами данных. Однако Wireshark включает возможность анализа потоков, что позволяет при небольших объемах трафика построить картину того, как и куда обращаются пользователи сети. На рис. 1 представлен пример такого анализа.

Для анализа больших объемов трафика хорошо подходит продукт ntopng компании ntop [3]. Компания ntop также известна своими разработками для углубленного анализа пакетов (*deep packet inspection*, DPI). Для сбора большого количества трафика компания предлагает nProbe Cento – продукт, который может собирать трафик, передаваемый на скоростях от 40Гбит/с. Для просмотра собранного трафика и анализа пакетов, а также просмотра общей статистики сети используется продукт ntopng.

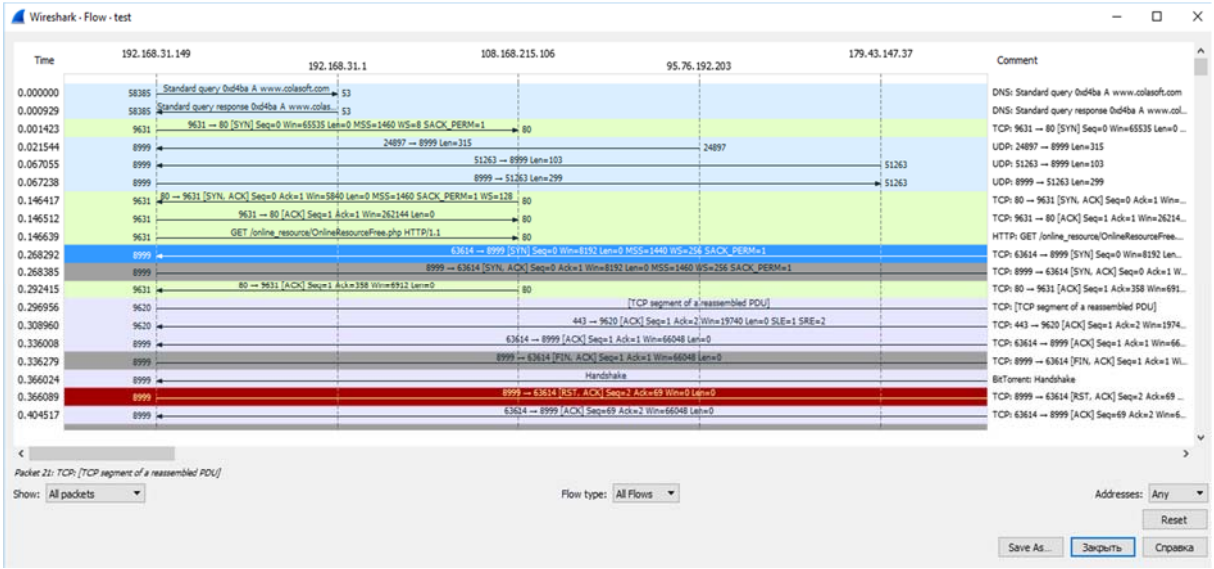


Рис. 1. Анализ потоков в программе Wireshark

ntopng имеет веб-интерфейс, с помощью которого и происходит взаимодействие с пользователем. В качестве сборщика трафика выступает nProbe Cento, с помощью которого можно собирать и анализировать очень большие объемы трафика. На рис. 2 показан пример представления трафика в ntopng.

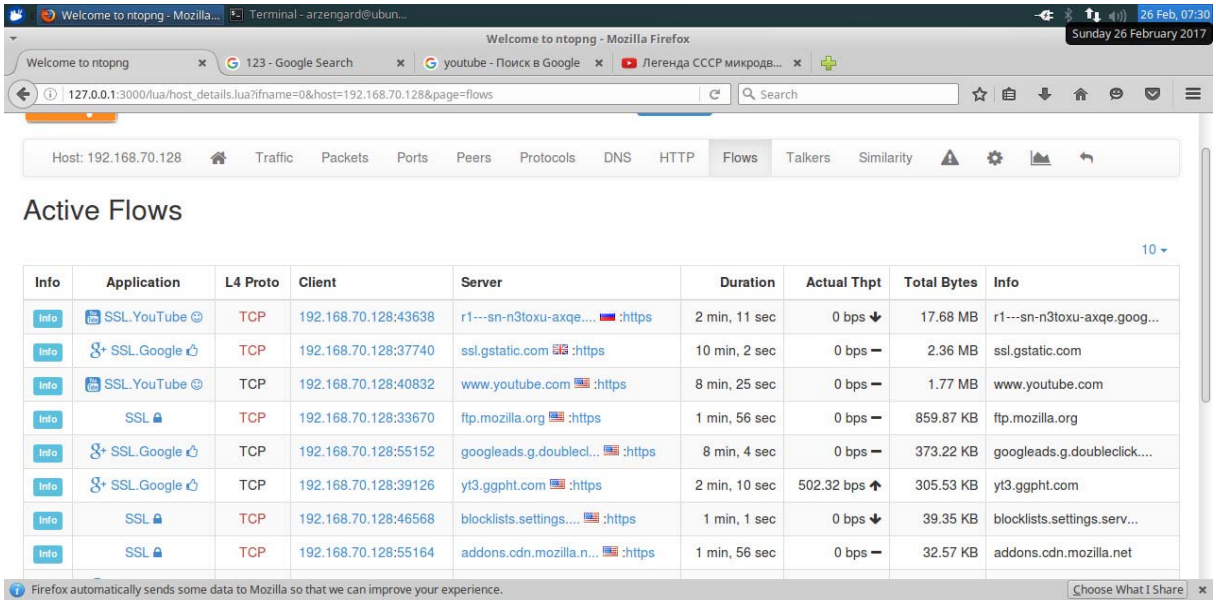


Рис. 2. Анализ потоков в программе в ntopng

Для анализа трафика в ntopng существует множество функций. Одна из них – это демонстрация наиболее активных участников транзакций (ширина канала на картинке динамически изменяется, рис. 3). Также поддерживается сохранение трафика отдельного узла в формате *.pcap для более углубленного анализа. Программа ntopng имеет возможность разделять файлы, при достижение определенного количества пакетов в них, что, безусловно, очень удобно для последующего анализа средствами Wireshark.

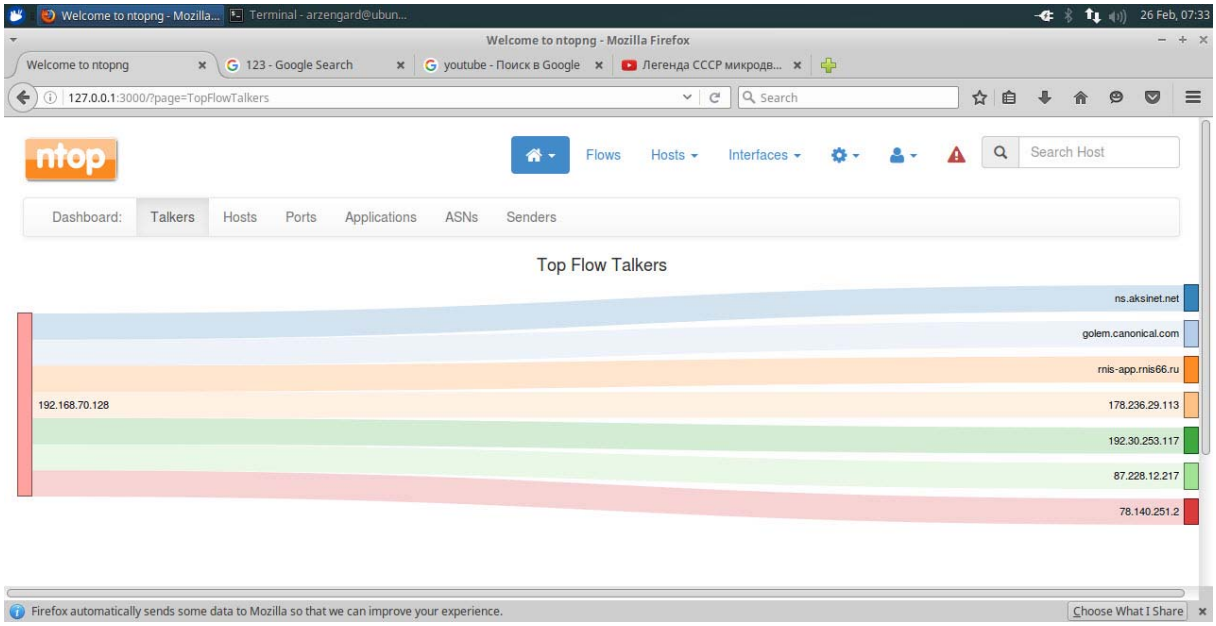


Рис. 3. Самые активные пользователи

Третий продукт, на который нужно обратить внимание – это SteelCentral Packet Analyzer компании Riverbed Technology [4]. Данное решение также поддерживает экспорт собранного трафика в Wireshark и другие аналогичные программы. SteelCentral Packet Analyzer также, как и ntopng, может формировать различные графики, например, на рис. 4 представлены график загруженности канала.

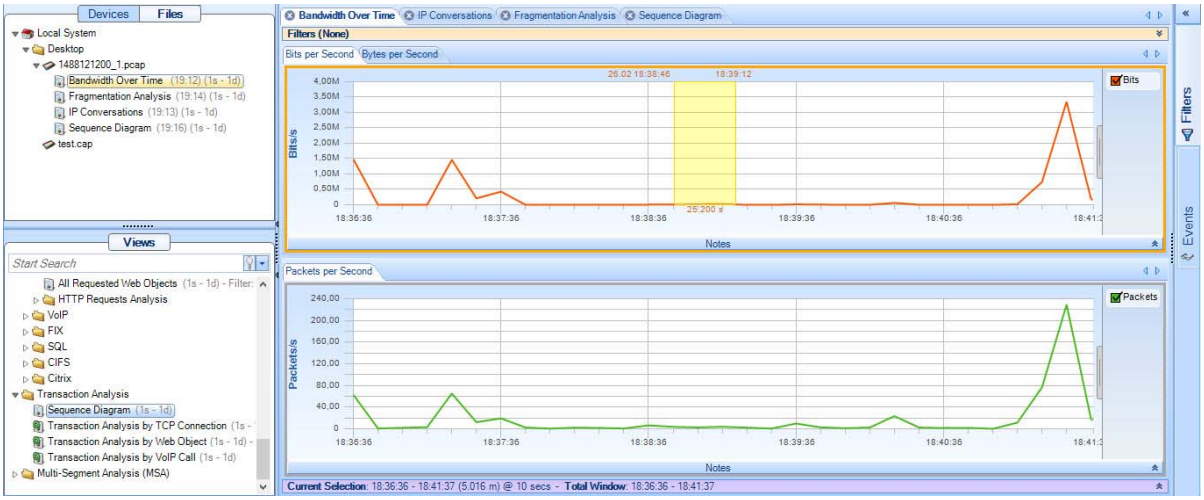


Рис. 4. Загруженность канала в единицу времени

Анализ потоков посредством SteelCentral Packet Analyzer достаточно затруднителен (пример такого графика представлен на рис. 5). На этом графике сложно отличить отдельные транзакции. Даже имея возможность выделить какую-либо транзакцию сложно понять, как и с кем она происходила.

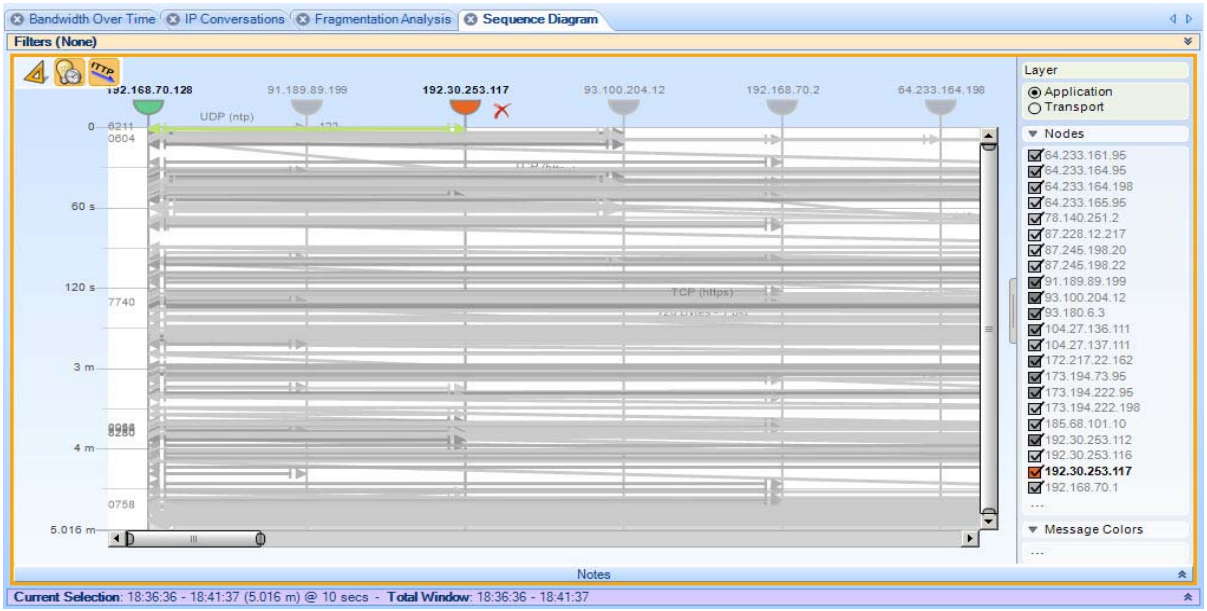


Рис. 5. Анализ потоков в программе SteelCentral Packet Analyzer

В заключение хочется еще раз отметить весьма удачный подход компании ntop к организации сбора и анализа трафика: веб-интерфейс обеспечивает мультиплатформенность, анализатор не перегружен различными кнопками и выглядит лаконично, и, что самое важное, все графики наглядны и позволяют легко определить проблему в сети. Минусом nProbe является довольная сложная установка и настройка.

Список используемых источников

1. Cisco IOS NetFlow [Электронный ресурс]. URL: http://www.cisco.com/c/en/us/products/ios-nx-os-software/ios-netflow/index.html (дата обращения 29.03.2017).

2. Wireshark [Электронный ресурс]. URL: https://www.wireshark.org/ (дата обращения 29.03.2017).

3. nProbe Cento [Электронный ресурс]. URL: http://www.ntop.org/products/netflow/nprobe-cento/ (дата обращения 29.03.2017).

4. SteelCentral Packet Analyzer [Электронный ресурс]. URL: https://www.riverbed.com/ru/products/steelcentral/steelcentral-packet-analyzer-personal-edition.html (дата обращения 29.03.2017).

УДК 004.732

РАДИООБСЛЕДОВАНИЕ ОБЩЕЖИТИЯ «ЛЕСНОЕ» СПбГУТ

Р. А. Дунайцев, Д. А. Наумичева

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

В статье представлены результаты радиообследования общежития «Лесное», принадлежащего СПбГУТ. В ходе работы с помощью специализированного программного обеспечения были собраны данные по числу установленных проживающими Wi-Fi роутеров, используемые этими роутерами частотные каналы и диапазоны, а также методы шифрования и версии стандарта IEEE 802.11.

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

Ни один студент в наше время не может обойтись без современных информационных технологий: рефераты, курсовые работы, доклады – все это подразумевает поиск дополнительной информации, которую, разумеется, легче всего найти в глобальной сети Интернет. Для студентов, проживающих в общежитии, очень важно, чтобы у них был выход в Интернет со всех имеющихся цифровых устройств: настольных компьютеров, ноутбуков,

планшетов и смартфонов. «Лесное» – общежитие коридорного типа с небольшими комнатами, рассчитанными на 2–3 человека (рис. 1), при этом кабель в комнату заводится только один. Поэтому для одновременного доступа в Интернет студенты устанавливают у себя в комнатах и собственноручно настраивают Wi-Fi роутеры (далее «точки доступа», ТД), что позволяет им пользоваться как технологией Ethernet с проводным подключением, так и Wi-Fi с беспроводным доступом. К сожалению, очень часто при настройке ТД в своих комнатах студенты не задумываются об особенностях беспроводной среды передачи и тонкостях радиочастотного планирования.

Рис. 1. Расположение комнат в общежитии «Лесное»

Целью работы был анализ характеристик сетей Wi-Fi в общежитии «Лесное». Для этого была использована программа Ekahau Site Survey версии 8.6.2 [1], установленная на ноутбуке. В программу были загружены поэтажные планы здания, затем планы этажей были выровнены по контрольным точкам, задана высота потолков и толщина перекрытий. Поскольку радиообследование проводилась в рамках студенческой исследовательской работы, пришлось ограничиться лишь обходом коридоров без посещения комнат. Радиообследование проводилось в пошаговом (stop-and-go) режиме: отметив свое текущее местоположение на плане соответствующего этажа, запускали сканирование каналов Wi-Fi, оставаясь на месте до завершения цикла сканирования. Затем перемещались на несколько метров вперед, и процедура повторялась. Проход по коридору осуществлялся дважды, при этом внешний адаптер сперва находился ближе к комнатам по одну сторону коридора, а на обратном пути – ближе к комнатам по другую сторону. На рис. 2 места проведения сканирований отмечены зелеными кружками.

Поскольку встроенный в ноутбук адаптер Atheros AR956x поддерживает лишь диапазон 2,4 ГГц, то для полноты картины было решено использовать внешний адаптер Linksys WUSB6300, который поддерживает как диапазон 2,4 ГГц, так и диапазон 5 ГГц.

В результате радиообследования программа выявила 211 ТД, из них около 60 % сумела распределить по этажам. Обнаруженные ТД можно отсортировать по следующим показателям: используемые методы шифрования, поддерживаемые диапазоны и версии стандарта IEEE 802.11 [2], ширина каналов.

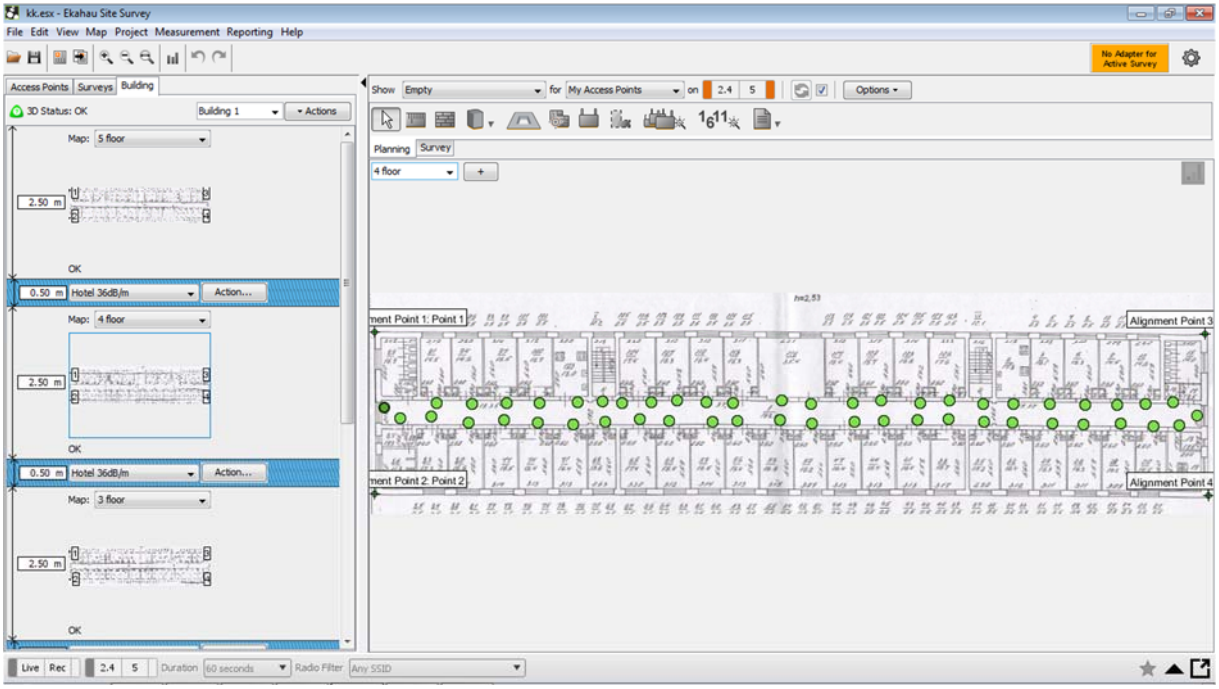


Рис. 2. Окно программы Ekahau Site Survey

Анализ собранных данных, представленных в таблице 1, показывает, что открытых ТД всего 3, а с шифрованием WEP нет вообще. Это означает, что студенты используют современные ТД, которые не так просто «взломать». Абсолютное большинство ТД использует метод шифрования WPA2, что является хорошим показателем.

ТАБЛИЦА 1. Используемые методы шифрования

Шифрование	Число ТД	Доля, %
Нет (Open)	3	1,4
WEP	0	0
WPA	6	2,8
WPA2	202	95,8
ВСЕГО	211	100

Результаты в таблице 2 позволяют предположить, что в данном общежитии нет ТД, работающих в диапазоне 5 ГГц. Конечно, программа могла просто не «услышать» такие ТД, так как чем выше частота сигнала, тем больше он подвержен затуханию. Но эту гипотезу можно практически исключить, поскольку стены в общежитии очень тонкие, двери деревянные, а максимальное расстояние от ноутбука с Ekahau Site Survey до ближайшей ТД в каждой точке сканирования не могло превышать 6 метров (замеры проводились напротив каждой комнаты, длина которых в данном общежитии

составляет 5,6 м). Также из таблицы 2 видно, что в основном используются ТД с версией стандарта IEEE 802.11n.

ТАБЛИЦА 2. Используемые диапазоны и версии стандарта IEEE 802.11

IEEE 802.11	2,4 ГГц	5 ГГц
b	1	–
g	14	–
n	196	0
a	–	0
ac	–	0
ВСЕГО	211	0

Самым важным в работе было изучение частотных каналов и соблюдения правил радиочастотного планирования [3]. Поскольку ТД устанавливаются и настраиваются не централизованно администрацией общежития, а самими студентами, частотно-территориальное планирование как таковое отсутствует, повсеместно наблюдается наложение как одноименных (*co-channel overlap*), так и смежных (*adjacent-channel overlap*) каналов [4] [5].

В общежитии было выявлено 88 ТД с шириной канала 20 МГц и 123 ТД с шириной канала 40 МГц (табл. 3 и 4 соответственно). Из этого можно сделать вывод, что, хотя объединение каналов (*channel bonding*) в диапазоне 2,4 ГГц и не рекомендуется к использованию, но, тем не менее, широко применяется пользователями при настройке своего оборудования.

Из таблицы 3 видно, что в основном ТД используют каналы 1, 6 и 11, которые лежат в основе радиочастотного планирования сетей Wi-Fi в диапазоне 2,4 ГГц, так как данные каналы практически не пересекаются и не создают взаимной интерференции. Возможно, эти каналы установлены в ТД по умолчанию, либо сами студенты выбирают один из этих каналов, будучи знакомы с «классической» схемой 1/6/11. Но все преимущества непересекающихся каналов перечеркиваются использованием каналов 2, 3, 4, 5, 7, 8, 9, 10, 12, и 13. Возможно, выбор этих каналов производится ТД автоматически в поисках незанятого канала, либо же сами владельцы вручную устанавливают данные каналы в настройках своих ТД.

ТАБЛИЦА 3. Используемые каналы шириной 20 МГц

№ канала	1	2	3	4	5	6	7	8	9	10	11	12	13
Число ТД	13	5	2	3	4	23	2	1	6	6	13	0	10
ВСЕГО	88 (42 % от общего числа обнаруженных ТД)												

ТАБЛИЦА 4. Используемые каналы шириной 40 МГц

№№ каналов	1+5 5+1	2+6 6+2	3+7 7+3	4+8 8+4	5+9 9+5	6+10 10+6	7+11 11+7	8+12 12+8	9+13 13+9
Число ТД	25	17	17	13	7	11	24	3	6
ВСЕГО	123 (58 % от общего числа обнаруженных ТД)								

Итак, в результате проведенного радиообследования было выявлено, что в основном студенты используют современные ТД с шифрованием WPA2 и поддержкой стандарта IEEE 802.11n. Все обнаруженные ТД работают в диапазоне 2,4 ГГц. К сожалению, принципы территориально-частотного планирования не соблюдаются и часто расположенные рядом ТД используют либо одноименные, либо смежные каналы. Кроме того, около 60 % ТД использует каналы шириной 40 МГц, создавая помехи для своих соседей.

Список используемых источников

1. Ekahau Wi-Fi Design Solutions [Электронный ресурс]. URL: https://www.ekahau.com/ (дата обращения 29.03.2017).

2. IEEE Std 802.11-2012 (Revision of IEEE Std 802.11-2007). 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. 29 March 2012.

3. О важности радиоразведки и радиопланирования при развертывании Wi-Fi сетей [Электронный ресурс]. URL: http://www.pcweek.ua/themes/detail.php?ID=148474 (дата обращения 29.03.2017).

4. Why Channels 1, 6 and 11? [Электронный ресурс]. URL: http://www.metageek.com/training/resources/why-channels-1-6-11.html (дата обращения 29.03.2017).

5. Adjacent and Co-Channel Congestion [Электронный ресурс]. URL: http://www.metageek.com/training/resources/adjacent-channel-congestion.html (дата обращения 29.03.2017).

УДК 004.75

ОБЗОР ОБЛАЧНЫХ ИГРОВЫХ СЕРВИСОВ

Р. А. Дунайцев, О. Д. Романова

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

Данная статья посвящена рассмотрению набирающей популярность технологии под названием «облачные игровые сервисы». В ходе исследования были проанализиро-

ваны следующие моменты: история возникновения, типы игровых сервисов и их характеристики, принципы работы, успехи и ошибки первых компаний в данной сфере, технические возможности и перспективы.

OnLive, Playkey, облачные игровые сервисы.

С каждым годом технический прогресс увеличивает темпы, что позволяет разработчикам игр добиваться все более реалистичной графики и все более увлекательного игрового процесса, тем самым привлекая к своему продукту внимание целевой аудитории. Но постоянно поддерживать «железо» своего ПК на топовом уровне, как того требуют новинки игровой индустрии – задача не из дешевых, что заставляет пользователей иногда отказывать себе в удовольствии поиграть в недавно вышедшую игру. Поэтому на данный момент стал актуален вопрос об использования облачных игровых сервисов, дающих возможность большому числу игроков обойтись без дорогостоящего апгрейда имеющегося ПК или покупки нового. Для начала стоит разобраться, что же такое в принципе «игры в облаке». Под играми в облаке (*cloud gaming*) подразумевают обеспечение удаленного доступа к играм, запущенным на сервере компании и не требующим их установки на ПК пользователя. Среди них можно выделить 3 типа:

1) Системы с потоковой передачей части игры по мере надобности (*file streaming*): с покупкой игры происходит загрузка части кода (примерно 5 %) на ПК для ее мгновенного запуска; остальная же часть загружается и устанавливается по ходу игры (проекты *Kalydo* и *Utomik*).

2) Системы с передачей потокового видео (*video streaming*): хостинг и обработка игрового контента происходит на удаленном сервере (проекты *OnLive*, *LiquidSky* и *Playkey*). Здесь выделяют 2 подтипа:

- системы с возможностью играть только в доступные у поставщика сервиса игры;
- системы с покупкой ресурса на удаленном сервере, на котором будет запускаться купленный в Steam или другого поставщика контент.

3) Системы с передачей данных с одного устройства пользователя на другое: процесс обработки контента происходит на домашней приставке, а данные передаются на ПК (*remote play*).

В связи с тем, что video streaming является наиболее распространенным и востребованным типом сервисов, речь в данной статье пойдет именно о нем.

Момент возникновения идеи об облаках различные источники относят к разным годам. К примеру, по мнению компании Big Fish (разработчика казуальных компьютерных игр), идея появилась еще в 1950-х годах [1]. Информация на сайте Википедии утверждает иное время – 1960-е [2]. Игровые

сервисы появились намного позже, но закрепиться на рынке смогли далеко не все.

Первыми сервисами в данной области, достигшими больших успехов, можно назвать OnLive и Gaikai. Принцип работы у проектов был схожим. Игра, запрашиваемая пользователем, обрабатывалась на удаленном сервере, а игрок получал потоковое видео игрового процесса и возможность управления им. Команды пользователя (нажатия клавиш, движения мышью, т. д.) поступали на сервер по шифрованному соединению, обрабатывались, а их результаты отправлялись видеопотоком обратно. При подключении игрока к сервису производился поиск сервера с наименьшим показателем задержки. Все игровые файлы (т. н. «сохранения») и профили игроков хранились на удаленном сервере. Тем самым единственное, что требовалось от игрока, – это ПК со средними характеристиками и стабильное Интернет-соединение с низкой задержкой (на данный момент минимальная требуемая скорость соединения составляет 5 Мбит/с). Ныне существующие проекты работают по аналогичной схеме.

В 2009 г. на конференции Game Developers Conference был анонсирован первый игровой облачный сервис OnLive, позволявший пользователям играть в то, что они желают, а не в то, что может потянуть их маломощный ПК. Компания разработала ряд передовых на то время технологий. Одной из них был аппаратный чип, отвечающий за работу видеокодека для видеокомпрессии (сжатое видео передавалось по Интернет-соединению и декодировалось на стороне пользователя), запатентованный создателями OnLive. Ими также был разработан чип для обеспечения стабильной работы системы с минимальными задержками при обеспечении хорошего соединения со стороны пользователя. Однако это не спасло компанию от банкротства, причиной которого в основном стали вопросы менеджмента и рентабельности: начиная от недостаточного разнообразия игр в библиотеке и заканчивая финансовыми проблемами. OnLive использовал подписочную модель с абонентской платой за использование того или иного сборника игр. Это не позволяло пополнять библиотеку хитами и новинками, так как было невыгодно издателям. Количество серверов (которые размещались только в пределах США) и затраты на их содержание (в первую очередь оборудование собственного производства) не окупались вследствие того, что одновременно сервис посещался небольшим количеством пользователей, многие из которых ограничивались бесплатным тестовым доступом.

В 2012 г. активы компании были проданы, позже проект был перезапущен. Но ни передовые технологии, ни использование сервиса CloudLift, позволяющего выбирать игры из Steam и продолжать прерванную сессию на любом другом устройстве, не помогли OnLive укрепить позиции. В 2015 г. патенты были проданы компании Sony и проект прекратил свое существование.

Сервис Gaikai, анонсированный в том же 2009 г. на конференции Game Developers Conference, был успешнее своего конкурента. Создатели характеризовали его как проект, созданный «для реального Интернета». В первую очередь это выражалось в требованиях к соединению: была необходима меньшая скорость (от 0,5 до 2 Мбит/с, тогда как *OnLive* требовал от 1,5 до 5 Мбит/с). В то же время задержка составляла в среднем 55 миллисекунд. Серверы Gaikai размещались не только в США, но и в Европе, что давало преимущество перед OnLive. Стоит также учесть выбор иной бизнес-модели, позволившей увеличивать расходы постепенно с притоком клиентов: масштабируемая модель подразумевала создание изначально небольшой по мощности и территории охвата сети серверов, которая увеличивалась пропорционально росту числа пользователей, что позволило не тратить с самого начала огромные денежные средства на поддержку оборудования. Как и OnLive, Gaikai использовал для работы на клиентском оборудовании веб-браузер, но первый требовал установку специального плагина, тогда как последний – ничего (использовалась технология *Adobe Flash*). Еще одно отличие – услуги, которые предоставляли сервисы. Gaikai был нацелен на производителя компьютерных игр, предоставляя ему платформу для демоверсий своих новинок. Пользователь мог бесплатно попробовать продукты из широкого ассортимента, что давало игроку возможность не только ознакомиться с игрой перед потенциальной покупкой, не скачивая и не устанавливая на свой ПК пробную версию. В 2012 г. проект был продан компании Sony, которая основала на готовых технологиях сервис PlayStation Now, существующий и на сегодняшний день.

Несмотря на то, что на 2012 г. OnLive и Gaikai обладали схожими технологиями по уровню, судьбы проектов отличаются. И основную роль в этом сыграло не новаторство в техническом вопросе, а грамотный менеджмент и правильная расстановка приоритетов на каждом этапе развития компании.

Сегодня существует ряд проектов, предоставляющих аналогичные услуги. Сервис LiquidSky [3], находящийся на данный момент в режиме бета-тестирования, разработан на технологии Nvidia GRID (платформа для виртуализации графики, обеспечивающая ускорение работы виртуальных рабочих столов и приложений на графических процессорах Nvidia). Сервис предоставляет игрокам возможность установить на удаленном сервере купленные ими в Steam игры и запускать их, оставаясь при этом в системе Steam. На данный момент проект насчитывает более 500000 пользователей.

Playkey [4] – отечественный проект, работающий также на технологии Nvidia GRID. В самом начале своего запуска (2014–2015 гг.) компания допускала те же ошибки, что и OnLive, но смогла изменить ситуацию, пересмотрев бизнес-модель. Фокус был переведен на игры, которые имели

высокие системные требования и пользовались спросом. Тем самым изменилась подписка (от оплаты каталога игр к использованию серверных мощностей), ставшая более привлекательной: доступ предоставляется к 150 бесплатным играм и возможность покупать остальные по желанию. На 2016 г. количество зарегистрированных пользователей составляло около 200000, оформивших подписку – 10000, и 4000 постоянно платящих проекту. Оба проекта LiquidSky и Playkey требуют установку своего приложения на ПК пользователя.

Упомянутый ранее PlayStation Now позволяет играть в игры для PlayStation 3 на ПК, телевизорах, мобильных устройствах, PlayStation 3, PlayStation 4, PlayStation Vita [5]. Сервис был запущен на территории США в 2015 г., в 2016 – в Британии, Бельгии, Нидерландах. Используется также подписная модель, дающая доступ к 400 играм для PS3. Для использования необходимо скачать приложение и иметь джойстик.

Каждый проект интересен по-своему и имеет ряд преимуществ и недостатков. Ближайший к российскому пользователю сервер LiquidSky расположен в Германии, что сказывается на задержках и общем комфорте игры. У Playkey отсутствует синхронизация с Steam, однако игрок может выбрать любую игру из библиотеки и практически мгновенно запустить ее, тогда как LiquidSky требует время на загрузку и установку. Сервер PlayStation Now, к сожалению, недоступен в России на данный момент.

Однозначно использование облачных игровых серверов – это экономия на покупке нового ПК. Проще использовать уже существующее и подходящее по всем параметрам оборудование. Современные игры могут достигать размеров в 10–20 ГБ, поэтому их запуск на удаленном сервере позволяет освободить место на локальном диске. Подобные проекты дают возможность использовать продукт вне зависимости от того, на какое устройство изначально он был ориентирован: запуск возможен с телефона, планшета, телевизора, приставки, ПК.

В то же время встает проблема Интернет-соединения. Качество поступающего видеопотока будет потреблять тем больше ресурсов, чем выше разрешение и детализация (поэтому поставщики нередко сжимают размер картинки). Расход трафика (до 3 ГБ за час игры) при распространении услуги может привести к чрезмерной нагрузке на сеть. Не стоит забывать, что задержка была, есть и будет, поэтому игра, установленная на ПК, будет работать быстрее, нежели в облаке. Да и сами подписки и покупки игр на серверах – это всего лишь их аренда, и она не защищена от банкротства компаний.

Подводя итог, отметим, что облачные игровые сервисы – это выход для пользователей, не готовых постоянно обновлять собственное оборудование и не тратящих большое количество времени на игры (зачастую подписки рассчитаны на определенное игровое время в течение месяца).

Использование собственного ПК остается пока более надежным и качественным вариантом. Но технологии развиваются, как и качество каналов доступа в Интернет, поэтому облачные игровые сервисы будут только набирать популярность.

Список используемых источников

1. The Rise of Cloud Gaming [Электронный ресурс]. URL: http://www.bigfish-games.com/daily/cloud-gaming/static/ (дата обращения 30.03.2017).

2 Cloud gaming [Электронный ресурс]. URL: https://en.wikipedia.org/wiki/Cloud_gaming (дата обращения 30.03.2017).

3. The Ultimate Free Cloud Gaming PC [Электронный ресурс]. URL: https://liquidsky.com/ (дата обращения 30.03.2017).

4. PLAYKEY | игры онлайн [Электронный ресурс]. URL: https://playkey.net/ru/intro_know/ (дата обращения 30.03.2017).

5. PlayStation Now [Электронный ресурс]. URL: https://www.playstation.com/ (дата обращения 30.03.2017).

УДК 004.732

РАДИООБСЛЕДОВАНИЕ ОБЩЕЖИТИЯ «РЫБАЦКОЕ» СПбГУТ

Р. А. Дунайцев, А. В. Тампио

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

В статье рассматриваются результаты радиообследования, проведенного в общежитии «Рыбацкое» СПбГУТ. Проводится анализ количества установленных студентами Wi-Fi роутеров, используемых частотных диапазонов и каналов, методов шифрования и версий стандарта IEEE 802.11. Приводятся данные по скорости передачи в нисходящем (download) и восходящем (upload) направлениях при использовании Ethernet и Wi-Fi.

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

Жизнь современного человека невозможно представить без доступа к ресурсам глобальной сети Интернет. Что уж говорить про студентов, для которых Интернет – это не только среда общения и развлекательный контент, но и доступ к всевозможным учебным и научным материалам. Поэтому возможность подключения к сети Интернет необходима не только

на территории ВУЗа, но и в студенческих общежитиях. Согласно результатам мониторинга трафика, в общежитиях ВУЗов Москвы пятая часть всех запросов приходится на образовательные ресурсы [1].

В то время как точки доступа (ТД) в московских общежитиях входят в бесплатную городскую Wi-Fi сеть и устанавливаются централизовано [2], в большинстве студенческих общежитий других городов, в лучшем случае, на нескольких проживающих приходится всего одна розетка RJ-45. Так как в среднем у каждого студента имеется два и более устройств с выходом в Интернет [1], для реализации возможности одновременного доступа студенты сами покупают и устанавливают Wi-Fi роутеры (далее ТД). В результате на территории общежития функционирует множество Wi-Fi сетей, каждая из которых состоит из одной ТД и нескольких клиентских устройств, использующих ее для выхода в Интернет.

«Рыбацкое» – это общежитие квартирного типа с 2–3 комнатами в квартире, в каждой из которых проживают 2–3 студента (рис. 1). Целью данного исследования было определить количество действующих ТД, используемые частотные диапазоны и каналы, методы шифрования и версии стандарта IEEE 802.11 [3]. Для этого была выбрана программа Ekahau Site Survey версии 8.6.2 [4], устанавливаемая на ноутбуке. Так как встроенный в ноутбук адаптер Dell Wireless 1703 поддерживал лишь диапазон 2,4 ГГц, для сканирования каналов в обоих диапазонах было решено использовать внешний USB-адаптер. Обход общежития совершался по коридорам этажей, но без посещения жилых помещений.

Рис. 1. Общий коридор общежития «Рыбацкое» и тамбур квартиры с двумя комнатами

Сперва в качестве внешнего адаптера был выбран D-Link DWA-160/B [5]. Но поскольку, проходя лишь по коридорам, мы находимся доста-

точно далеко от ТД, установленных в комнатах и отделенных от нас несколькими стенами и металлическими дверями, чувствительность адаптера позволила Ekahau Site Survey определить примерное местоположение лишь 10 % ТД из всех обнаруженных в процессе радиообследования (рис. 2). Поэтому D-Link DWA-160/B был заменен высокочувствительным адаптером NETGEAR A6210 с откидной антенной [6]. С его помощью программе удалось расставить по этажам более 30 % обнаруженных ТД (рис. 3).

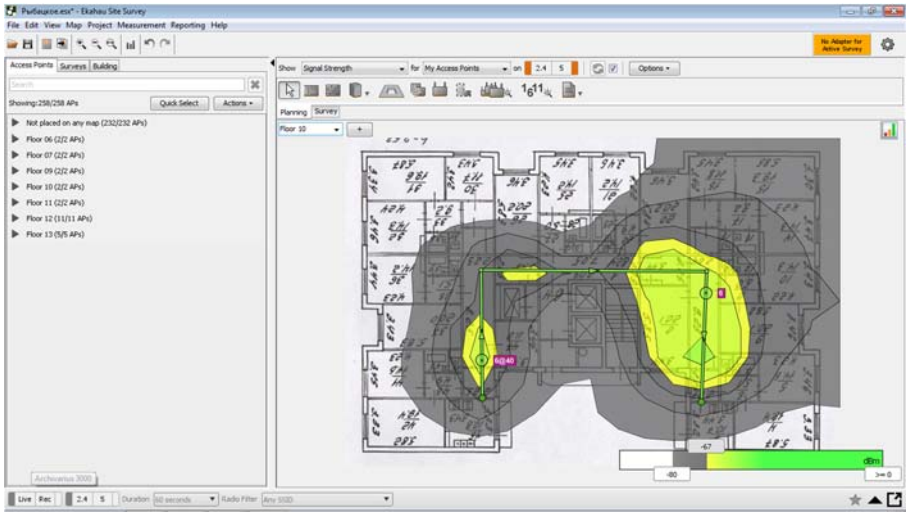


Рис. 2. Карта покрытия при использовании внешнего адаптера D-Link DWA-160/B

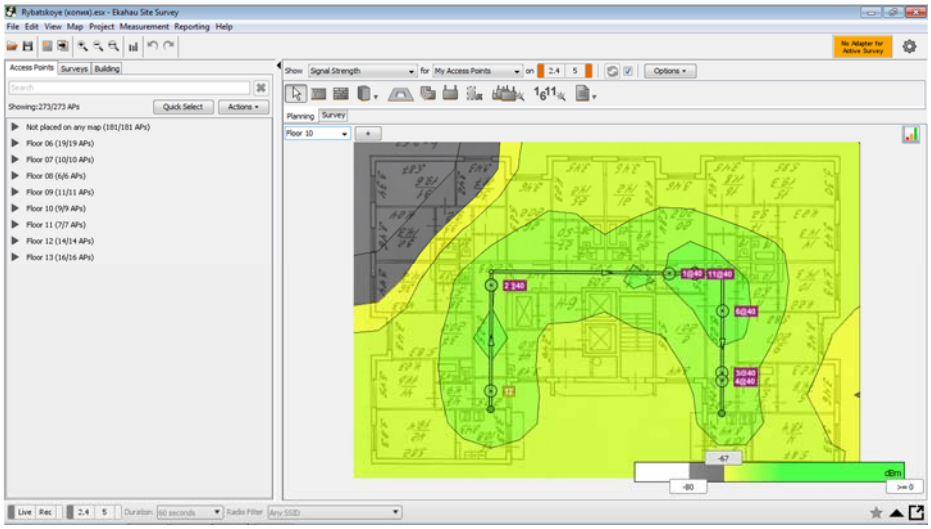


Рис. 3. Карта покрытия при использовании внешнего адаптера NETGEAR A6210

Радиообследование проводилось в непрерывном (continuous) режиме: отметив свое начальное местоположение на плане этажа, мы двигались равномерно и прямолинейно по коридору, делая в программе отметку всякий раз, когда направление движения изменялось (рис. 2 и 3). Все это время шло сканирование каналов Wi-Fi, а затем данные, собранные между двумя по-

следовательными отметками, равномерно распределялись между этими точками. По достижении конца коридора, ставилась последняя отметка на плане этажа и сбор данных прекращался.

В ходе радиообследования программа выявила 333 ТД. Самым распространенным методом шифрования оказался WPA2, тогда как WPA используют менее 5% обнаруженных ТД, а WEP не используется вообще (табл. 1).

ТАБЛИЦА 1. Используемые методы шифрования

Шифрование	Число ТД	Доля, %
Нет (Open)	6	1,8
WEP	0	0
WPA	16	4,8
WPA2	311	93,4
ВСЕГО	333	100

Согласно данным, представленным в таблице 2, наиболее активно используется диапазон 2,4 ГГц, в то время как в диапазоне 5 ГГц работает всего 9 ТД. Однако, как известно, чем выше частота радиосигнала, тем он более подвержен затуханию при прохождении через препятствия (стены, двери, шкафы и т. п.). Поэтому возможно, что в общежитии были и другие ТД, работающие в диапазоне 5 ГГц, но сигнал от них в коридоре был столь слаб, что адаптер их просто не «услышал».

Как видно из таблицы 2, большинство ТД использует версию стандарта 802.11n, работая при этом в смешанном режиме (mixed mode), который позволяет использовать как устройства 802.11n, так и 802.11b/g.

ТАБЛИЦА 2. Используемые диапазоны и версии стандарта IEEE 802.11

IEEE 802.11	2,4 ГГц	5 ГГц
b	1	–
g	3	–
b, g	45	–
b, g, n	271	–
g, n	4	–
a, n	–	4
a, n, ac	–	5
ВСЕГО	324	9

Согласно данным таблицы 3, в диапазоне 2,4 ГГц примерно половина ТД использует каналы шириной 20 МГц, причем наиболее часто выбираются каналы 1, 6 и 11. В таблице 4 представлена собранная статистика по ТД в диапазоне 2,4 ГГц с шириной канала 40 МГц.

ТАБЛИЦА 3. Используемые каналы шириной 20 МГц в диапазоне 2,4 ГГц

№ канала	1	2	3	4	5	6	7	8	9	10	11	12	13
Число ТД	30	12	6	5	10	36	2	8	3	4	29	6	16
ВСЕГО	167 (51,5 % от общего числа ТД, работающих в диапазоне 2,4 ГГц)												

ТАБЛИЦА 4. Используемые каналы шириной 40 МГц в диапазоне 2,4 ГГц

№№ каналов	1+5 5+1	2+6 6+2	3+7 7+3	4+8 8+4	5+9 9+5	6+10 10+6	7+11 11+7	8+12 12+8	9+13 13+9
Число ТД	28	22	15	21	14	15	22	5	15
ВСЕГО	157 (48,5 % от общего числа ТД, работающих в диапазоне 2,4 ГГц)								

В диапазоне 5 ГГц обнаруженные ТД используют каналы шириной 20, 40 и 80 МГц, использования каналов шириной 160 МГц зафиксировано не было (табл. 5).

ТАБЛИЦА 5. Используемая ширина канала в диапазоне 5 ГГц

IEEE 802.11	20 МГц	40 МГц	80 МГц
a, n	1	3	-
a, n, ac	0	0	5
ВСЕГО	9		

С помощью сервиса [7] в течение одного дня были проведены измерения скорости передачи данных в нисходящем (*download*) и восходящем (*upload*) направлениях. Измерения проводились утром, днем и вечером сериями по 10 тестов, при этом измерения в каждой серии делались попарно с использованием проводного подключения Ethernet и беспроводного Wi-Fi. Полученные средние значения при доверительной вероятности 0,95 представлены в таблице 6. Анализ результатов тестов показал, что скорость проводного соединения в общежитии достаточно низкая и подвержена существенным колебаниям даже на коротком временном отрезке, поэтому использование сервиса [7] и ему подобных внешних ресурсов не позволяет

оценить максимальную скорость передачи беспроводного канала отдельно от проводного участка. В дальнейшем планируется продолжить данные исследования и изучить влияние соседских Wi-Fi сетей путем использования испытательного стенда.

ТАБЛИЦА 6. Средняя скорость загрузки (download) и отправки (upload) данных

	Ethernet, Мбит/с		Wi-Fi, Мбит/с	
	Download	Upload	Download	Upload
Утро	7,8±1,0	10,0±0,9	5,6±1,3	8,7±2,8
День	6,3±1,0	10,3±1,1	6,0±0,9	9,0±1,4
Вечер	9,2±1,0	12,3±2,3	5,5±0,8	7,4±1,3

Список используемых источников

1. Объем Wi-Fi-трафика в московских общежитиях составил 3,5 ПБ за полгода [Электронный ресурс]. URL: http://www.cnews.ru/news/line/2016-08-02_obem_wifitrafika_v_moskovskih_obshchezhitiyah_sostavil (дата обращения 30.03.2017).

2. Общежития студентов подключили к Wi-Fi [Электронный ресурс]. URL: http://www.rspectr.com/news/wi-fi-dormitory/ (дата обращения 30.03.2017).

3. IEEE Std 802.11-2012 (Revision of IEEE Std 802.11-2007). 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. 29 March 2012.

4. Ekahau Wi-Fi Design Solutions [Электронный ресурс]. URL: https://www.ekahau.com/ (дата обращения 30.03.2017).

5. USB-адаптер DWA-160/B [Электронный ресурс]. URL: http://www.dlink.ru/ru/products/2/1158.html (дата обращения 30.03.2017).

6. USB-адаптер NETGEAR A6210 (AC1200) [Электронный ресурс]. URL: http://www.netgear.ru/home/products/networking/wifi-adapters/a6210.aspx (дата обращения 30.03.2017).

7. Speedtest.net by Ookla [Электронный ресурс]. URL: http://www.speedtest.net/ (дата обращения 30.03.2017).

УДК 004.942, 621.39

НЕЛИНЕЙНЫЕ ЯВЛЕНИЯ В ПОЛУПРОВОДНИКОВЫХ ОПТИЧЕСКИХ УСИЛИТЕЛЯХ

Л. Ю. Дуров, А. С. Дюбов

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

В статье рассмотрены конструкция и принцип работы полупроводниковых оптических усилителей. Одной из особенностей этого класса приборов является наличие сильно выраженных нелинейных эффектов. В статье приведены результаты моделирования нелинейных эффектов четырехволнового смешения и взаимной модуляции в полупроводниковом усилителе, показано применение этих эффектов для выполнения конвертации длин волн. Моделирование выполнено в среде OptiSystem.

полупроводниковый оптический усилитель, компьютерное моделирование, нелинейные эффекты, четырехволновое смешение, взаимная модуляция.

В современных волоконно-оптических системах связи основными ограничивающими факторами являются затухание, дисперсия и нелинейные оптические эффекты. Для компенсации потерь оптической мощности в тракте используют такие устройства как оптические усилители. Оптический усилитель обеспечивает увеличение мощности оптического излучения без промежуточного преобразования оптического сигнала в электрический. Одним из таких устройств является полупроводниковый оптический усилитель.

В таких усилителях в качестве активной средой используются гетероэпитаксиальные структуры. Можно выделить три основных типа таких веществ, в зависимости от диапазона работы усилителя. При усилении света с диной волны 820–850 нм используются такие химические соединения, как GaAs или AlGaAs. При длине волны 1280–1330 нм используются InP и InGaAs. При 1530–1560 нм – GaSb и структуры на основе InGaAsP [1, 2].

Конструкция полупроводникового усилителя представляет собой две металлические подложки, между которыми располагаются слои вещества с *p*- и *n*-типом проводимости, через которые проходит электрический ток накачки, а также слой активного вещества. Торцы этой конструкции покрыты антиотражающим покрытием.

Усиливаемое излучение вводится в активный волновод при его прямом состыковании с подводимым оптическим волокном. Таким же образом усиленное излучение выводится из активного волновода. Инверсия населенности в полупроводнике создается за счет инжекции тока в полупроводник.

Фотоны входящего излучения, попадая на слой активного вещества, вызывают электронную эмиссию, результатом которой является переход электронов с верхнего энергетического уровня на нижний и излучение веществом вторичных фотонов. Один фотон входного сигнала вызывает появление N вторичных фотонов, возникает *N*-кратное оптическое усиление [1, 2, 3].

Полупроводниковые оптические усилители не получили столь широкого распространения, как усилители на примесном волокне. Дело в том, что они обладают рядом существенных недостатков.

Во-первых, поперечный разрез активного слоя имеет величину в единицы микрометров, в то время как диаметр сердцевины одномодового оптического волокна ~ 9 мкм. Вследствие этого часть светового потока не попадает в активную область, и не испытывает усиления. Это уменьшает КПД усилителя.

Во-вторых, коэффициент усиления полупроводникового усилителя зависит от направления поляризации и может отличаться на 4–8 дБ для двух ортогональных поляризаций [3].

Оба эти недостатка можно скомпенсировать, усложнив конструкцию усилителя, что приводит к увеличению его стоимости и может привести к ухудшению некоторых параметров усилителя. Среди прочих недостатков полупроводникового усилителя в сравнении с усилителем на примесном волокне, можно отметить то, что для них характерен более высокий уровень шумов усиления. Так же, усиление сигнала с помощью полупроводникового усилителя может достигать до 30 дБ, тогда как волоконный усилитель обеспечивает усиление до 50 дБ.

Среди прочего, полупроводниковые усилители сильнее подвержены нелинейным искажениям, таким как кроссмодуляция усиления, фазовая кроссмодуляция, фазовая самомодуляция и четырехволновое смешение (ЧВС). Эти нежелательные явления могут быть использованы для обработки оптических сигналов. Благодаря этим свойствам, на основе полупроводниковых усилителей создаются устройства, служащие для регенерации сигнала и преобразования длины волны. В данной работе рассматривается и моделируется работа оптического конвертера, в основе которого лежат эффекты кроссмодуляции усиления и ЧВС [4].

Основное преимущество преобразования частоты на основе ЧВС является независимость от формата модуляции и скорости передачи в битах. Дополнительным преимуществом этого метода является инверсия спектра сигнала и полученный в результате чирпинг. Это свойство может быть использовано для достижения компенсации дисперсии. Основным недостатком преобразователя ЧВС является его низкая эффективность преобразования [5].

На рис. 1 представлена схема модуляции, позволяющая наблюдать перестройку частоты сигнала с помощью ЧВС.

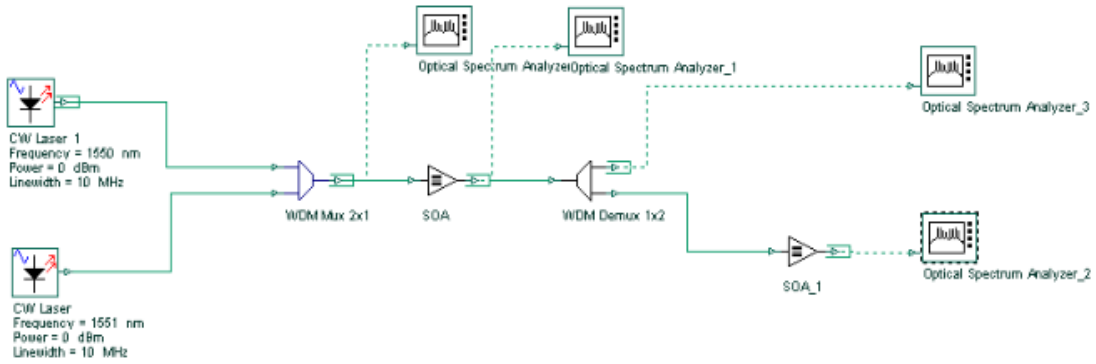


Рис. 1. Схема моделирования четырехволнового смешения

Схема включает в себя два источника излучения с длинами волн 1550 нм (сигнал накачки) и 1551 нм (основной сигнал), с уровнем мощности излучения 0 дБ. Сигналы этих источников мультиплексируются, и усиливаются с помощью полупроводникового усилителя. В процессе прохождения через усилитель, фотоны с длинами волн 1550 и 1551 нм взаимодействуют друг с другом, приводя к появлению фотонов с длинами волн 1549 и 1552 нм. После этого новый сигнал на частоте 1552 нм демультиплексируется, и вновь подвергается усилению. На рис. 2 представлен процесс изменения спектра сигнала (спектр мультиплексированного сигнала до прохождения усилителя, после прохождения усилителя и после демультиплексирования и последующего усиления). В результате мы видим, что сигнал с длиной волны 1551 нм был преобразован в сигнал с длиной волны 1552 нм. Однако данный способ позволяет лишь незначительно перестраивать частоты, так как с увеличением межканального интервала значительно уменьшается эффективность ЧВС.

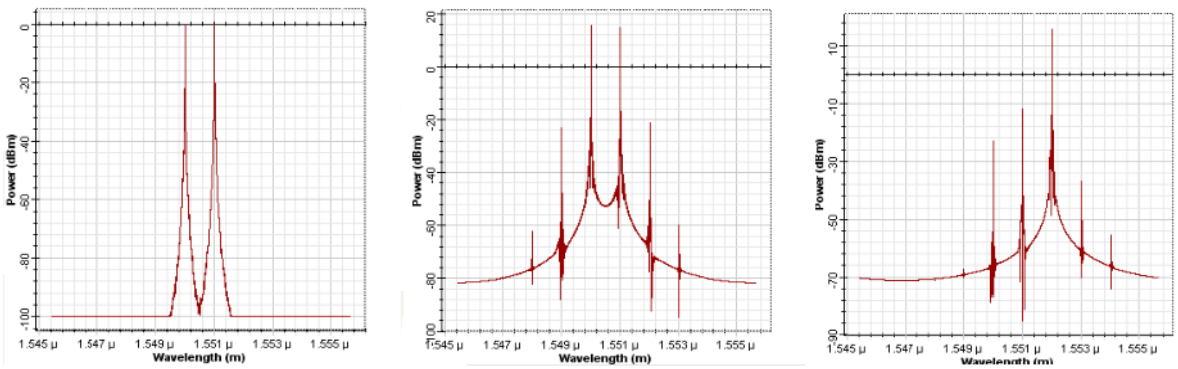


Рис. 2. Изменение спектра сигнала

В основе принципа использования кроссмодуляции усиления для перестройки частоты сигнала лежит уменьшение коэффициента усиления усилителя. Этот эффект наблюдается при прохождении через усилитель двух и более волн. Каждая из волн приводит к уменьшению инверсии населенности в активной среде там большей, чем выше их оптическая мощность [6]. Благодаря этому эффекту непрерывный сигнал на выбранной длине волны можно подвергнуть модуляции по интенсивности, в результате чего он будет нести в себе ту же информацию, что и модулирующий сигнал. Непрерывный сигнал может быть запущен в линию связи как сонаправлено с модулирующим сигналом, так и в противоположном направлении [6, 7].

Схема на рис. 3 рассматривает случай сонаправленного введения непрерывного сигнала.

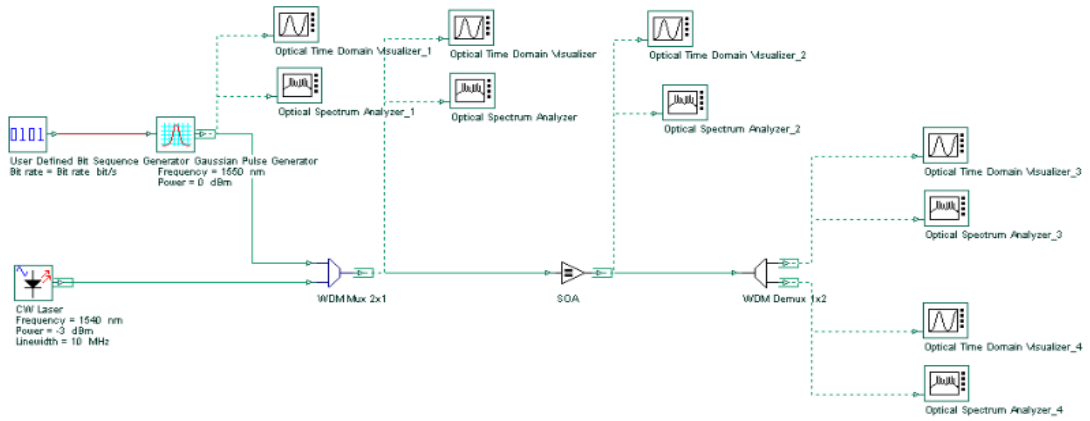


Рис. 3. Схема исследования конвертора на кроссмодуляции усиления

На вход мультиплексора, помимо непрерывного оптического сигнала с длиной волны 1540 нм, поступает последовательность гауссовских импульсов с длиной волны 1550 нм, рис. 4, Vizualizer 1.

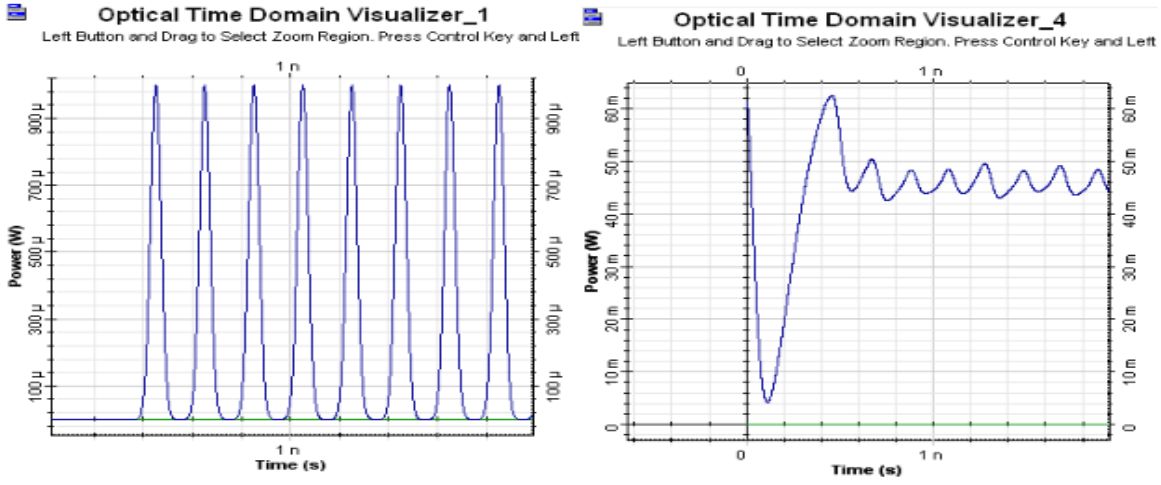


Рис. 4. Гауссовские импульсы и промодулированный ими сигнал

Его форма после демультиплексирования показана на рис. 4, Vizualizer 4. Превращение спектра в процессе преобразования сигнала продемонстрировано на рис. 5 (мультиплексированный сигнал до прохождения усилителя, после прохождения усилителя и после демультиплексирования).

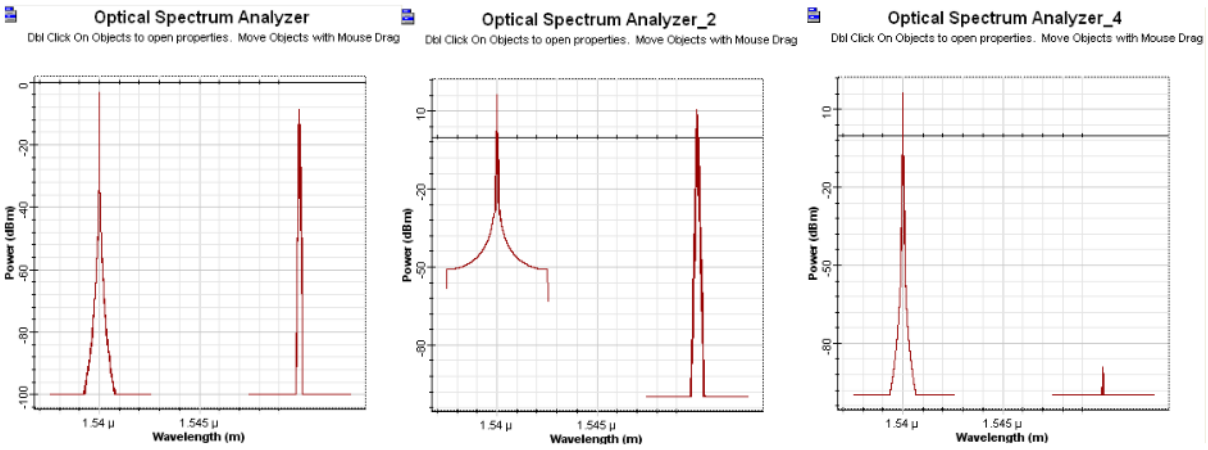


Рис. 5. Изменение спектра сигнала при прохождении тракта

Использование нелинейных явлений в полупроводниковых оптических усилителях позволяет реализовать полностью оптические конвертеры длин волн. Подобные устройства очень важны для увеличения пропускной способности и гибкости оптических сетей с временным и спектральным уплотнением каналов.

Список используемых источников

1. Michael J. Connelly Semiconductor Optical Amplifiers and their Applications, Kluwer Academic Publishers, 2004.

2. Дураев В., Казаков А., Медведев С. Полупроводниковый оптический усилитель // Фотоника, 2010. № 1. С. 16–18.

3. Дмитриев А. Л. Оптические системы передачи информации: учебное пособие. СПб. : СПбГУИТМО, 2007. 96 с.

4. Kevin Carney Investigation of In-Situ Parameter Control in Novel Semiconductor Optical Amplifiers // A thesis for the Degree of Doctor of Philosophy. School of Electronic Engineering Faculty of Engineering and Computing Dublin City University, 2012. PP. 212.

5. OptiSystem Optical Communication System Design Software, version 13 // Tutorial, Volume 2. 2014.

6. Vikas Thakur, Ms. Geetanjli Pandove, Tarun Gupta Optical wavelength converters based on cross gain modulation and cross phase modulation in SOA // International Journal of Electronics and Computer Science Engineering, Volume 1, Number 3.

7. Ng T. T., Pérez A., Sales S., Richardson D. J., Petropoulos P. Characterization of XGM and XPM in a SOA-MZI using a Linear Frequency Resolved Gating Technique // Lasers and Electro-Optics Society, 2007. LEOS 2007. The 20th Annual Meeting of the IEEE.

УДК 621.39

АНАЛИЗ ХАРАКТЕРИСТИК ОПТИЧЕСКИХ OFDM СИСТЕМ СВЯЗИ

А. С. Дюбов, А. В. Царегородцев

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

Технология ортогонального частотного мультиплексирования с прямым и когерентным способом приема в настоящее время рассматривается как наиболее перспективная для организации протяженных оптических каналов связи. В статье рассмотрено моделирование работы OFDM системы связи на основе схемы-проекта, входящего в состав программного обеспечения Optisystem. Приведены рассчитанные сигнальные созвездия электрических сигналов (до и после прохождения по каналу связи), характеризующие достоверность передачи информации.

технология ортогонального частотного мультиплексирования, оптическая система связи, оптическое волокно, сигнальное созвездие, OFDM.

Технология ортогонального частотного мультиплексирования OFDM (*Orthogonal frequency division multiplexing*) является частным случаем передачи данных, при котором информационный поток разделяется и передается множеством подканалов с более низкой скоростью. Сигнал OFDM может рассматриваться не как одиночный широкополосный сигнал, а как множество узкополосных сигналов, причем ортогональность поднесущих позволяет сигналам даже частично перекрывать друг друга в частотном спектре и при этом не оказывать негативного взаимного влияния. Технология OFDM обеспечивает значительное увеличение использования полосы пропускания за счет улучшения спектральной эффективности.

Данная технология получила широкое распространение в области радиочастотной связи. Начиная с конца 1990-х гг. принцип OFDM активно развивается в приложениях волоконно-оптической связи. Достоинством ортогонального частотного мультиплексирования является повышенная устойчивость к различным негативным факторам, присутствующим в оптическом канале: затуханию, дисперсии и шумам. Технологии OFDM в последнее время уделяется большое внимание, множество публикаций посвящены данной теме [1, 2, 3, 4].

Для изучения и демонстрации работы оптической OFDM системы связи используем программное обеспечение Optisystem и один из файлов-проектов, поставляемых разработчиком вместе с программой. В данном

случае рассматривается система с когерентным приемом Coherent Optical OFDM (CO-OFDM). Особенностью таких систем является наличие в приемнике источника опорного сигнала. Схема моделирования OFDM системы связи приведена на рис. 1.

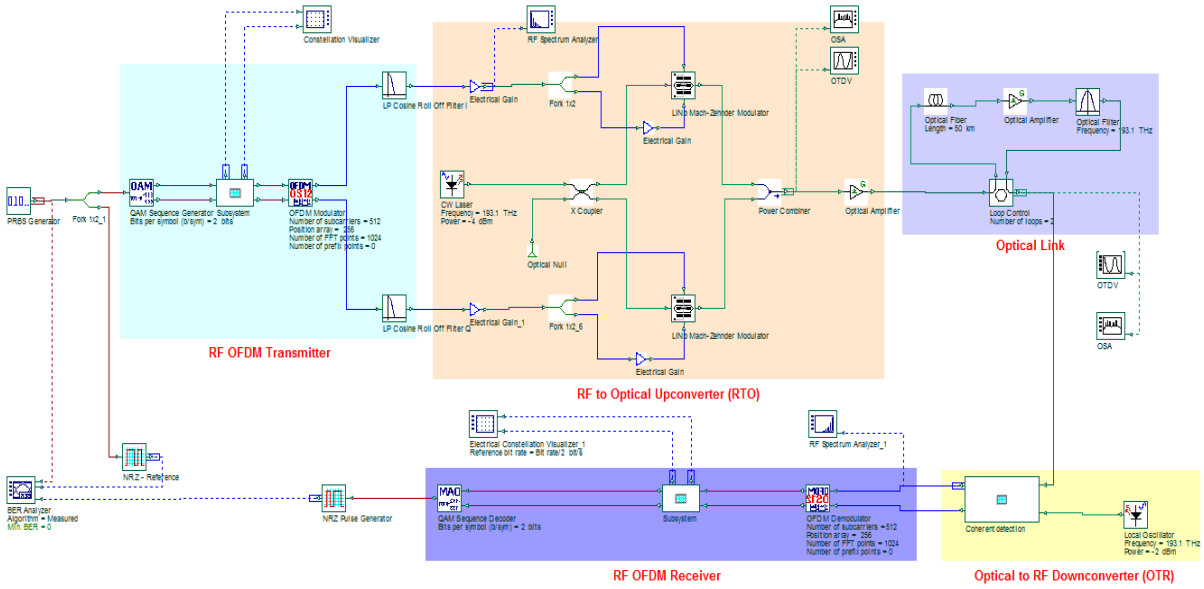


Рис. 1. Схема моделирования системы CO-OFDM

Приведенная схема CO-OFDM системы связи содержит радиочастотный передатчик OFDM сигнала (RF OFDM *Transmitter*), конвертер радиочастотного сигнала в оптический (*RF to Optical Upconverter*), модель оптической линии связи (*Optical Link*), конвертер оптического сигнала в радиочастотный (*Optical to RF Downconverter*), радиочастотный приемник OFDM сигнала (RF OFDM *Receiver*). Источником тестового сигнала служит генератор псевдослучайной битовой последовательности (PRBS *Generator*). Имеющийся в схеме измеритель коэффициента ошибок (BER *Analyzer*) служит для оценки качества связи. Помимо названных блоков схема дополнена виртуальными измерительными приборами (*Analyzer*): электрическими и оптическими анализаторами спектра (RF *Spectrum Analyzer*), (*Optical Spectrum Analyzer* – OSA), приборами для наблюдения формы сигналов (OTDV), измерителями созвездий электрического сигнала.

В данной схеме моделируется работа системы связи со скоростью 10 Гбит/с. Информационный поток разбивается на 512 подканалов, в каждом подканале применяется модуляция 4-QAM. Перенос сигнала радиочастотного спектра в оптический диапазон выполняется посредством двух модуляторов Маха-Цендера входящих в блок «RF to Optical Upconverter». На рис. 2 приведены спектры радиочастотного и оптического сигналов.

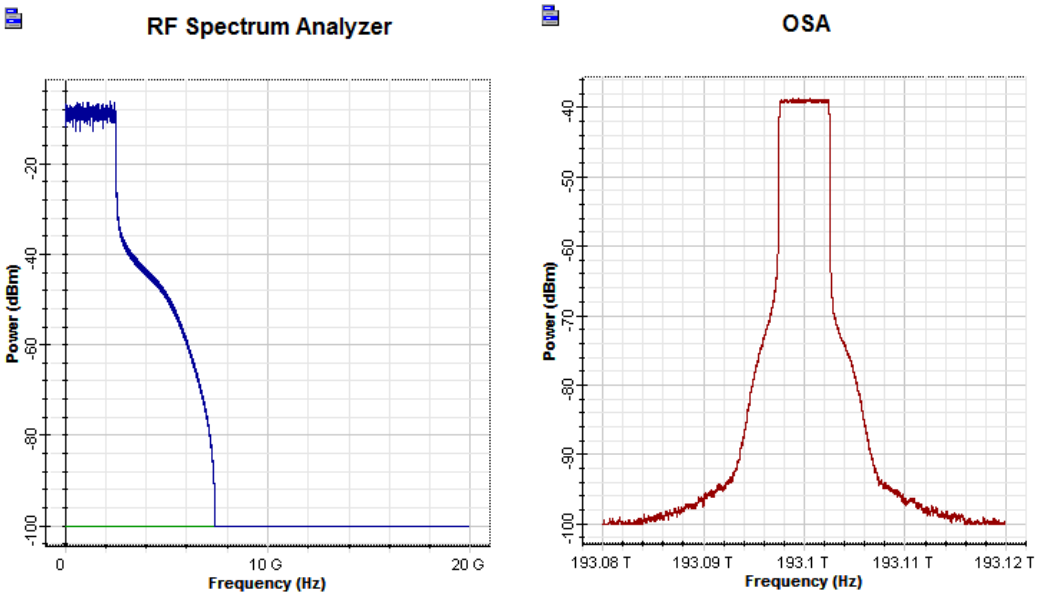


Рис. 2. Спектр радиочастотного (слева) и оптического сигналов (справа)

При прохождении по оптической линии связи сигнал искажается. На приемной стороне происходит обратное преобразование сигнала из оптического диапазона в радиочастотный. Для оценки качества принимаемого сигнала наблюдают сигнальные созвездия. По степени «размытости» сигнального созвездия можно судить о характере и величине искажений и помех, оценить достоверность приема цифрового сигнала. На рис. 3 представлены сигнальные созвездия на передаче и на приеме, при протяженности оптической линии 100 км.

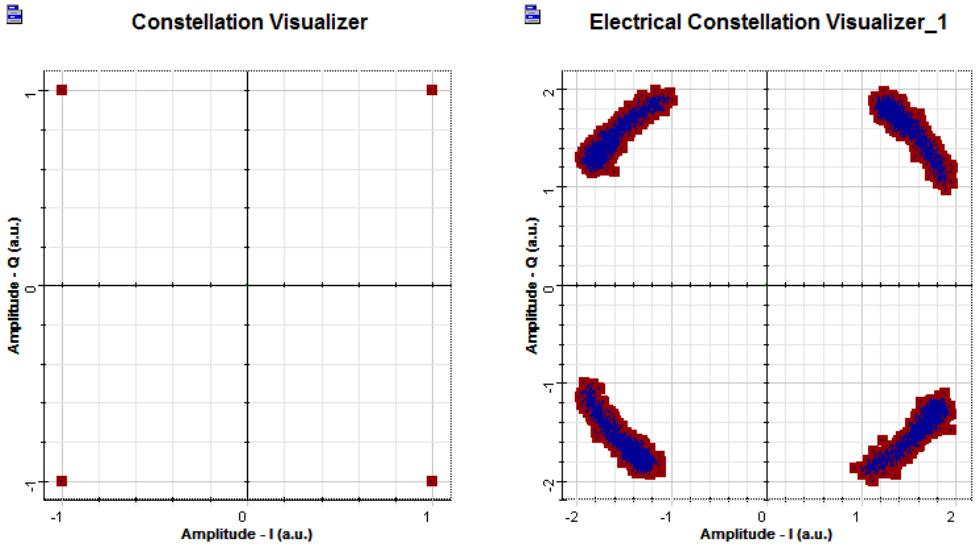


Рис. 3. Сигнальные созвездия: на передаче (слева) на приеме (справа)

На рис. 4 приведены сигнальные созвездия на приеме при увеличенной протяженности оптического тракта, составляющей 200 км и 300 км.

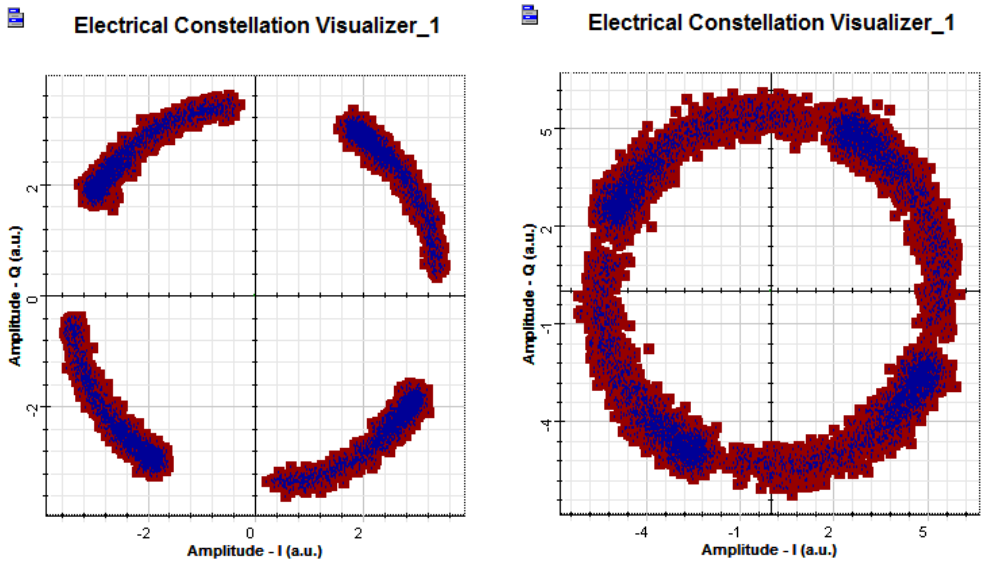


Рис. 4. Сигнальные созвездия, при участке 200 км (слева) и 300 км (справа)

Из рис. 3 и 4 очевидно, что увеличение протяженности участка ведет к увеличению искажений и снижению достоверности приема.

Список используемых источников

1. Ivan B. Djordjevic and Bane Vasic Orthogonal frequency division multiplexing for high-speed optical transmission // OPTICS EXPRESS Vol. 14, No. 9. May 2006.

2. OptiSystem Optical Communication System Design Software, version 13 // Tutorial, Volume 2. 2014.

3. Coherent Optical OFDM / Optiwave Design Software for photonics [Электронный ресурс:] URL: https://optiwave.com/applications/coherent-optical-ofdm-2/

4. Chao Li, Qi Yanga. Optical OFDM/OQAM for the Future Fiber-optics Communications // Procedia Engineering 140 (2016). PP. 99–106.

УДК 004.72 (004.77)

ЭФФЕКТИВНОСТЬ DPI-СИСТЕМЫ ДЛЯ ОБЕСПЕЧЕНИЯ ПОКАЗАТЕЛЕЙ КАЧЕСТВА OTT-УСЛУГ

В. С. Елагин, А. В. Онуфриенко

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

В настоящей статье авторы вводят определение термина OTT-сервисов, приводят описание услуг данных сервисов и краткое сравнение с услугами традиционных

управляемых услуг. Авторы приводят основные показатели сетевых характеристик, необходимых для обеспечения заданного качества обслуживания при предоставлении и передаче трафика разного вида. В докладе описываются проблемы, связанные с появлением OTT-сервисов на сети оператора. В связи с чем, в качестве перспективного варианта монетизации OTT-сервисов авторы приводят подходы и процедуры DPI-системы, обеспечивающие необходимые требования для QoS при предоставлении ресурсов своей сети для OTT-сервисов. В заключении приводятся основные преимущества от внедрения технологии DPI в сеть оператора связи для передачи определенного пользовательского контента.

OTT, OTT-сервис, OTT-услуга, DPI, Deep Packet Inspection, QoS, качество обслуживания.

Широкое распространение высокоскоростного доступа с одновременным снижением стоимости трафика и распространения сетевых технологий все больше приводит к появлению таких сервисов, как OTT.

Классификация OTT сервисов

OTT (англ. OVER THE TOP) – метод предоставления услуг (информации) через интернет и предоставления контента на широкий спектр пользовательских устройств (приставку, компьютер, мобильный телефон) по сетям передачи данных без участия оператора в управлении и распределении контента. Такие услуги и приложения потенциально конкурируют с традиционными услугами электросвязи и вещания, такими как голосовая телефонная связь, СМС и видео-вызовы, а также загрузка видео/аудио контента или вовсе заменяют их.

OTT-сервис – сервис, оказывающий услуги по предоставлению пользователям доступа к контенту на платной и/или бесплатной основе методом OTT. Пользователю достаточно иметь доступ в Интернет, и он сможет подключиться к OTT-сервису. Данная технология, обеспечивает доступ к услугам где угодно, и когда угодно.

Услуги, предоставляемые OTT-сервисами, подразделяются на:

1) Потоковое вещание – непрерывная трансляция аудиовизуальных материалов в потоковом режиме.
2) Видео по запросу – система индивидуальной доставки контента по запросу пользователя.
3) Текстовые мессенджеры – службы мгновенных сообщений, программы онлайн для обмена сообщениями в реальном времени.
4) Голосовые мессенджеры – службы, программы для передачи и приема голосовых сообщений в реальном времени через Интернет.
5) Социальные сети – платформа, сервис предназначенные для построения, отражения и организации социальных взаимоотношений в Интернете.

6) Облачные сервисы – это модель предоставления сетевого доступа в режиме «по требованию» к набору настраиваемых вычислительных ресурсов, которые пользователь может оперативно задействовать под свои задачи.

7) Другие.

Ситуация на российском рынке

OTT-контент быстро проникает во все сегменты IT-рынка. Потребители могут просматривать онлайн-видео, вместо традиционного телевидения, онлайн платформы, посредством которых может обмениваться мгновенными сообщениями, выполнять голосовые звонки, а также пользоваться видеосвязью.

На рис. 1 показано, как рост интернет-приложений для обмена сообщениями повлиял на объем передачи SMS.

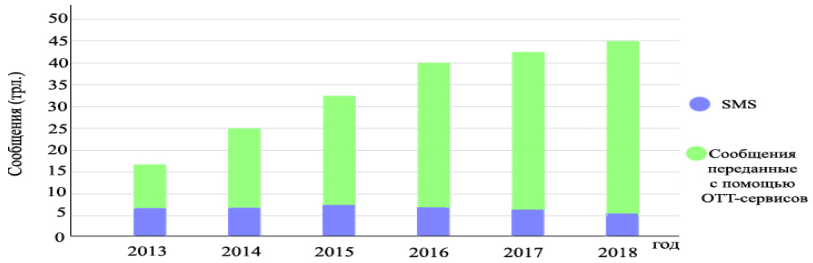


Рис. 1. Объем сообщений с мобильных телефонов (источник: *Analysys Mason*)

Как показано на рис. 2, мировой объем сообщений, отправленных с использованием услуг OTT, таких как Whatsapp, уже в 2013 г. превысил объем сообщений использованием традиционного оператора.

Российский рынок OTT-сервисов к 2017 г. увеличится в 4,8 раза по сравнению с данными с 2013 г., при этом среднегодовые темпы роста составят 48 %.

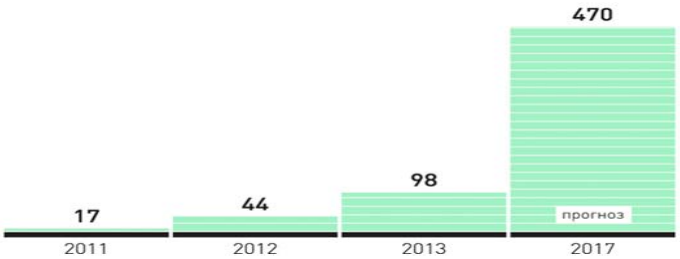


Рис. 2. Российский рынок OTT, млн долларов (источник: *j'son&partners consulting*)

OTT-сервисы в свою очередь, предоставляет зрителю существенную свободу выбора сервисов, персональный подбор услуг, так же технология не привязана к определенному провайдеру, что позволяет получить к ней доступ в любой точке мира при наличии подключения к интернету [1].

Однако Интернет является «неуправляемой» сетью, где ширина полосы не может контролироваться на всем маршруте передачи видео и звука от серверов до конечного пользователя.

Предполагается, что пользователи справедливо разделяют доступные сетевые ресурсы, но при этом не гарантируется обеспечение предварительно заданного качества обслуживания, что означает, что нет гарантии в том, что пакет будет доставлен в заданное время или, что он будет доставлен вообще, причем вне зависимости от типа трафика. Как только появляется недостаток ресурсов, ведущий к увеличению вероятности потерь пакетов и росту их задержек, для приложений реального времени необходимые показатели качества не могут быть обеспечены. В результате ухудшения скорости потока приложение периодически останавливает воспроизведение или происходит отказ в выполнении той или иной операции, что отрицательно сказывается на впечатлении пользователей о качестве услуг [2].

Желаемые сетевые характеристики

Нормы на параметры доставки пакетов IP с разделением по классам обслуживания указаны в таблице 1 (модель ITU-T Y.1541[3]).

Таблица 1. Нормы на параметры доставки пакетов IP

Сетевые характеристики	Классы QoS					
	0	1	2	3	4	5
Задержка доставки пакета	100 мс	400 мс	100 мс	400 мс	1 с	Н
Вариация задержки пакета	50 мс	50 мс	Н	Н	Н	Н
Коэффициент потери пакетов	1×10^{-3}	1×10^{-3}	1×10^{-3}	1×10^{-3}	1×10^{-3}	Н
Коэффициент ошибок пакетов	1×10^{-4}	1×10^{-4}	1×10^{-4}	1×10^{-4}	1×10^{-4}	Н

Качество обслуживания (англ. *QoS Quality of Service*) – совокупность характеристик услуги электросвязи, которые имеют отношение к ее возможности удовлетворять установленные и предполагаемые потребности пользователя услуги.

Проблема: обеспечить оператору связи гарантированной QoS для отдельных сервисов на своей сети для получения дополнительной прибыли от OTT-провайдеров.

DPI в OTT-сервисах

Ввиду развития технологии DPI перспективно рассмотреть технологические решения, по обеспечению QoS на сети провайдера для выделения OTT-сервисов.

Deep Packet Inspection – совокупное название технологий, при которых оборудование реагирует не только на заголовки пакетов разного уровня, но и на содержимое. Интернет-провайдеры получили возможность контролировать проходящий трафик своих клиентов, и соответственно заниматься приоритизацией трафика.

В сочетании с возможностью удаленного управления и анализом данных система дает возможность гибкого управления услугами и обеспечения QoS для поставщика заданных услуг. Система DPI позволяет изменять поле приоритета в проходящих через него пакетах в зависимости от детектированного протокола, что позволяет маршрутизаторам использовать эту разметку для обеспечения нужного уровня QoS.

Результат такого подхода, с точки зрения пользователя, является то, что некоторые приложения будут работать лучше, чем другие.

Возможности применения DPI в OTT

Существует несколько методов идентификации трафика. Совместное их использование позволяет наиболее точно определить трафик и затем применить к нему соответствующие правила и политики.

DPI анализ основывается на следующих механизмах:

1) Явно заданные правила.

2) Сигнатурный анализ.

3) Эвристический анализ.

4) Анализ поведения трафика.

Для корректной работы системы необходимо контролировать правильность и полноту сигнатурной базы. А также иметь ввиду, что может существовать некая погрешность выделения нужного трафика (погрешность на неопределение и погрешность неверно воспринятого пакета).

Для рассмотрения данных погрешностей были рассмотрены частные случаи определения трафика OTT-сервисов. SopCast – это программа для просмотра потокового видео по технологии peer to peer. Для проведения эксперимента была использована система nDPI для анализа трафика, и для проверки правильности и целостности написанной сигнатуры был использован сниффер «Wireshark» (табл. 2).

Для оценки погрешности неопределения интересующего нас трафика воспользуемся расчетами погрешностей одиночных измерений.

Абсолютная погрешность каждого однократного измерения:

$$\Delta i = U - U \times i,\ i = 1, \ldots,\ n.$$

Оценку систематической составляющей: Δсист. $= \frac{1}{n}\sum_{i=1}^{n} \Delta i$

Случайные составляющие погрешности каждого измерения:

$$\Delta\text{случ.} = \Delta i - \Delta\text{сист.}$$

Оценки среднего квадратического отклонения случайной составляющей погрешности однократного измерения:

$$\sigma = \left[\frac{1}{n-1}\sum_{i=1}^{n} \Delta\text{случ.}^2\right]^{1/2}.$$

Доверительные интервалы случайной погрешности однократного измерения: $\Delta\text{дов.}\, i = t * \sigma$, где $t = 1{,}83$ – коэффициент Стьюдента.

Оценка суммарной абсолютной погрешности:

$$\Delta\text{сум.}\, i = \Delta\text{сист.} \pm \Delta\text{дов.}\, i.$$

ТАБЛИЦА 2. Оценка погрешности исследуемого трафика (представлены 3 эксперимента)

№	Канал	Wireshark	Ntopng	Δ*i*	Δ сист.	Δслуч.	σ	Δсум. *i*
1	25788	12,07	12,06	0,01	0,0533	0,0433	0,0115	0,0533±0,0212
2	25771	18,55	18,54	0,01	0,0533	0,0433	0,0115	0,0533±0,0212
3	8893	23,95	23,89	0,06	0,0533	0,0067	0,0018	0,0533±0,0037

График сравнения.

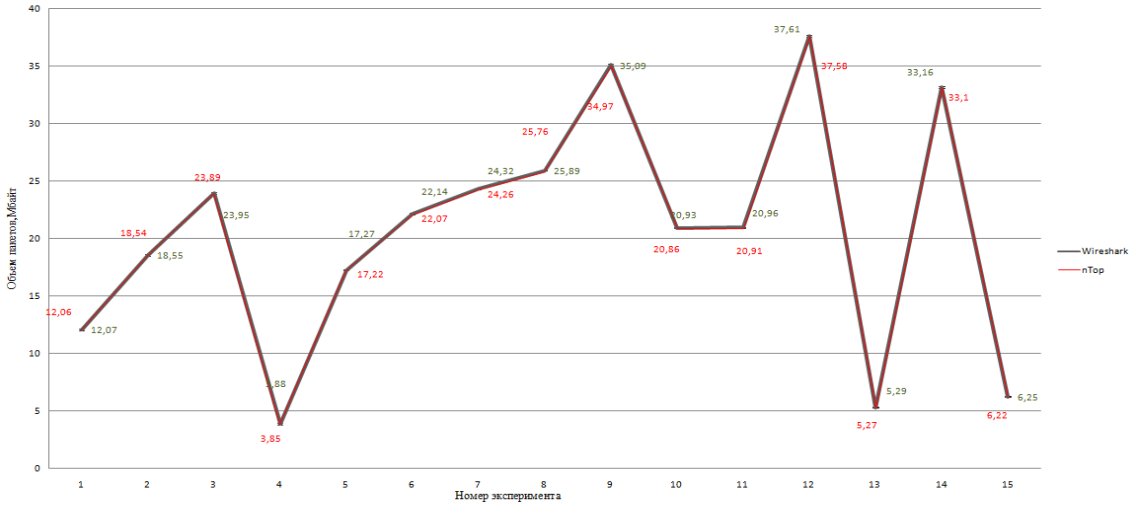


Рис.3. Значения экспериментов и погрешностей измерений

Выводы

Таким образом система DPI является одним из актуальнейших решений для выделения нужного трафика, назначения ему определенного уровня приоритета, и предоставления качественной и своевременной доставки пакетов. Что позволяет оператору стать не только средством для передачи трафика через свою сеть, но и извлечь практическую выгоду за счет предо-

ставления дополнительной услуги. Однако существует необходимость рассмотрения технических особенностей внедрения данных услуг, и влияние данного новшества на характеристики всей сети.

Список используемых источников

1. Елагин В. С., Онуфриенко А. В. Как оператору заработать на OTT-сервисах и при чем тут SDN? // T-COMM. 2017. N 1. С. 17–21.

2. Гольдштейн Б. С., Соколов Н. А., Яновский Г. Г. Сети связи. СПб.: БХВ-Петербург, 2010. 400 с.

3. Рекомендация ITU-T Y.1541 (12/2011). Аспекты межсетевого протокола – Качество обслуживания сервисов и сети: производительность сети для услуг IP сети. 2011. 66 с.

УДК 004.7 (004.942)

ТЕХНОЛОГИЧЕСКИЕ АСПЕКТЫ ЗАКОННОГО ПЕРЕХВАТА ТРАФИКА В SDN

В. С. Елагин, В. А. Сорокин

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

Современное бурное развитие информационных технологий требует гибкости и масштабируемости от сети. Традиционные сети не всегда способны эффективно реагировать на новые потребности пользователя. Одним из перспективных направлений модернизации существующей архитектуры сети является концепция SDN. В статье рассмотрена концепция построения SDN, нормативно-правовые требования к сетям общего пользования и текущие сложности, возникающие при реализации законного перехвата трафика в сетях SDN.

законный перехват программно-конфигурируемые сети, SDN, COPM. DPI.

Современное бурное развитие информационных технологий требует гибкости и масштабируемости от сети. Количество подключённых устройств каждый год растёт в геометрической прогрессии, лишь устройств Интернета вещей к 2021 г. ожидается до 46 млрд штук [1]. Увеличивается и объём генерируемого трафика. Традиционные сети не всегда способны эффективно реагировать на новые потребности пользователя. Требуется модернизация существующей архитектуры сети. Одним из перспективных направлений развития информационных сетей является SDN.

SDN (*Software Defined Network*) – программно-конфигурируемая сеть, технология построения архитектуры сетей связи, основанная на принципе

разделения функций управления и функций передачи. В традиционных маршрутизаторах и коммутаторах данные функции неотделимы друг от друга, и каждый элемент принимает решения самостоятельно и относительно независимо.

Концепция SDN предполагает вынести функции управления в отдельное устройство – контроллер, а коммутаторам оставить только функцию передачи трафика. Взаимодействие между контролером и коммутаторами осуществляется по средством протокола управления. Первым открытым стандартизированным протоколом является OpenFlow. Управление данными в OpenFlow осуществляется на уровне потоков, а не отдельных пакетов. Правила в коммутаторе устанавливаются с участием контроллера только для первого пакета, потом все последующие пакеты потока его используют. Стандарт принят большинством производителей сетевого оборудования, и уже доступны OpenFlow-решения на рынке сетевого оборудования. Существуют и проприетарные решения протоколов управления, но в связи с их закрытой документацией нет возможности изучить их.

Преимуществом перехода к концепции SDN является:

– Снижение капитальных затрат. Уменьшение выполняемых задач коммутаторами позволят существенно снизить их стоимость.

– Централизованное управление. К контроллеру подключены все коммутаторы в сети, соответственно он будет иметь представление о состоянии сети, что позволит производить балансировку нагрузки.

– Гибкость. Вся логика управления сетевыми устройствами в SDN реализуется программным способом, что позволяют разработчикам создавать собственные приложения для управления сетью через программные интерфейсы(API) контроллера. Тем самым SDN позволяет создавать новые источники дохода от сети.

– Автоматизация. Возможность производить конфигурацию, предоставление новых услуг используя готовые алгоритмы.

Одним из нерешенных вопросов на сети SDN является реализация функций законного перехвата [2]. Согласно приказу № 83 Министерства связи и массовых коммуникаций РФ от 16 апреля 2014 года, все операторы сетей передачи данных до 31 марта 2015 года должны привести используемое, а также вводимое в эксплуатацию оборудование коммутации и маршрутизации пакетов информации в соответствие с требованиями, указанными в приказе.

Как говорилось ранее, концепция SDN предполагает реализацию функции управления сетью и сложных сетевых функций на контроллере, поэтому удобно было бы реализовать СОРМ на контроллере в виде сетевого приложения и получать требуемые приказом идентификаторы через API. Реализация системы законного перехвата трафика на контроллере позволит

централизованно следить и собирать необходимую информацию в одном узле сети.

Для рассмотрения возможности данной реализации, требуется провести сравнительный анализ параметров, установленных приказом № 83 Министерства связи и массовых коммуникаций, с классификаторами, определенными в потоковых таблицах OpenFlow-коммутаторов. Для проведения анализа информации, передаваемой по протоколу OpenFlow был произведён эксперимент с установлением сессий протоколами разных уровней модели OSI: ICMP, ARP, HTTP.

Введем некоторые условные обозначения:

– h1..h9 – хосты подключенные к OpenFlow-коммутаторам;
– eth0..eth4 – интерфейсы подключения (Ethernet);
– s1..s4 – OpenFlow-коммутаторы;
– c0 – контроллер с сетевой операционной системой Floodlight;
– выноски обозначают DPID каждого OpenFlow-комутатора.

Схема эксперимента представлена на рис. 1.

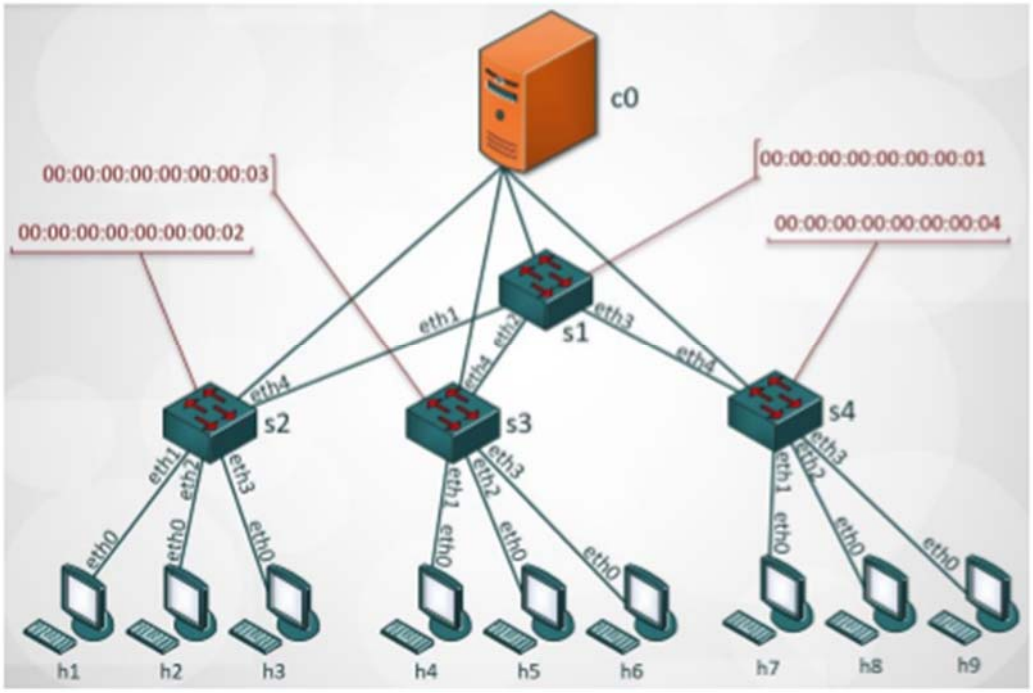


Рис. 1. Архитектура сети эксперимента

По результатам эксперимента было установлено, что контроллер, благодаря полям соответствия классификаторов протокола OpenFlow, имеет возможность получать информацию о потоках(пакетах) включительно до транспортного уровня, чего недостаточно для интеграции СОРМ в контроллер SDN сети, так как некоторые параметры контроля передаются с по-

мощью высокоуровневых протоколов. Таким образом, если реализовать систему законного перехвата трафика в контроллере без внесения изменений в имеющиеся классификаторы OpenFlow протокола, то СОРМ будет реализован неполноценно и трафик с параметрами передаваемые в высокоуровневых протоколах, не будут обнаруживаться.

В качестве второго варианта, рассмотрим модель реализации СОРМ на уровне коммутаторов SDN (рис. 2). Идеей данной модели будет заключатся в пассивном режиме съёма трафика, путём настройки «зеркалирования» трафика коммутаторов на специальный узел связи, где будет происходить дальнейший его анализ. Для получения идентификаторов высокоуровневых протоколов потребуется реализовывать технологию DPI.

Суть технологии DPI (*Deep Packet Inspection*) заключается в глубоком анализе пакета на верхних уровнях модели OSI. Анализ и идентификация протокола/приложения может осуществляется не только по формату заголовков, номерам портов и т. п., но и на базе поведенческого анализа трафика.

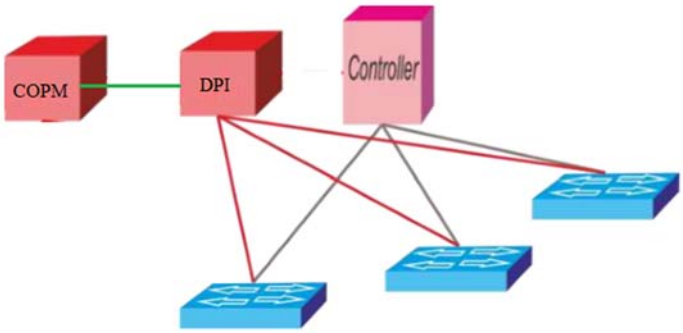


Рис. 2. Схема подключения при реализации модели СОРМ на уровне коммутаторов

Реализация DPI в SDN позволит на основе анализа пакетов получать и своевременно обнаруживать параметры контроля, передаваемые с помощью высокоуровневых протоколов (не использующие алгоритмы шифрования). Внедрение технологии DPI непосредственно на коммутаторы будет требовать больших мощностей и производительности от коммутаторов, приводя тем самым к увеличению стоимости коммутаторов, лишая концепцию SDN одного из свойств-преимуществ. Поэтому было решено вынести функционал DPI в отдельный узел. Для осуществления запросов на основе параметров контроля СОРМ будет подключён к узлу с DPI напрямую.

У каждой из рассмотренных моделей реализаций имеются свои преимущества и недостатки. Внедрение функции СОРМ на контроллере в виде сетевого приложения требует добавление и отслеживание классификаторов высокоуровневых протоколов на коммутаторах, что приведёт к их усложнению, либо производить на коммутаторах полную инкапсуляцию приходящего на пакет и отправлять его на контроллер, этот вариант приведёт к увеличению нагрузки на служебный канал. Модель реализации СОРМ

на уровне коммутаторов имеет шанс на существование, но требует большого капиталовложения в оборудование, усложнения схемы и дальнейшего исследования данной реализации. Об окончательной модели реализации СОРМ говорить пока рано, ввиду продолжающегося становления и развития самой концепции SDN. Однако уже существуют готовые решения для организации сети на базе данной концепции, и можно предположить их практическое внедрение в ближайшее время поэтому вопрос организации СОРМ на программно-конфигурируемых сетях является своевременным и важным.

Список используемых источников

1. Приказ Минкомсвязи РФ от 16 апреля 2014 года №83 «Об утверждении Правил применения оборудования систем коммутации, включая программное обеспечение, обеспечивающего выполнение установленных действий при проведении оперативно-розыскных мероприятий. Часть III. Правила применения оборудования коммутации и маршрутизации пакетов информации сетей передачи данных, включая программное обеспечение, обеспечивающего выполнение установленных действий при проведении оперативно-розыскных мероприятий» // Рос. Газ. 2014 – 18 июля.

2. Елагин В. С. Подходы к моделированию систем законного перехвата трафика в SDN // Актуальные проблемы инфотелекоммуникаций в науке и образовании. V международная научно-техническая и научно-методическая конференция: сб. науч. ст. / под. ред. С. В. Бачевского. СПб. : СПБГУТ, 2016. С. 353–358.

УДК.621.391

АРХИТЕКТУРА ПРОГАММНО-КОНФИГУРИРУЕМЫХ СЕТЕЙ SDN ДЛЯ МОБИЛЬНЫХ СЕТЕЙ ПЯТОГО ПОКОЛЕНИЯ 5G

В. Б. Жуланов, А. С. Мутханна

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

Большинство исследователей в этой области предлагают, что будущие системы 5G станут инфраструктурой для развертывания Интернета вещей IoT. Взаимодействие устройство-устройство D2D является ключевой коммуникационной парадигмой, которая поддерживает соединение неоднородных объектов между собой и обеспечивает ряд важных преимуществ. Одной из основных задач и проблем для сотовых систем 5G является проектирование гибких сетевых архитектур, которые могут быть реализованы на принципах программно-конфигурируемых сетей SDN. Существующие коммерческие сотовые системы основываются на закрытых и сложноуправляемых архитектурах, базирующихся на аппаратных средствах как в интерфейсе радиодоступа,

так и в базовой сети. Эти проблемы существенно задерживают принятие и внедрение новых стандартов, налагают значительные трудности в части реализации новых методов для увеличения пропускной способности сети. В работе рассматриваются преимущества архитектуры SDN для сетей пятого поколения.

контроллер SDN, архитектура, радиодоступ, интерфейс, программно-конфигурируемая сеть, беспроводной.

Введение

Согласно требованиям к системам сотовой связи 5G ультравысокой ёмкости, они должны иметь в 1000 раз большую емкость на квадратный километр по сравнению с LTE, задержка на пользовательском радио интерфейсе доступа должна быть менее 1 миллисекунды, а также скорость передачи должна быть в 100 раз больше, чем на существующих сотовых сетях (пропускная способность 1 Гбит/с повсеместно) [1]. Некоторые технологии должны использоваться в сетях 5G, такие, как программно-конфигурируемые сети (SDN – *software defined networking*) и виртуализация сетевых функций (NFV). Другие технологии используются на краю сети, чтобы разгрузить базовую сеть, а также гарантировать низкую задержку. Эти технологии подобны коммуникации устройства-устройства (D2D – *device to device*) [1, 2]. Вызовы, с которыми сталкиваются в настоящее время сетевые архитектуры, не могут быть решены без радикального сдвига парадигмы в области разработки беспроводных сетей нового поколения. Поэтому предлагается использование концепции программно-конфигурируемых сетей в сетях нового поколения 5G, введение новой архитектуры для беспроводных SDN [3, 4]. SDN облегчает внедрение и развёртывание новых приложений и услуг по сравнению с классическими аппаратно-зависимыми стандартами [5].

В этой статье основное внимание акцентируется на новой архитектуре беспроводных SDN, называемой SoftAir. В предлагаемой архитектуре плоскость управления состоит из управления сетью и инструментов оптимизации и осуществляется на серверах. Плоскость данных состоит из программно-конфигурируемых базовых станций (SD-BS) в сети радиодоступа и SDN коммутаторов в базовой сети сотовой связи.

Архитектура Softair предлагает пять основных свойств.

1) Программируемость – SDN узлы (базовые станции SDN и SDN коммутаторы) могут быть перепрограммированы в режиме реального времени путем динамического определения и создания сетевых алгоритмов.

2) Кооперативность – SDN узлы могут быть объединены в кластеры для совместного управления и оптимизации, для повышения общей производительности сети.

3) Виртуализация – на одной SoftAir могут быть созданы несколько виртуальных беспроводных сетей, каждая из которых работает независимо

в соответствии с ее собственными сетевыми протоколами и ресурсами, выделяемыми по запросу.

4) Открытость – элементы плоскости данных независимы от базовых технологий и поставщиков и имеют единые интерфейсы управления (например, CPRI и OpenFlow), что существенно упрощает мониторинг и менеджмент плоскости данных.

5) Обзор (мониторинг) – централизованные контроллеры имеют общее представление о состоянии сети, состоящей из базовых станций и коммутаторов.

Как показано на рисунке, архитектура SoftAir состоит из плоскости данных и плоскости управления. Плоскость данных является открытой, программируемой и виртуализированной сетевой инфраструктурой, которая состоит из программно-конфигурируемой сети радиодоступа SD-RAN и программно-конфигурируемой базовой сети SD-CN. SD-RAN состоит из базовых станций SDN, в то время как SD-CN из SDN коммутаторов.

Рисунок. Общая архитектура SoftAir

Виртуализация сетевых функций отделяет сетевые функции от аппаратного обеспечения и объединяет их на сетевых серверах. Это обеспечивает высокую гибкость в сетевой инфраструктуре, так как сеть может быстро адаптироваться к меняющимся условиям. Но возникает проблема с масштабируемостью сети.

Архитектура программно-конфигурируемой базовой сети

Специализированные приложения SDN, например, управление мобильностью, QoS, политики биллинга, классификация трафика, могут быть развернуты на сетевом контроллере.

Масштабируемость базовой SDN сети может значительно улучшиться за счет использования высокопроизводительных контроллеров и оптимизированных схем управления сетью [6, 7]. Например, для существующих SDN, один контроллер может обработать до 12 миллионов запросов в секунду для управляющих сообщений между контроллером и коммутаторами. Такая высокая производительность была достигнута за счет разделения сети на кластеры и использования многопоточной технологии. С помощью метода Альтернативного направления коэффициентов Alternating Direction Method of Multipliers ADMM, задержки между контроллером и коммутаторами могут быть сведены к минимуму.

Стандартный интерфейс CPRI (*Common Public Radio Interface*), совместно разработанный такими компаниями, как Ericsson, Huawei, NEC, Alcatel Lucent и Nokia Siemens, может предоставлять высокую скорость (до 10 Гбит/с с низкой частотой битовых ошибок до 10^{-12}) и обмен данными между удаленными радио серверами RRH и серверами модуляции BBS на дальние расстояния (до 40 миль), обеспечивая при этом высокую степень синхронизации.

Существующая распределенная RAN обладает неравномерным распределением функций между RRH и серверами модуляции. На сервера модуляции BBS возложены функции как всей обработки основной полосы частот, так и операции с MAC-уровнем, в то время, как RRH реализует только внешний радио интерфейс. Из-за такого подхода, требуется чрезвычайно высокие скорости передачи данных на транспортной сети. Например, согласно расчетам, для транспортировки 20 МГц LTE сигнала по интерфейсу CPRI между BBS и полудуплексным RRH с восемью антеннами для передачи требуется скорость 7, 46 Гбит/с. Это противоречит текущим тенденциям в беспроводных технологиях, развивающимся в сторону массивной MIMO, полнодуплексных приемопередатчиков, миллиметровых волн и терагерцовой полосы частот.

Для решения этих проблем, SoftAir принял новую концепцию высокой степени декомпозиции базовой станции, где обработка основной полосы частот возлагается на RRH, при этом остальные функции, например, MIMO кодирование, кодирование на источнике и MAC уровень возлагается на BBS.

В предлагаемой архитектуре программно-конфигурируемой RAN, реализуется интерфейс OpenFlow для каждой программно- конфигурируемой базовой станции с помощью использования программных коммутаторов

Open vSwitch (OVS). Такая архитектура позволяет мобильным пользователям перемещаться между базовыми станциями, используя различные беспроводные стандарты, исключая сбои в сети предоставления услуг. Также, применяя интерфейс OpenFlow как на SDN коммутаторах, так и на базовых станциях SDN, обеспечиваются прозрачные взаимосвязи между базовой сетью и интерфейсом радиодоступа и появляется универсальный интерфейс управления всех SoftAir.

Новые возможности при виртуализации сети

Виртуализация сети позволяет использовать несколько изолированных виртуальных сетей, например, M2M, самые популярные операторские сервисы, сотовые сети оператора связи, разделяя при этом физическую инфраструктуру сети. Это означает разделение сетевых ресурсов для нескольких виртуальных сетей. Например, каждая виртуальная сеть адаптирует протоколы физического, канального и сетевого уровня под себя, не прерывая при этом операции и не снижая производительность других виртуальных сетей. SoftAir с виртуализацией сети предлагает широкий спектр новых приложений, например, предлагая MVNO адаптировать и принимать различные беспроводные стандарты (HetNets, LTE, WiMAX, WiFi), что позволяет более эффективно использовать ресурс RAN и сэкономить операторам до 60 миллиардов долларов в течение 5 лет за счет сокращения расходов на оборудование в районах с низким уровнем трафика.

Заключение

Архитектура SoftAir – это новая парадигма в сфере беспроводных сетей нового поколения. SoftAir обеспечивает высокую степень гибкости сетевой архитектуры, что ускорит развитие как аппаратной инфраструктуры, так и сетевых программных алгоритмов. Также SoftAir предлагает эффективное и адаптивное использование сетевых ресурсов за счет виртуализации сети, динамического распределения вычислительных мощностей и повышения энергоэффективности. Но необходимо отметить, что существует ряд преград на пути к созданию полноценной беспроводной инфраструктуры 5G на базе SDN/NFV, в частности проблема масштабируемости сети, проблема реализации открытых стандартизированных интерфейсов. Только в ближайшем будущем мы сможем увидеть полный пакет решений.

Список используемых источников

1. 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. PP. 395–403.

2. Мутханна А. С., Кучерявый А. Е. D2D-коммуникации в сетях мобильной связи пятого поколения 5g // Информационные технологии и телекоммуникации. 2014. № 4 (8). С. 51–63.

3. Ateya A., Muthanna A., Gudkova I., Vybornova A. and Koucheryavy A. Intelligent core network for Tactile Internet system // International Conference on Future Networks and Distributed Systems, ACM, P.15, Cambridge, Jul. 2017.

4. Akyildiz, Ian F.; Wang, Pu; Lin, Shih-Chun. 2015. SoftAir: a software defined networking architecture for 5G wireless systems // Computer Networks, vol. 85, 5 July 2015: pp 1–18.

5. Vladyko A., Muthanna A., Kirichek R. Comprehensive sdn testing based on model network // Lecture notes in computer science. 2016. PP. 539–549.

6. Kirichek, R., Vladyko, A. Zakharov, M., Koucheryavy, A.: Model Networks for Internet of Things and SDN // In: 18th International Conference on Advanced Communication Technology (ICACT), pp. 76–79. IEEE (2016).

7. Xia, W., Wen, Y., Foh, C., Niyato, D., Xie, H.: A Survey on Software-Defined Networking // IEEE Communications Surveys & Tutorials, 17 (1), 27–51 (2015).

УДК 004.7

СТРУКТУРНАЯ МОДЕЛЬ РЕСУРСОВ МУЛЬТИСЕРВИСНОЙ СЕТИ СВЯЗИ ОГРАНИЧЕННОГО ПОЛЬЗОВАНИЯ

Е. П. Журавель[1], Е. А. Исупова[2]

[1]Акционерное общество «Научно-исследовательский институт «Рубин»
[2]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Рассмотрена структурная модель ресурсов мультисервисной сети связи ограниченного пользования, приведены технологии построения составляющих её ресурсов, предложен подход к их формализации, обоснована необходимость уточнения моделей источников угроз, угроз и воздействий для формирования адекватных моделей контрмер.

мультисервисная сеть связи ограниченного пользования, ресурсы сети связи.

В соответствии с федеральным законом (ФЗ) «О связи» единая сеть электрической связи (ЕСЭС) является сетевой основой всех телекоммуникаций Российской Федерации (РФ) и состоит из сетей связи общего пользования и сетей связи ограниченного пользования (ОгП). В общем составе сетей связи, входящих в ЕСЭС, сеть связи общего пользования является доминирующей, обслуживает подавляющее число пользователей ЕСЭС и определяет устойчивость функционирования ЕСЭС в целом. Сети связи

ОгП ЕСЭС РФ представляют собой сетевую инфраструктуру хозяйствующих субъектов, органов государственной власти и местного самоуправления, государственных структур в сфере обороны, безопасности и охраны правопорядка [1].

Основным видом телекоммуникационной сети связи сетей связи всех категорий ЕСЭС РФ является мультисервисная сеть связи (МССС) с использованием преимущественно пакетных методов передачи, представляющая собой совокупность телекоммуникационных и информационных ресурсов, совместная эксплуатация которых направлена на удовлетворение потребностей пользователей ЕСЭС в традиционных и перспективных услугах связи. В МССС выделяют сети связи общего пользования, которые предоставляют услуги связи конечным пользователям, и технологические сети связи, которые обеспечивают как управление услугами и телекоммуникационным оборудованием (ТКО) сетей связи общего пользования, так и предоставление услуг с использованием тех или иных протоколов взаимодействия.

Взаимодействие ресурсов МССС ОП и ОгП показано на рисунке, ориентировано на предоставление услуг пользователям МССС ОгП, минимизацию количества передаваемой информации между сетями связи, обеспечение безопасности передаваемой информации, формирование отказоустойчивой конфигурации сети связи для обеспечения пользователей услугами доступа к информационным ресурсам (телематическим службам).

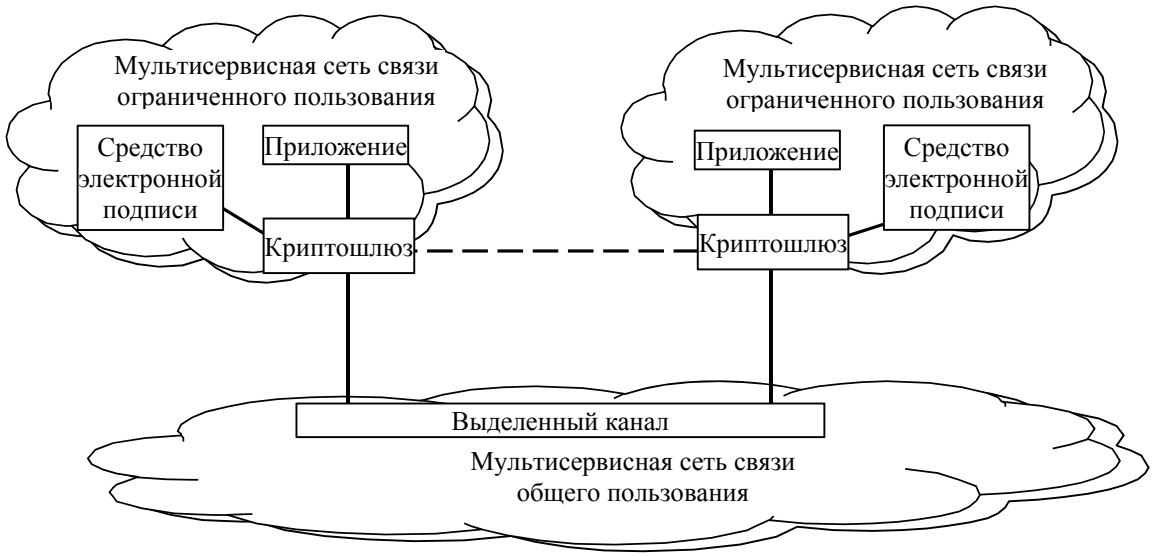


Рисунок. Взаимодействие ресурсов мультисервисной сети связи ограниченного пользования

Ресурсы МССС ОгП в общем случае включают в себя [2, 3] программное приложение пользователя и программное средство электронной подписи, функционирующие на средствах вычислительной техники (СВТ)

и предназначенные для обработки информации, содержащей сведения ограниченного пользования и соединенные между собой прямыми проводами (темным волокном) посредством ТКО, обеспечивающим требуемую стойкость шифрования передаваемой информации (криптошлюзом), а в случае территориальной распределенности, использующие выделенные каналы МССС ОП для передачи информации между соответствующими сегментами МССС ОгП.

Построение выделенного канала для связи МССС ОгП с использованием ресурсов МССС ОП может быть выполнено [4]:

виртуализацией сетей на уровне звена данных эталонной модели взаимодействия открытых систем (ЭМВОС) – бриджами, возможно, с использованием VLAN (*virtualized L2 domain*);

использованием одного или нескольких виртуальных маршрутизаторов на сетевом уровне ЭМВОС, каждый из которых управляет своими интерфейсами, своими маршрутными таблицами и использует свои протоколы маршрутизации и т. д. (*Virtual Routing and Forwarding*, VRFs);

виртуальным («серым») адресным пространством с локальными (частными, внутренними) ip-адресами за («белым») глобальным (публичным, внешним) ip/ppp-адресом на 3 уровне ЭМВОС (Network Address Translation, NAT);

виртуализацией за счет интеграции уровня звена данных и сетевого уровня ЭМВОС с разделением функций пересылки пакетов и управления пересылкой пакетов с использованием последовательных меток (*MultiProtocol Label Switching virtualized path*, MPLS);

виртуализацией псевдопроводом, при которой оборудование как бы подключено к другому оборудованию напрямую, хотя в действительности между соответствующими портами экземпляров оборудования может быть более одной сети передачи (*pseudowire for Ethernet*, EoMPLS *Tunnel*);

виртуализацией, при которой некоторая часть различного оборудования провайдера является одним виртуальным коммутатором, соединяющим точки подключения клиента, при этом не имеющем информации о типе передаваемого трафика и не осуществляющим управление сетью клиента (*Virtual Private* LAN *Service*, VPLS).

С учетом рассмотренных выше особенностей построения и функционирования сегментов, составляющих МССС ОгП целесообразно выделить следующие её основные модели [5]:

модели характеристик ресурсов МССС ОгП,

модель точки присутствия (ТП) ресурсов МССС ОгП,

модели ТКО и СВТ оператора связи, размещенные в ТП МССС ОгП,

модели линейно-технических элементов сетевой инфраструктуры (ЛТЭСИ) МССС ОгП,

модели связей ЛТЭСИ и ТКО и СВТ МССС ОгП,

модели связей ТКО и СВТ и услуг МССС ОгП.

Для перечисленных моделей ресурсов МССС ОгП в соответствии с [6, 7] и учетом особенностей перечисленных выше вариантов реализации выделенных каналов связи МССС ОгП целесообразно выполнить уточнение:

модели источников угроз (модели нарушителей),

модели угроз,

модели воздействий

и, на их основе, выполнить доработку и/или уточнение адекватности моделей контрмер [8] и оценку их качества.

Список используемых источников

1. Федеральный закон Российской Федерации от 7 июля 2003 г. № 126-ФЗ «О связи». Доступ из справ.-правовой системы полнотекстовой базы данных.

2. Стогней А. Перевод приставу: банки начнут массово списывать деньги с должников по судебным решениям [Электронный ресурс]. М. : РБК, 2015. URL: http://quote.rbc.ru/print_news.shtml?news_id=34414237 (дата обращения 17.12.2016).

3. Выписка из перечня средств защиты информации, сертифицированных ФСБ России (по состоянию на 1 декабря 2016 года) [Электронный ресурс]. М. : ФСБ России, 2016. URL: http://clsz.fsb.ru/files/download/svedenia_po_sertifikatam_(011216).doc (дата обращения 17.12.2016).

4. Журавель Е. П., Шерстюк Ю. М. Информационная безопасность в расширенной схеме деятельности организации связи // Проблемы информационной безопасности. Компьютерные системы. 2016. N 2. С. 29–36.

5. Журавель Е. П. Модели ресурсов мультисервисной сети связи // Региональная информатика (РИ-2016) : материалы XV междунар. конф., СПб., 26–28 окт. 2016 г. СПб. : 2013. СПОИСУ, 2016. С. 84.

6. ГОСТ Р ИСО/МЭК 15408-1-2012. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. М. : Стандартинформ, 2014. 51 с. : ил.

7. Исупова Е. А., Курносов В. И., Демидов А. А. Модель негласного добывания нарушителем информации, обрабатываемой на объекте информатизации // Теоретические и прикладные проблемы развития и совершенствования автоматизированных систем управления военного назначения : материалы всеросс. науч.-техн. конф., СПб., 29–30 окт. 2013 г. СПб. : ВИКА им. А. Ф. Можайского, 2013. Ч. 2. Т. 1. С. 151–156.

8. Исупова Е. А., Курносов В. И., Демидов А. А. Модель процесса контроля защищенности информации, обрабатываемой на объекте информатизации // Теоретические и прикладные проблемы развития и совершенствования автоматизированных систем управления военного назначения : материалы всеросс. науч.-техн. конф., СПб, 29 – 30 окт. 2013 г. СПб. : ВИКА им. А. Ф. Можайского, 2013. Ч. 2. Т. 1. С. 161–165.

УДК 004.042:004.91;351.9

АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ СОЗДАНИИ ПРИЛОЖЕНИЙ НА ОСНОВЕ НАБОРОВ ОТКРЫТЫХ ДАННЫХ

Д. В. Журкин[1], О. Н. Рябова[2], Д. В. Сахаров[1]

[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 (Роскомнадзор) по Северо-Западному федеральному округу

В работе даны определения открытым данным, описаны нормативно-правовые акты, рассматриваются возможные уязвимости и недостатки публикации открытых данных. Предлагается эффективный способ использования открытых данных – прототип собственного приложения, использующий набор открытых данных, публикующийся на сайте Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций – Реестр операторов, осуществляющих обработку персональных данных.

открытые данные, общедоступные данные, форматы открытых данных, уязвимости раскрытия открытых данных, приложения на основе открытых данных.

Развитие идеологии открытости власти и широкого привлечения населения к развитию гражданского общества привело к тому, что один из инструментов открытости – открытые данные – становятся не просто наборами статистической информации, а полноценными источниками для технологий BigData и основой для множества социально-полезных приложений. По определению, данному в законодательных актах, открытые данные – это, в первую очередь, информация о деятельности государственных органов и органов местного самоуправления, размещенная в телекоммуникационной сети Интернет в виде наборов, в машиночитаемом формате, предполагающем их автоматическую обработку в целях повторного использования без предварительного изменения человеком, и на условиях ее свободного использования, ограниченного лишь требованиями отсутствия искажений и законности применения [1].

Основные нормативно-правовые акты, которыми регулируется сфера открытых данных: Указ Президента РФ № 601 от 7 мая 2012 г. «Об основных направлениях совершенствования системы государственного управления»; ФЗ № 8 от 09.02.2009 «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления»; ФЗ № 112 от 01.07.2013 «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации».

Распоряжением Правительства РФ № 1187-р от 10 июля 2013 г., определяются 2 перечня общедоступной информации, раскрытие которой в форе открытых данных обязательно.

Первый перечень (для федеральных государственных органов) состоит из 8-ми пунктов, и содержит, помимо перечня названий органов и подотчетных организаций, в том числе сведения о проверках юридических лиц и индивидуальных предпринимателей на очередной год, формируемые в процессе деятельности реестры, сведения о вакантных должностях и так далее. Второй перечень (для органов субъектов Российской Федерации и органов местного самоуправления) значительно длиннее. В него входят 17 пунктов: наименования органов ЗАГСа, занятости населения, органов экспертизы проектной документации, экологической экспертизы, лесной, охот хозяйственный реестры, реестры лицензий на образовательную, медицинскую, фармацевтическую деятельность, другие сведения. Также отметим, что с июля 2017 г. в соответствии с Федеральным законом от 01.05.2016 № 134-ФЗ «О внесении изменений в статью 102 части первой Налогового кодекса Российской Федерации» на сайте ФНС России будут размещены сведения в форме открытых данных о компаниях, такие как среднесписочная численность работников организации за календарный год, о доходах и расходах компании, об уплаченных налогах и сборах, о суммах недоимки и задолженности по пеням и штрафам. Исключение составят только сведения, являющиеся государственной тайной. Благодаря этому налогоплательщики получат дополнительную возможность оценить риски при выборе контрагента.

Наборы открытых данных размещаются в сети Интернет, в том числе на сайте государственного органа и органа местного самоуправления в следующих форматах: CSV (формат представления табличных данных *comma-separated values*) или XML (язык разметки *Extensible Markup Language*). В формате CSV рекомендуется публиковать данные, имеющие плоскую табличную форму, сложные иерархические данные рекомендуется публиковать в форматах XML. Кроме того, вместе с данными, публикуемыми в формате XML, должны публиковаться файлы структурного описания формата в виде схемы XSD (язык описания структуры XML *Schem*a, текстовый формат txt, csv), имеющего спецификацию в виде открытого стандарта. В последнее время широко используется также формат JSON, текстовый формат обмена данными, основанный на JavaScript. Его преимущество в том, что он легко читается людьми, при этом считается независимым от конкретного языка программирования и может использоваться почти с любым из них, во многих есть готовый код для создания и использования данных в формате JSON [2].

На едином портале открытых данных data.gov.ru на декабрь 2016 г. опубликовано более 11,5 тыс. наборов данных, востребованность которых

подтверждается более чем 1,5 млн просмотров и 44,4 тыс. скачиваний, из них только 21 набор – это данные негосударственных структур.

Повышение числа и качества выкладываемых наборов приводит к тому, что ежегодно создается все больше сервисов на основе открытых данных, полезных для населения. Например, запись в поликлинику, отслеживание транспорта и планирование маршрута по мегаполису, рейтинги качества вузов и т. д. Эти сервисы легко доступны – после несложной процедуры регистрации в магазине приложений к ним может быть предоставлен доступ миллионам пользователей. Подобная доступность имеет обратную сторону – стремительное развитие цифровых технологий приводит к тому, что разработчики не успевают учесть все риски кибербезопасности и внедрить эффективные меры их снижения.

Технологически существует два варианта архитектуры: полуавтоматическая Semi-automatic – наборы данных загружаются на портал открытых данных вручную (через веб-интерфейс) и архитектура Real-time (реального масштаба времени) – данные динамически загружаются из порталов открытых данных органов государственной власти либо из других веб-сервисов [3].

Архитектура Semi-automatic подвержена трем рискам:

– фальсификация открытых данных – взломав портал, злоумышленник может подделать открытые данные, повлияв тем самым на работу использующих их цифровых сервисов;

– подделка порталов – злоумышленники могут создать подделки порталов открытых данных, представившись доверенным источником для мобильных сервисов;

– атака на бренд «открытые данные» – рассылка спама с предложениями получить доступ к «расширенным открытым данным» в рамках тестирования или за небольшую плату. На самом деле письма будут содержать вирусы и эксплойты.

В результате реализации этих ситуаций – финансовые и социальные негативные последствия, снижение доверия к открытым данным.

Архитектура Real-time подвержена трем вышеописанным и двум специфичным рискам:

– DDoS-атаки – отказ в обслуживании может привести к недоступности использующих данные цифровых сервисов.

– комплексные целевые атаки – веб-сервис может быть использован как «точка входа» (*entry point*) в ИТ-инфраструктуру органа власти. Даже если ОГВ использует внешние ИТ-ресурсы – веб-сервис необходимо поддерживать и обновлять, а значит ИТ-специалист ОГВ рано или поздно подсоединится к веб-сервису, где его может ждать хакерская утилита, готовая

вытащить его администраторские пароли из оперативной памяти. Таким образом злоумышленники получают плацдарм для изучения и дальнейшего взлома информационных структур ОГВ.

Вышеописанные риски могут привести к значимым негативным социальным и финансовым последствиям, например, социальные волнения (очереди в поликлиниках, претензии национальных меньшинств); убытки предприятий (фальсификация используемой предприятиями нормативно-справочной информации); эффективные теракты (искусственное увеличение плотности человеческого потока в слабо охраняемых местах).

Существуют также плохо исследованные риски, которые могут возникнуть при конгломерации, сравнении и анализе различных наборов ОД, умышленной или неумышленной неверной интерпретации данных и/или применения к ним неподходящих методов анализа; риск того, что из наших открытых данных другие страны-конкуренты извлекут намного больше пользы в ущерб российским компаниям [4].

Для исследования цифровых и нетехнологических рисков при создании приложения на основе ОД госоргана создается собственное защищенное приложение на основе наборов открытых данных под условным названием «Персональные данные под защитой». Суть его следующем: в случаях, когда у нас просят или даже требуют оставить свои персональные данные, например, при заполнении всевозможных анкет или при участии в акциях, при взаимодействии с учреждениями здравоохранения, операторами мобильной связи, различными автосалонами, страховыми компаниями, банками и другими структурами желательно, во-первых, убедиться, что интервьюер включен в реестр операторов персональных данных, во-вторых – запомнить, где и кому мы оставляли свои данные. На сайте Роскомнадзора публикуется набор в формате открытых данных: Реестр операторов, осуществляющих обработку персональных данных. На его основе и создано приложение, позволяющее, прежде чем заполнить какую-либо анкету или просто ответить на вопросы о себе, убедиться в том, что контрагент включен в Реестр операторов ПД. Как минимум, это даст уверенность в том, что он обязан соблюдать требования по защите персональных данных граждан. Прежде чем использовать, а тем более передавать третьим лицам информацию, оператор должен получить от вас письменное согласие на обработку данных в рамках трудового договора, контракта, договора на оказание услуг.

В исполняемый файл приложения внедряются определенные метки, с помощью которых планируется отслеживать запуск приложения и анализировать его использование. Рассматривается возможность ограничить использование приложения только территорией Российской федерации ввиду текущей политической обстановки [5].

На рисунке представлен веб-интерфейс приложения.

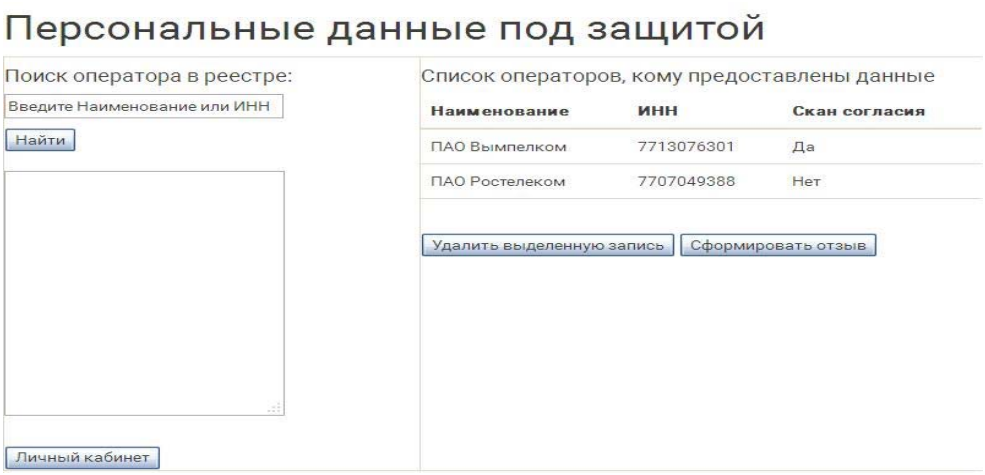


Рисунок. Веб-интерфейс приложения

Перед попаданием в главное меню необходима обязательная аутентификация пользователя. Слева расположен компонент приложения, отвечающий за поиск оператора ПД в реестре, а также личный кабинет пользователя. Справа находится сохраненный список организаций, получивших ваше согласие на обработку персональных данных, в котором пользователь может добавлять редактировать и удалять записи. Реализована возможность формирования отзыва согласия на обработку персональных данных, который можно направить на электронную почту и впоследствии распечатать.

Список используемых источников

1. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

2. Методические рекомендации по реализации принципов открытости в федеральных органах исполнительной власти (утверждены протоколом заседания Правительственной комиссии по координации деятельности открытого правительства от 29 мая 2014 г. N АМ-П36-89пр) [Электронный ресурс]. URL: http://data.gov.ru/metodicheskie-rekomendacii-po-realizacii-principov-otkrytosti-v-federalnyh-organah-ispolnitelnoy (дата обращения 10.02.2017).

3. Бодрик А. Кибербезопасность открытых данных как предпосылка устойчивого развития цифровой экономики [Электронный ресурс] // Компьютерная неделя: электрон. научн. журн. 2016. N 20. С. 9. URL: https://www.pcweek.ru/ gover/article/detail.php?ID=189841 (дата обращения 15.02.2017).

4. Сахаров Д. В., Рябова О. Н. Электронный документооборот ФОИВ. Некоторые аспекты обеспечения информационной безопасности СЭД // Невский Диалог. 2016.

5. Штеренберг С. И., Виткова Л. А., Просихин В. П. Методика применения концепции адаптивной саморазвивающейся системы // Информационные технологии и телекоммуникации. 2014. № 4 (8). С. 126–133.

УДК 621.372

ЧТО ТАКОЕ DWDM СИСТЕМЫ. ЕЁ ОСНОВНЫЕ КОМПОНЕНТЫ. АКТУАЛЬНОСТЬ ИСПОЛЬЗОВАНИЯ И ДАЛЬНЕЙШЕЙ РАЗРАБОТКИ В РОССИИ

В. В. Загорельский, М. С. Корчагин, Ю. А. Фролова

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

Проблема обеспечения растущего спроса на обмен информацией. Необходимость высокой скорости передачи информации на большие расстояния, сохраняя надежность связи. Рассмотрен вариант решения данной проблемы, основанный на принципе плотного волнового мультиплексирования.

плотное волновое мультиплексирование, пропускная способность каналов, мультиплексор, транспондер, усилитель, регенератор.

За последние десять лет многократно выросли потребности людей в обмене информацией. Мировой объем данных, передаваемых по всем сетям, за это время вырос в тысячу раз. Каждый год количество информации в интернете, как минимум, удваивается. Во много раз увеличилась скорость сетей передачи данных и их географический охват. Быстрая и надежная передача видео, голоса и данных приобрела исключительную важность для развития многих сторон жизни современного человека, государственного управления, промышленности и общества в целом.

Повышение скорости и надежности связи стало одной из основных задач государственной важности и национальной безопасности. Для Российской Федерации с ее необъятными просторами величина и скорость информационных потоков вдвойне актуальна, особенно в таких отраслях, как добыча нефти и газа, транспорт, энергетика.

Как удержать высокие темпы роста потребности к передаче и приеме большого количества данных? Оптическое волокно оказалось именно той средой передачи, которая смогла справиться с этими огромными потоками информации. В первое время для деления громадной полосы пропускания отдельного волокна на выделенные каналы связи применялось временное мультиплексирование TDM (*Time Division Multiplexing*). Однако рост сложности оборудования для модуляции и мультиплексирования при увеличении скоростей передачи данных ограничил применения этой технологии.

Дальнейшее [1] увеличение полосы пропускания смог обеспечить альтернативный подход – волновое мультиплексирование WDM (*Wavelength*

Division Multiplexing). Одной из технологий WDM является DWDM (*Dense Wavelength Division Multiplexing*) – плотное волновое мультиплексирование.

Системы спектрального уплотнения DWDM позволяют параллельно использовать несколько оптических несущих для параллельной передачи данных в одном оптоволоконном канале. Они могут использовать один из двух диапазонов несущих длин волн [1]: C-диапазон – 1525–1565 нм (также может встречаться *conventional band* или *C-band*) и L-диапазон – 1570–1610 нм (также может встречаться *long wavelength band* или *L-band*).

Деление на два диапазона обосновано использованием разных оптических усилителей с различными рабочими диапазонами усиления. Ширина полосы усиления для традиционной конфигурации усилителя составляет примерно 30 нм, 1530–1560 нм [1], что является C-диапазоном. Для усиления в длинноволновом диапазоне (L-диапазон) конфигурация эрбиевого усилителя меняется путем удлинения эрбиевого волокна, что приводит к смещению диапазона усиления в длины волн 1560–1600 нм.

Для начала следует разобраться, из чего обычно состоит система уплотнения DWDM (рис. 1):

1) Транспондер.
2) Мультиплексор/демультиплексор.
3) Оптический усилитель.
4) Компенсатор хроматической дисперсии (регенератор).

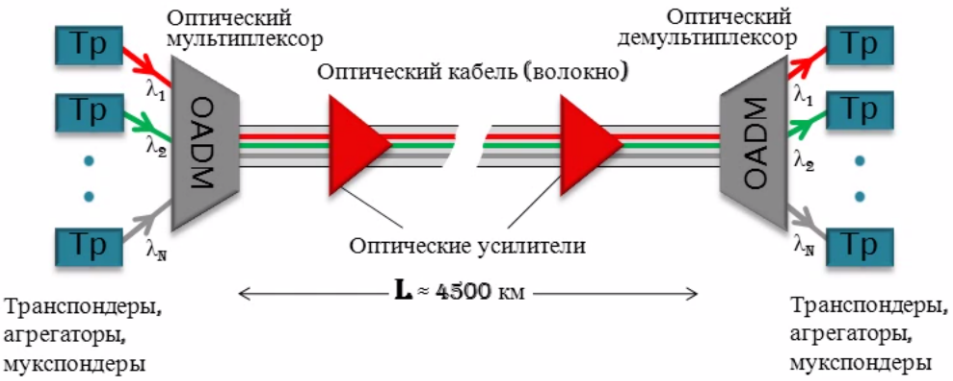


Рис. 1. Система уплотнения DWDM

Транспондер производит 3R-регенерацию («*reshaping*», «*re-amplifying*», «*retiming*» – восстановление формы, мощности и синхронизации сигнала) приходящего клиентского оптического сигнала и позволяет преобразовать длину волны излучения оконечного устройства в длину волны DWDM для передачи в мультиплексор (рис. 2). Транспондер [2] может производить также конвертацию клиентского трафика из одного прото-

кола передачи (зачастую *Ethernet*) в другой, более помехозащищенный (например, OTN с использованием FEC) и передавать сигнал в линейный порт.

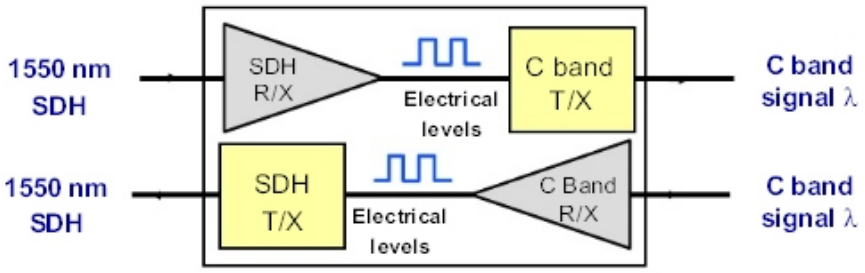


Рис. 2. Транспондер DWDM

Оптические мультиплексоры предназначены для объединения (смешения) отдельных WDM-каналов в групповой сигнал для одновременной их передачи по одному оптическому волокну. Оптические демультиплексоры предназначены для разделения принятого группового сигнала на приемной стороне. В современных системах уплотнения, функции мультиплексирования и демультиплексирования выполняет одно устройство – мультиплексор/демультиплексор.

Поскольку мультиплексоры DWDM рассчитаны на работу с большим числом каналов до 32-ух и более, то наряду с устройствами DWDM, в которых мультиплексируются (демультиплексируются) одновременно все каналы, допускаются также новые устройства (оптический мультиплексор ввода-вывода), не имеющие аналогов в системах WDM и работающие в режиме добавления или вывода одного и более каналов в/из основного мультиплексного потока, представленного большим числом других каналов.

Оптический усилитель на основе примесного оптического волокна, легированного эрбием (*Erbium Doped Fibre Amplifier*-EDFA), увеличивает мощность входящего в него группового (без предварительного демультиплексирования) оптического сигнала без оптоэлектронного преобразования (рис. 3). Усилитель EDFA состоит из двух активных элементов: активного волокна, легированного Er3+ и подходящей накачки. В зависимости от типа, EDFA может обеспечить выходную мощность от +16 до +26 дБм. Увеличение длины передачи сигнала можно быть достигнуто благодаря применению встречного рамановского усиления и удаленной накачки эрбиевых [3] усилителей (до 500 км при скорости 100Гбит/с).

Компенсатор хроматической дисперсии служит для восстановления формы группового сигнала, подавления джиттера и улучшения соотношения сигнал/шум.

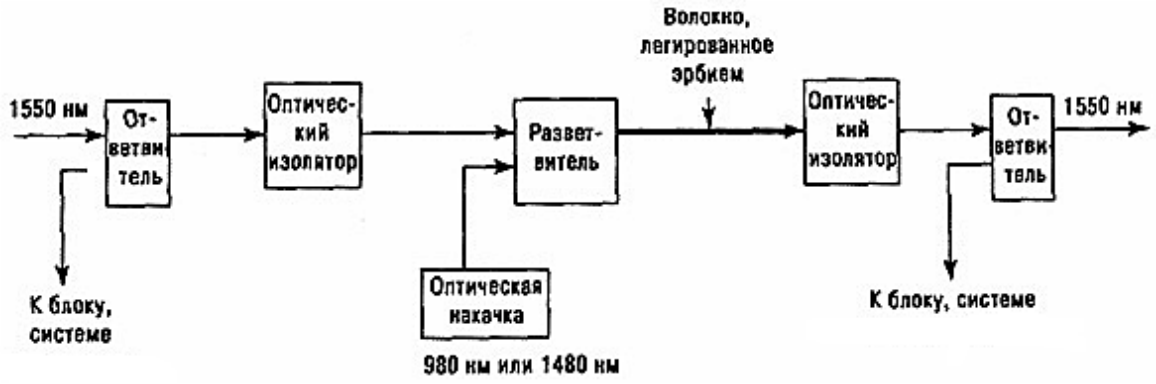


Рис. 3. Схема оптического усилителя DWDM

Наиболее используемый компенсатор хроматической дисперсии на основе решетки Брэгга – DCM FBG (*Dispersion Compensation Module Fiber Bragg Grating*). Пассивное оптическое устройство, состоящее из чирпированного волокна и оптического циркулятора (рис. 4). Чирпированное волокно за счет структуры создает условно отрицательную хроматическую дисперсию входящих сигналов в диапазоне длин волн 1525–1600 нм. Оптический циркулятор [4] в устройстве выполняет роль фильтрующего устройства, направляющего сигналы в соответствующие выводы.

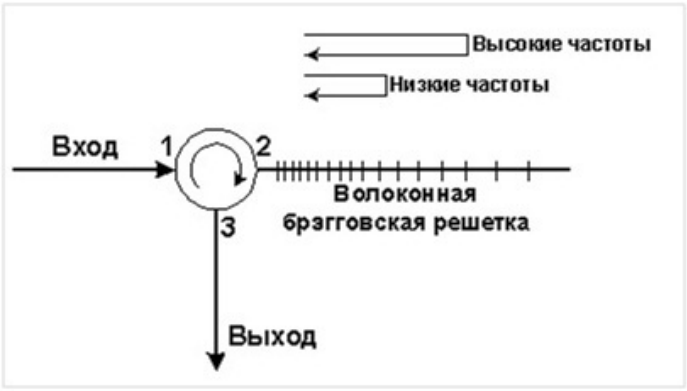


Рис. 4. Компенсатор хроматической дисперсии DWDM

Основные преимущества использования технологии DWDM:

1) высокая пропускная способность каналов (от 10Гбит/с до 1Тбит/с, ведутся разработки увеличения пропускной способности до 25Тбит/с);

2) из предыдущего пункта можно сделать вывод, что имеется возможность наращивания пропускной способности волоконно-оптической линии связи (ВОЛС) по мере роста требований рынка;

3) передача данных со скоростью 100Гбит/с на расстояния до 500 км без промежуточных усилителей (однопролетная линия) и до 8000 км в многопролетной линии, что очень важно в экономическом плане для нашей страны;

4) быстрая окупаемость вложенных в ее внедрение средств и получение прибыли. Более того, нет необходимости прокладывать новые линии, что также связано с дополнительными расходами и проблемами, так как эта технология создана не для создания новых волоконно-оптических сетей, а для модернизации и расширения существующих сетей в целях существенного повышения их пропускной способности и доступности.

5) на базе DWDM сетей можно объединять сети разных производителей для передачи разнородного трафика.

Заключение. В Российской Федерации есть множество компаний, которые занимаются научным исследованиями, разработкой и практическим применением технологии DWDM. Это такие компании как «ИРЭ-Полюс» и «Т8». Компании «Т8» удалось в лабораторных условиях передать 1 Тбит информации за одну секунду на линии 500 км без промежуточного усиления. Также разработана российская DWDM система с канальной скоростью 100 Гбит/с и спектральной эффективностью 3 бит/с/Гц. Пропускная способность такой системы – до 27 Тбит/с.

Из вышесказанного можно сделать вывод, что технология плотного волнового мультиплексирования DWDM это будущее инфокоммуникационных технологий. Для Российской Федерации очень важно повышение скорости и надежности связи, которые будут способствовать увеличению темпов роста экономики страны.

Список используемых источников

1. Андрэ Жирар. Руководство по технологии и тестированию систем WDM. М. : EXFO, 2001. 119 с.

2. Глудкин О.П., Черняев В.Н. Технология испытания микроэлементов радиоэлектронной аппаратуры и интегральных микросхем: учеб. пособие для вузов. М. : Энергия, 1980. 360 с.

3. Техническая статья Infinera [Электронный ресурс] // Скорость передача данных по суперканалам в сетях DWDM превышает 100 Гбит/с. WP-SC-12-2011. URL: https://www.infinera.com/russian/files/RU-Infinera-DWDM_Networks.pdf (дата обращения 02.02.2017).

4. Боровиков М. А. Методы мониторинга в системах DWDM (Часть 1) [Электронный ресурс]. URL: https://habrahabr.ru/post/246095/ (дата обращения 02.02.2017).

Статья представлена директором ИВО, кандидатом педагогических наук, доцентом А. А. Лубянниковым.

УДК 004.822

ПРИМЕНЕНИЕ ПОДХОДА LINKED KNOWLEDGE В ЗАДАЧАХ СЕМАНТИЧЕСКОГО АНАЛИЗА СЛАБОСТРУКТУРИРОВАННЫХ ИНФОРМАЦИОННЫХ РЕСУРСОВ

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 применения подхода Linked Knowledge в задачах семантического анализа слабоструктурированных ресурсов. Данный подход базируется на применении онтологической модели представления знаний о предметной области с учетом разнообразия семантических контекстов. В работе представлена структура базы знаний, разработанной на основании предложенной модели.

семантика, онтология, Linked Knowledge, слабоструктурированные ресурсы.

Задача выделения семантики из слабоструктурированных информационных ресурсов, представленных конструкциями на естественном языке (ЕЯ), в настоящий момент является наиболее актуальной в области информационной безопасности, а также при поддержке принятия управленческих решений в режиме временных ограничений [1, 2, 3].

Использование подхода Linked Knowledge (с англ. «связанные знания») предполагает адаптацию алгоритмов анализа ЕЯ к особенностям конкретной ПрО и позволяет решить проблемы описания и идентификации связей между понятиями ПрО с целью извлечения ее семантической составляющей.

В первую очередь, подход Linked Knowledge базируется на применении модели онтологии предметной базы знаний (БЗ), позволяющей описать ПрО с учетом многообразия ее контекстов, под которыми понимается состояние содержимого БЗ, которое может быть сформировано из множества состояний БЗ, полученного в результате формирования содержимого БЗ с различных точек зрения («*points of view*») [4].

В широком смысле, онтологии – это модели, являющиеся формой представления знаний в рамках отдельных контекстов ПрО в виде семантических информационно-логических сетей взаимосвязанных объектов, где в качестве главных элементов выступают понятия ПрО с их свойствами и отношения между объектами [5].

Онтологии выполняют интегрирующую функцию, обеспечивая общий семантический базис в процессах принятия решений, интеллектуального анализа данных и единую платформу для объединения разнообразных информационных систем.

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 [6].

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*»).

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.

Архитектура БЗ, реализованной на основе описанной модели, представлена на рис. 1.

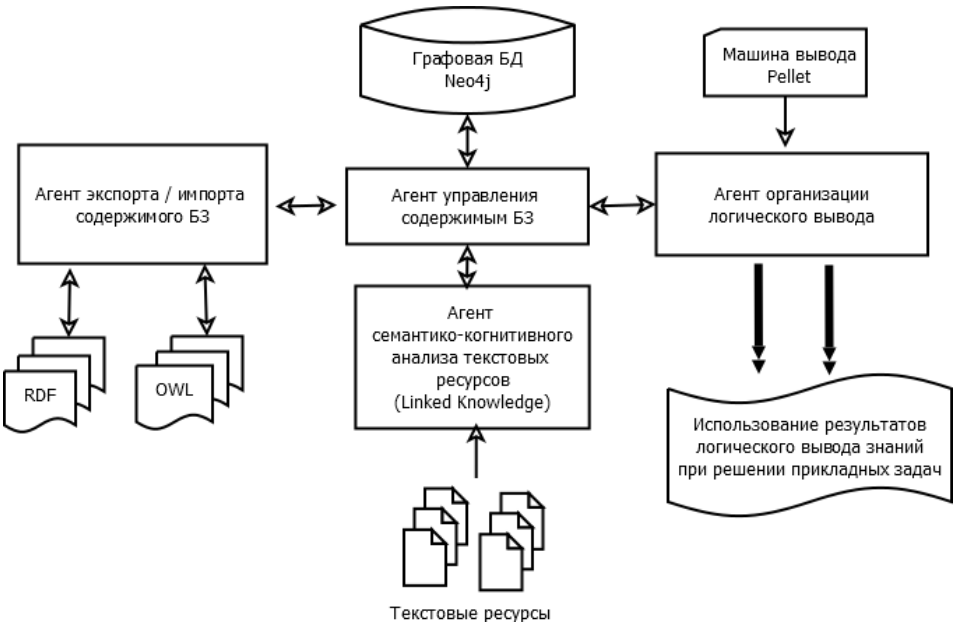


Рис. 1. Архитектура БЗ

БЗ состоит из нескольких агентов, которые тесно взаимодействуют между собой:

– агент управления содержимым БЗ;

– агент импорта/экспорта содержимого БЗ из/в различные форматы описания онтологии ПрО (RDF, OWL и т. д.);

– агент семантико-когнитивного анализа текстов;

– агент для организации логического вывода по содержимому БЗ.

В качестве хранилища онтологии агента управления знаниями используется графовая база данных Neo4j [7], обладающая следующими преимуществами:

1. Нативный формат хранения графов.

2. Один экземпляр СУБД может обслуживать графы с миллиардами узлов и связей.

3. Может обрабатывать графы, которые полностью не помещаются в оперативную память.

Агенты выполняются в контейнере сервлетов Jetty [8], имеющем модульную архитектуру, что позволяет использовать только необходимый функционал, снижая нагрузку на сервер. Также Jetty хорошо масштабируется для обслуживания многих соединений со значительным временем простоя между запросами и позволяет обслуживать большее количество пользователей.

Все перечисленные ресурсы, приложения и технологии являются бесплатными и свободно распространяемыми.

Разработанная в рамках данного проекта программная система позволила реализовать следующую структуру элементов базы знаний с учетом

контекстов «points-of-view» на примере предметной области структуры и строения кораблей ВМФ РФ (рис. 2).

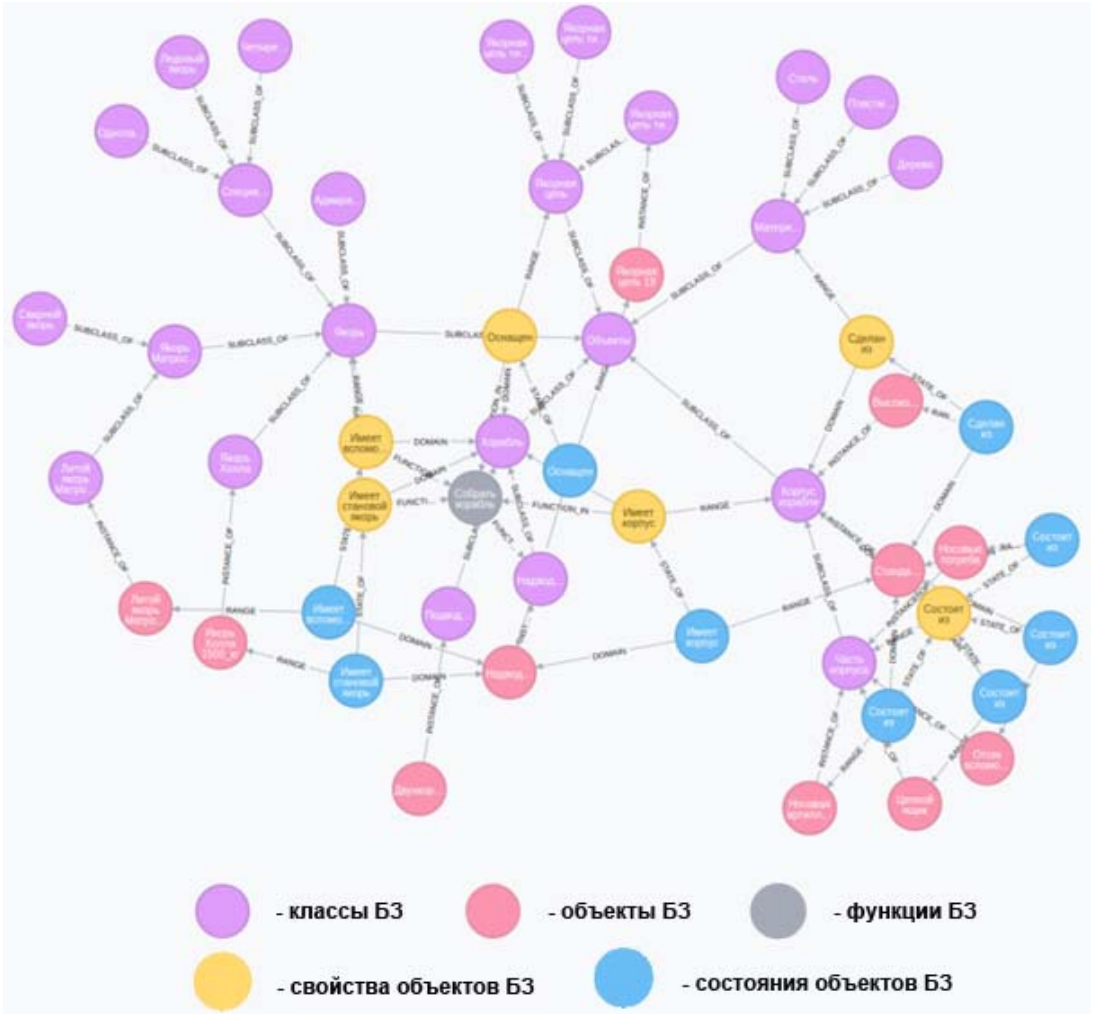


Рис. 2. Граф БЗ

В заключении необходимо отметить, что использование методологии Linked Knowledge в процессе извлечения семантико-когнитивной составляющей слабоструктурированных ресурсов позволит решать множество прикладных задач, связанных с удаленной технической поддержкой, с возможностью оценки правильности ответов, изложенных на естественном языке, а также с обеспечением информационной безопасности посредством обнаружения утечки персональных данных, а также данных, составляющих корпоративную или государственную тайну.

Исследование выполнено в рамках ПНИЭР по теме «Разработка архитектуры, методов и моделей построения программно-аппаратного комплекса семантического анализа слабоструктурированных информационных ресур-

сов 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. Грибова В. В., Клещев А. С. Управление проектированием и реализацией пользовательского интерфейса на основе онтологий // Проблемы управления. 2006. № 2. С. 58–62.

2. Загорулько Ю. А. Построение порталов научных знаний на основе онтологии // Вычислительные технологии. 2007. Т. 12. № S2. С. 169–177.

3. Филиппов А. А., Наместников А. М., Субхангулов Р. А. Разработка инструментария для интеллектуального анализа технической документации // Известия Самарского научного центра Российской академии наук. 2011. Том 13. № 4. С. 984–990.

4. 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.

5. Гаврилова Т. А. Онтологический подход к управлению знаниями при разработке корпоративных информационных систем // Новости искусственного интеллекта. 2003. № 2. С. 24.

6. Карабач А. Е. Системы интеграции информации на основе семантических технологий // Наука, техника и образование. 2014. № 2 (2). С. 58–62.

7. Neo4j. URL: https://neo4j.com/product (дата обращения 10.03.2017).

8. Greg Wilkins Jetty vs Tomcat: A Comparative Analysis, 2008. URL: http://www.webtide.com/choose/jetty.jsp (дата обращения 9.03.2017).

УДК 004.056

АНАЛИЗ СУЩЕСТВУЮЩИХ НОРМАТИВНЫХ ДОКУМЕНТОВ ДЛЯ ФОРМИРОВАНИЯ ПОЛИТИКИ БЕЗОПАСНОСТИ В СИСТЕМЕ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА ВУЗА

Т. Е. Захарова, А. Ю. Цветков

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

Рассмотрено понятие системы электронного документооборота. Выделены основные российские стандарты, и выявлена необходимость в рекомендациях для внедрения системы электронного документооборота и формирования безопасности

для разного типа организации. Показан возможный способ защиты информации на основе существующих нормативно-правовых документов в сфере электронного документооборота на примере высшего учебного заведения.

система электронного документооборота, защита данных, информационная безопасность, нормативные документы, контроль доступа, аутентификация, электронная подпись, смарт-карта.

В век информатизации высшие учебные заведение по всей стране развиваются с необычайно высокой скорость, качество обучение требует поиска и реализации более эффективных направлений деятельности в области использования информационно-телекоммуникационных технологий в управлении вузом и во всем учебном процессе. Одной из таких технологий является система электронного документооборота.

Система электронного документооборота (СЭД) – это автоматизированная многопользовательская система, позволяющая организовать работу с электронными документами (создание, изменение, поиск, хранение), а также взаимодействие между сотрудниками (обмен документами, назначение заданий, отправка уведомлений).

На текущий момент в Российской Федерации (РФ) СЭД находится в стадии внедрения во многие государственные учреждения. К сожалению, пока не для всех типов организации существуют государственных стандартов (ГОСТ) для внедрения СЭД, но есть несколько ГОСТов, определяющих различные сферы электронного документооборота.

Например, ГОСТ 53898-2013 [1]. Этот российский стандарт, устанавливающий требования к электронному сообщению (ЭС), обеспечивающему взаимодействие систем управления документами, в части формата, состава и содержания. В данном ГОСТе сделан акцент на описании паспорта и конверта ЭС, которые являются обязательной его частью. Также описаны структура, заголовки и другие составляющие дополнительных сообщений, которые не являются обязательными.

Любую систему, а тем более связанную с информационными технологиями (ИТ) и данными в цифровом формате, необходимо обезопасить от взломов и краж. Поэтому стоит уделить внимание нормативно-правовым документам по обеспечению информационной безопасности (ИБ) электронного документооборота (ЭД). Под информационной безопасностью во всем мире понимают механизмы защиты, обеспечивающие конфиденциальность, целостность и доступность.

Для начала рассмотрим ГОСТ 15408 [2]. Он описывает методы и средства обеспечения безопасности, критерии оценки безопасности информационных технологий, по результатам которых при эксплуатации, внедренной СЭД пользователи могут решить, отвечает ли она ИТ потребностям в безопасности. Благодаря этому ГОСТу можно достичь определённого уровня

уверенности, что функциональные возможности безопасности системы, а также меры доверия, предпринятые по отношению к ней, отвечают предъявляемым требованиям.

Существует несколько национальных стандартов РФ для информационных технологий «Методы и средства обеспечения безопасности», непосредственно связанных друг с другом. Рассмотрим некоторые из них.

ГОСТ 27001-2006 – предполагаемая модель для разработки, внедрения, функционирования, мониторинга, анализа, поддержки и улучшения системы менеджмента информационной безопасности (СМИБ) [3]. Немаловажную роль на внедрение СМИБ влияют потребности и цели, преследуемые пользователями, требования безопасности, используемые процессы, а также масштабы деятельности и структура организации.

ГОСТ 27002-2012 состоит из нескольких глав, которые с разных сторон описывают информационные технологии, а точнее различные правила безопасного и эффективного управления ими [4]. Требования к ИБ определяются с помощью трех факторов: оценка рисков, законодательные и юридические требования и специфический для каждой организации набор целей, принципов и требований. В каждом разделе можно найти меры и средства контроля и управления, рекомендации по реализации и дополнительную информацию по той или иной сфера менеджмента ИБ.

Так как одной из важной частью надежности СЭД для пользователей является возможность безопасного входа с разграничением доступа для разных пользователей, то в данном стандарте стоит особое внимание уделить главе «Управление доступом».

Данный раздел содержит информацию о различных направлениях в сфере контроля доступа. Представлена политика и регламент требований организации. Описана важность обеспечения контроля за доступом пользователей начиная от регистрации и заканчивая снятием их с таковой. Рассматриваются обязанности пользователей по использованию паролей и оборудования, находящегося в их ведомстве. Сделан акцент на контроле сетевого доступа, доступа к операционной системе и приложениям. Важно контролировать обращение легитимных и нелегитимных пользователей к внутренним и внешним сетевым ресурсам компании. Должен быть составлен план, определяющий права сотрудников и ресурсы, к которым возможен доступ. Всевозможные вторжения, ошибки и неправомерные действия можно предупредить, если в организации введен мониторинг и анализ действий, происходящих в системе. Сбор и обработка информации позволят не просто обнаружить отклонения от требований политики контроля доступа, но и доказать все неавторизованные действия.

Рекомендации мер, средств и способов реализации контроля и управления, указанные в главе «Управление доступом» должны обеспечить

достижение целей ИБ, их можно принять как руководящие. Данные мероприятия значительно снизят риски и затраты на устранение проблем, если включить их в план еще на стадии разработки проекта информационной системы.

Рассмотрим возможные способы защитить информацию в СЭД на основе вышеописанных рекомендаций ГОСТ.

Для непосредственной защиты электронного документа используется электронная подпись документа (ЭП). Она представляет собой информацию в электронном виде – реквизиты, которые привязаны к электронному документу (ЭД). Эти реквизиты получаются за счет криптографических преобразований с использованием закрытого ключа подписи, благодаря им можно проверить была ли переданная информация искажена после формирования подписи, авторство и сам факт подписания ЭД.

В России существует федеральный закон № 63, описывающий виды электронной подписи (ЭП), принципы её использования, правовое регулирование отношений в этой сфере, условия равнозначности с обычной подписью, средства и компоненты подписи, а также возможность получения ЭП [5]. Описание процессов формирования и проверки электронной подписи дается в ГОСТ 34.10-2012 [6]. Данный стандарт основывается в свою очередь на стандарте 34.11-2012 о хеш-функции [7]. В нем можно найти алгоритмы и процедуры вычисления ЭП.

Чтобы защитить информацию не только от подделки, но и от краж применяют аутентификацию пользователей. Сейчас существует несколько способов прохождение данной процедуры. Самая популярная – парольная. В ней сочетается логическая ясность и простота реализации. Но также она является наиболее уязвимой, поэтому всегда необходимо использовать комплекс мер по защите.

Аутентификация с помощью смарт-карт является одним из надежных способов персонализации пользователей. Смарт-карта – это пластиковая карта со встроенной микросхемой, позволяющая произвести аутентификацию, хранить некоторые данные в защищенной среде и проводить криптографические операции. Чаще всего их используют в системах контроля и управления доступом, например, студенческие в вузах и общежитиях, проездной билет, электронные и биометрические паспорта. Такие карты также можно использовать и для удостоверения личности пользователя в СЭД, если смарт-карта будет хранить в себе зашифрованные сертификаты аутентификации и электронной подписи, полученный от системы управления ключами вместе с другой информацией о владельце. Один из минусов такой системы – затраты на приобретение смарт-карт и оборудования для считывания.

Еще одним из популярных средств аутентификации стали токены. Это небольшие карманные устройства, обеспечивающие безопасность информации и идентификацию его владельца. Основное их предназначение – электронное удостоверение личности, при этом можно использовать как вместо пароля, так и совместно с ним (двухфакторная аутентификация). Данный метод чаще используют в банковских системах и системах, где есть необходимость обеспечить высокий уровень защиты. На данный момент существуют и программные токены встроенные в смартфон.

Не так давно европейские разработчики предложили миру новый способ аутентификации методом сравнения фоновых шумов – Sound-Proff. Необходимо лишь установить на смартфон программу и в дальнейшем на сайтах, поддерживающих эту технологию станет возможна авторизация с помощью данной технологии. Компьютер и смартфон в течении нескольких секунд анализируют фоновые шумы вокруг вас, и если они будут совпадать, то система разрешит вход. Данный метод не дает вам полной надежности сохранения данных и требует доработок.

Во всех выше описанных методов существует необходимость шифрования информации и безусловно важно чтобы такая защита происходила по нашим стандартам. В России с 1989 г. действует ГОСТ 28147 о криптографической защите и методах шифрования [8]. В нем описан единый алгоритм криптографического преобразования, который обязателен для всех организаций, обеспечивающих создание, обработку, хранение и другие действия с данными в электронном формате. Описаны 4 режима работы симметричного блочного шифрования: простой замены, гаммирования, гаммирования с обратной связью и выработка имитовставки. Важным достоинством является то, что атака полным перебором невозможна, как и навязывание ложных данных. Высокая эффективность и быстродействие на современных компьютерах являются преимуществами при использовании.

В результате анализа нормативных документов можно сделать следующие выводы:

– все стандарты в основном описывают лишь общие положения по обеспечению контроля доступа и управлением информацией;

– нет рекомендаций, которые позволят учесть специфику различных государственных организации, например, вузов.

В рамках внедрения СЭД в вузы есть потребность в описании более конкретной последовательности действий при защите информации в данной системе с учетом необходимых функции, принципов и потребностей пользователей.

Во-первых, следует обозначить тип аутентификации. Использование двухфакторной аутентификации (2FA), является наилучшим выбором. Это позволит точно идентифицировать личность пользователя, сделать пе-

редачу логина и пароля третьим лицам нецелесообразной, так как будет присутствовать второй тип аутентификации, который физически может находится только у его обладателя и присущ только ему. Пример средств 2FA:

1. Логин и пароль.
2. Смарт-карта с сертификатом аутентификации и ЭП.

Использование смарт-карт обусловлено тем, что в большинстве вузов уже используется данный тип оборудования в качестве пропуска в здания университета и общежития, следовательно, у них уже есть созданная база студентов с их идентификаторами, остается только дополнить необходимой информацией.

Помимо аутентификации необходимо правильно организовать процесс авторизации – спроектировать разграничения прав пользователей к тем или иным ресурсам. Рассмотрим классическую модель субъект – объект. Где существует субъект – администратор СЭД, имеющий право конфигурировать листы доступа для всех остальных субъектов системы. В такой модели для каждой пары (субъект-объект) необходимо задавать только очевидный и однозначный перечень легитимных правил доступа, являющиеся разрешенными для данного субъекта к данному объекту.

В структуре ВУЗа можно выделить 4 типа субъектов:

- администратор СЭД;
- администрация учреждения;
- административные работники;
- профессорско-преподавательский состав;
- студенты.

Примером реализации модели субъект-объект в данном случае может стать студент, который имеют возможность ознакомиться с учебно-методической литературой и таблицей учета посещаемости без права редактирования, а также вносить и редактировать отчетные документы по изученному теоретическому и практическому материалу.

Выше рассмотренные нормативные документы, а также существующие модели авторизации при применении к системе электронного документооборота на примере высшего учебного заведения требуют учесть множество индивидуальных направлений деятельности вуза, такие как учебно-методическая, научная, административная работа и каждая из них имеет свои особенности. Для унификации внешнего и внутреннего документооборота ВУЗов требуется разработать единый метод внедрения и развертывания СЭД, а также политику безопасности, соответствующую государственным стандартам Российской Федерации.

Список используемых источников

1. ГОСТ Р 53898-2013. Системы электронного документооборота. Взаимодействие систем управления документами. Технические требования к электронному сообщению. М. : Стандартинформ, 2015. 46 с.

2. ГОСТ 15408-1-2012. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. М. : Стандартинформ, 2014. 56 с.

3. ГОСТ Р ИСО/МЭК 27001-2006. Информационная технология. Методы и средства обеспечения безопасности. Систем менеджмента информационной безопасности. Требования. М. : Стандартинформ, 2008. 26 с.

4. ГОСТ Р ИСО/МЭК 27002-2012. Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности. М. : Стандартинформ, 2014. 97 с.

5. Федеральный закон от 06.04.2011 N 63-ФЗ (ред. от 23.06.2016) «Об электронной подписи». URL: http://www.consultant.ru/document/cons_doc_LAW_112701/ (дата обращения 15.02.2017).

6. ГОСТ Р 34.10-2012. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. М. : Стандартинформ, 2012. 29 с.

7. ГОСТ Р 34.11-2012. Информационная технология. Криптографическая защита информации. Функция хеширования. М. : Стандартинформ, 2012. 34 с.

8. ГОСТ 28147-89. Система обработки информации. Защита криптографическая. М. : ИПК Издательство стандартов, 1996. 26 с.

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

УДК 004.056.53

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ПРОЦЕССЕ СОЗДАНИЯ И ИСПОЛЬЗОВАНИЯ ПРОГРАММ ДЛЯ ЭВМ

А. Е. Зимин, Н. А. Косов

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

Данная работа посвящена вопросам обеспечения информационной безопасности в процессе создания и использования программ для ЭВМ, как объектов интеллектуальной собственности. Дается характеристика организационных, правовых и технических мер, обеспечивающих информационную безопасность при создании программ для ЭВМ. Анализируются проблемы защиты авторских прав в процессе использования программы

для ЭВМ. Предлагаются практические решения по усилению защиты исключительного права правообладателей в отношении программ для ЭВМ.

интеллектуальная собственность, программа для ЭВМ, авторское право, водяной знак.

Активное развитие информационных технологий и все большая компьютеризация нашего общества четко обозначают проблему обеспечения авторских прав на программные продукты.

«Программы для ЭВМ» являются одним из видов интеллектуальной собственности, и целесообразно говорить об обеспечении ее информационной безопасности в процессе создания и, особенно, использования, т. к. в случае неправомерного использования созданной программы для ЭВМ третьими лицами автор, либо правообладатель такой программы может нести финансовые убытки.

Согласно ст. 1261 ГК РФ, программой для ЭВМ является представленная в объективной форме совокупность данных и команд, предназначенных для функционирования ЭВМ и других компьютерных устройств в целях получения определенного результата, включая подготовительные материалы, полученные в ходе разработки программы для ЭВМ, и порождаемые ею аудиовизуальные отображения.

В настоящее время в большинстве стран мира программы для ЭВМ подлежат авторско-правовой охране, и занимают особое место среди других объектов авторских прав в силу специфических особенностей правового режима.

Согласно ст. 1259 действующего ГК РФ программы для ЭВМ охраняются как литературные произведения, но слово «как» лишь подчеркивает особый характер программ для ЭВМ как объекта прав, указывая на то, что литературными произведениями они не являются. Как отмечается: «Программы для ЭВМ условно приравниваются к литературным произведениям для целей охраны авторским правом» [1].

Выходит, что программы для ЭВМ – это объект интеллектуальной собственности, имеющий специфическую информационную природу, что обуславливает то, что защита авторских прав здесь теснейшим образом связаны с технологиями защиты информации.

Для обеспечения информационной безопасности программы для ЭВМ как объекта интеллектуальной собственности при ее создании и использовании, выделяются три следующих аспекта защиты авторских прав: правовые, организационные и технические.

Правовые средства защиты предусмотрены ГК РФ.

Согласно п. 3 ст. 1228 ГК РФ, исключительное право на результат интеллектуальной деятельности, созданный творческим трудом, первона-

чально возникает у его автора. Это право может быть передано автором другому лицу по договору, а также перейти к другим лицам по иным основаниям, установленным законом.

Ввиду потенциального распространения созданных программ для ЭВМ с целью получения прибыли, рационально также обеспечить организационные меры защиты авторских прав. Так, например, программа может быть зарегистрирована в Федеральной службе по интеллектуальной собственности (Роспатент). Но регистрация программы для ЭВМ происходит на добровольной основе и не всегда обязательна.

Самым же используемым организационным способом защиты интеллектуальной собственности является заключение лицензионного договора.

Как известно, право использования программы для ЭВМ может быть передано на основании лицензионного договора, заключаемого по общему правилу в письменной форме. Его нарушение влечет за собой ответственность, предусмотренную законодательством РФ.

Техническими признаются любые технологии, технические устройства или их компоненты, контролирующие доступ к произведению, предотвращающие либо ограничивающие осуществление действий, которые не разрешены автором или иным правообладателем в отношении произведения, а также препятствующие неправомерному переходу права авторства на программы для ЭВМ потенциальному злоумышленнику.

В наше время основное большинство программ разрабатывается на основе технологии Java.

Технология Java широко рассматривается, как эволюционная в связи со своим свойством портативности: идея заключается в том, что одна и та же программа может запускаться на многих разных типах компьютеров, потребительских гаджетов и других устройств. Для пользователей Java позволяет компьютерам и другим устройствам взаимодействовать друг с другом намного проще, чем когда-либо прежде. Тем не менее, это эволюционное свойство Java привело нас к проблеме защиты от кражи программы. Java-апплеты, размещенные на интернет-сайтах и Java-приложения, проданные пользователям, в настоящее время страдают от краж. Это связано с тем, что Java-программы можно легко разложить на многоразовые файлы классов и исследовать с помощью средства просмотра или редактора классов.

Кроме того, пользователи программы могут получить исходный код файла класса с помощью декомпиляторов, таких как Mocha, SourceAgain и т. д. В такой ситуации интеллектуальная собственность разработчика программы на Java может быть похищена, если пользователь программы украдет файл класса разработчика и встроит его в свою собственную программу. Мы называем это нарушением авторских прав путем кражи программы.

В этой статье предлагается метод, который препятствует краже программы, встраивая в программы Java цифровые водяные знаки. Мы утверждаем, что внедрение подписи разработчика программы в качестве водяного знака в Java-файлы классов будет препятствовать хищению программ. Ниже мы опишем основные особенности нашего метода применения водяных знаков:

1. Пользователи программы вряд ли могут узнать местоположение водяного знака, поэтому стирание и/или подделка водяного знака для них очень трудны.

2. Водяные знаки в программах будут храниться скрытно от пользователей программ, даже если бы наш метод встраивания или инструмент встраивания был открыт для публики.

3. Даже в случае, если только часть программы была украдена и встроена в другую программу, водяной знак легко декодируется там, где он может существовать в программе.

4. Водяные знаки в программах не снижают эффективность выполнения.

Водяные знаки могут использоваться как доказательство авторства программы.

Даже в случае обнаружения незаконной программы часто нелегко сказать, кто является истинным разработчиком этой программы. Потенциальный нарушитель, который украл какой-либо файл класса может настаивать на том, что именно он разработал эту программу. В этом случае нам нужно доказательство, чтобы опровергнуть заявление похитителя.

В этой ситуации подпись, ранее встроенная в программу в качестве водяного знака, подтверждает подлинность заявлений владельцев оригинальных приложений и защищает права собственности. Водяной знак в программе позволяет проверить факт выполнения программы. Расшифровка водяного знака из подозрительной программы позволит определить, кто является первоначальным разработчиком этой программы.

Одной из основных проблем в современном мире информационных технологий является поиск незаконного использования программ [2].

Разработчикам Java-приложений нелегко найти нелегальную программу, содержащую украденный файл класса.

Например, мы, возможно, не сможем выяснить, является ли программа незаконной или нет, выполнив ее, потому что незаконные программы часто не похожи на оригинальные программы в своих спецификациях, если украденная часть мала. Эта сложность в поиске нелегальной программы является одной из важнейших проблем для разработчиков Java-программ.

Мы считаем, что водяной знак эффективен для поиска незаконной программы в ситуации с Интернетом. Незаконные программы могут быть легко обнаружены с помощью агента-декодирования водяных знаков (робота),

который проходит через Интернет. Если программа оказалась незаконной, содержащей водяной знак оригинального разработчика программы, агент сообщит об этом разработчику. Используя этот агент, разработчики могут автоматически найти незаконную программу, чтобы они могли защитить свои программы от программных похитителей.

Учтем основные важные свойства водяных знаков, которые должны удовлетворить цели при разработке метода кодирования водяных знаков [3]. Мы утверждаем, что метод кодирования должен удовлетворять следующим шести критериям:

1) Кодирование водяных знаков не изменяет спецификации программы.

Это свойство должно быть удовлетворено в любом методе кодирования для компьютерных программ.

2) Человек, который кодировал водяной знак, может декодировать его автоматически.

Это естественно, что разработчики программ хотят легко проверять, содержит ли конечная программа украденную программу или нет. Разработчики программ не хотят читать или анализировать программу на поиск водяного знака. С этой точки зрения, водяные знаки должны быть автоматически декодируемы с конечной программы. Проектирование метода кодирования должно учитывать простоту декодирования.

3) Водяной знак в программе декодируем, в каком бы месте программы он ни находился.

Злоумышленник может украсть компонент программы различных размеров и встроить его в свои программы различными способами. В этом случае, алгоритм декодирования не должен зависеть от места нахождения водяного знака.

4) Метод стирания или фальсификации водяного знака не должен выводиться из метода кодирования водяного знака.

Не исключено, что похитители программного кода могут знать метод кодирования, поскольку мы описываем метод в этой статье.

5) Водяные знаки в программах не должны уменьшать эффективность исполнения.

Поскольку некоторые программы очень чувствительны к уменьшению эффективности исполнения, это свойство должно быть учтено.

6) Водяные знаки должны выдерживать преобразования программ.

Злоумышленники могут разбирать и заново собирать, декомпилировать и перекомпилировать, оптимизировать программу или использовать различные инструменты для преобразования программ, такие как обфускатор, шифратор и так далее. Водяные знаки должны быть надежно декодируемы даже после того, как были применены эти преобразования.

Список используемых источников

1. Близнец И. А., Леонтьев К. Б. Авторское право и смежные права: учебник / Под ред. И. А. Близнеца. М. : Проспект, 2011. 138 с.
2. Хомяков И. Н., Красов А. В. Скрытое вложение информации в структуру байт-кода Java // Системы управления и информационные технологии. 2014. Т. 56. № 2. С. 89–93.
3. Красов А. В., Штеренберг С. И. Разработка методов защиты от копирования ПО на основе цифровых водяных знаков внедряемых в исполняемые и библиотечные файлы // Актуальные проблемы инфотелекоммуникаций в науке и образовании. II Международная научно-техническая и научно-методическая конференция: сб. науч. ст. СПб. : СПбГУТ, 2013. С. 847–852.

Статья представлена научным руководителем, кандидатом философских наук, доцентом А. И. Пешковым.

УДК 621.391.579.72

АНАЛИЗ СПОСОБОВ ФОРМИРОВАНИЯ ОБЩЕГО КЛЮЧА ДЛЯ СОПРЯЖЕНИЯ МОБИЛЬНЫХ УСТРОЙСТВ

Е. О. Зуева, В. А. Яковлев

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

Проведен анализ способов аутентификации пары мобильных устройств, формирующих общий ключ для защищенной связи между ними. Рассмотрены способы на основе использования дополнительных каналов: визуального, акустического, вибрационного и магнитометрического. Разработана система показателей и критериев для сравнения этих способов с учетом удобства их использования пользователями.

аутентификация, мобильные устройства, дополнительный канал.

Широкое распространение мобильной связи привело к необходимости обеспечения безопасности соединений в режиме реального времени. Однако пользователь мобильного телефона не всегда может быть уверен в том, что его оператор сотовой связи защищает свои радиоканалы путем шифрования данных, передаваемых между абонентом и базовой станцией. В связи с этим развиваются способы создания безопасного соединения между двумя абонентами без помощи доверенной третьей стороны.

Для формирования ключа такого соединения используют, как правило, метод Диффи-Хеллмана, который требует дополнительной аутентификации

ключа. Эта задача может быть решена на основе использования дополнительных каналов: визуального, акустического, вибрационного или магнитометрического [1]. Дополнительный канал образуется между двумя мобильными устройствами при личной встрече их пользователей. В работе проведен сравнительный анализ этих способов.

Маккьюном М. [2] был предложен подход к сопряжению двух устройств на основе *визуального канала* связи, получивший название “Seeing-is-Believing” (SiB). SiB предполагает, что устройство ***A*** формирует двухмерный штрих-код, являющийся графическим аналогом хэш-функции ключевой информации, переданной устройству ***B*** [3]. Устройство ***B***, для проверки подлинности ***A***, считывает штрих-код при помощи фотокамеры и сравнивает значение хэш-функции с хэш-функцией, вычисленной из полученной ранее ключевой информации. В случае совпадения хэш-кодов ключ считается подлинным (рис. 1).

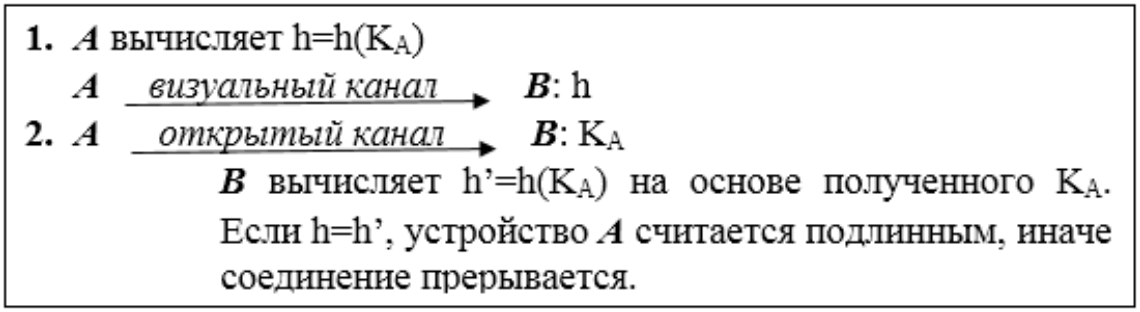


Рис. 1. Однонаправленная аутентификация SiB (B аутентифицирует A)

Для выполнения взаимной аутентификации предложен метод VisualauthenticationbasedonIntegrityChecking (VIC), в котором каждому устройству, исходя из публичных данных, требуется вычислить общую хэш-функцию (рис. 2).

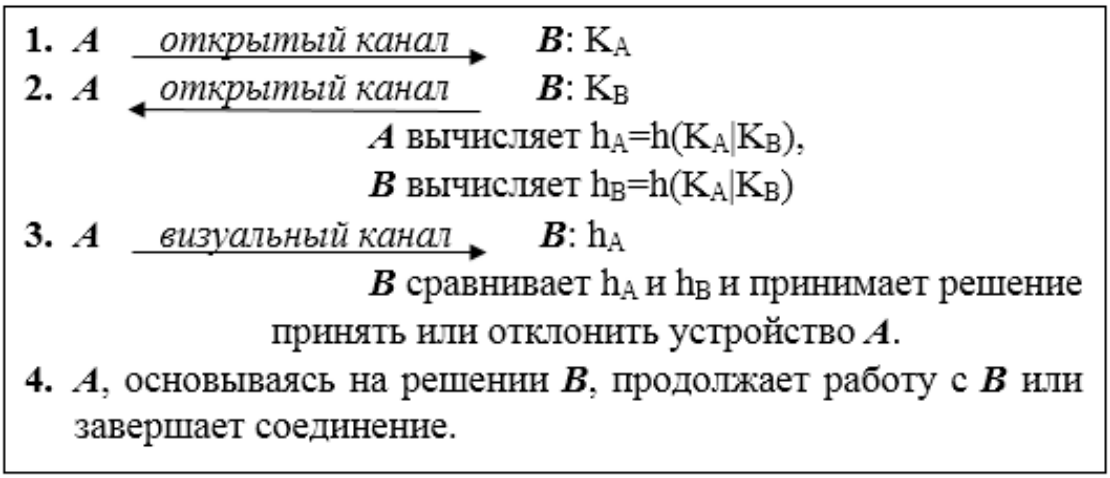


Рис. 2. Взаимная аутентификация VIC

Сопряжение устройств с использованием *акустического канала* связи предполагает передачу звукового сигнала от динамика, расположенного на стороне источника, до микрофона, находящегося на приемной стороне.

В способе «Beep-Beep» [4] динамик передает ключевую информацию при помощи прерывистого звукового сигнала. Принимающая сторона декодирует полученное сообщение (длинный гудок представляет собой «1», короткий – «0») и сравнивает полученные по акустическому и открытому каналам данные и принимает решение продолжить или прервать работу между устройствами.

Наряду со способом «Beep-Beep» для сопряжения устройств так же используют метод «Loud-and-Clear»(L&C) [5], позволяющий преобразовывать символьную строку в голосовой поток. Система L&Cв работе использует библиотеку Madlib, содержащую список всех возможных для передачи символов и соответствующие каждому символу слова различных типов, такие как: существительные, прилагательные, наречия, глаголы и др. Каждый передаваемый по акустическому каналу символ должен быть заменен на запись соответствующего слова из библиотеки. Метод L&C предполагает, что для аутентификации с использованием акустического канала связи устройство ***A*,** вычислив хэш-функцию переданной ранее ключевой информации, преобразует ее значение в последовательность слов, основываясь на библиотеке Madlib, и передает полученное предложение устройству ***B***. Устройство ***B*** декодирует полученное сообщение и сравнивает его со значением хэш-функции, вычисленной из полученной ранее от пользователя ***A*** ключевой информации. В случае совпадения значений устройство***A*** считается подлинным (рис. 3).

1. Пользователи ***A*** и ***B*** согласуют общий секрет работы библиотеки Madlib
2. ***A*** —*открытый канал*→ ***B***: K_A
3. ***A*** вычисляет $h=h(K_A)$. Используя библиотеку Madlib, заменяет h на последовательность соответствующих слов H_A
4. ***A*** —*акустический канал*→ ***B***: H_A

   B вычисляет $h'=h(K_A)$ на основе полученного K_A, используя Madlib, преобразует полученную последовательность h' в H'_A, сравнивает H_A и H'_A. Если $H_A = H'_A$, ***A*** считается подлинным, иначе соединение прерывается.

Рис. 3. Однонаправленная аутентификация L&C (B аутентифицирует A)

В основе метода «Smart-ItsFriends» [6] лежит *вибрационный канал*. Предполагается, что для генерирования общего ключа аутентификации два мобильных устройства встряхиваются, удерживая их в одной руке. Данный

метод представляется возможным для устройств, содержащих в себе датчики акселерометра, позволяющие считать информацию о положении мобильного устройства в пространстве и преобразовать ее в цифровой код согласно формуле:

$$\vec{\mathrm{A}}(t) = \sqrt{(A_X(t))^2 + (A_Y(t))^2 + (A_Z(t))^2},$$

где $A_X(t)A_Y(t)$,$A_Z(t)$ – координаты мобильного устройства в определенный момент времени.

Соответственно, два устройства (***A*** и ***B***), которые трясли вместе, на выходе получат идентичные ключевые последовательности $A_{\mathrm{A}}(t)$ и $A_{\mathrm{B}}(t)$.

В [7] для сопряжения устройств предложено использовать способ MagPairing, основанный на дополнительном *магнитометрическом канале*. Для этого два мобильных устройства, необходимо удерживать вблизи друг друга несколько секунд без выполнения каких-либо дополнительных операций. Устройства считывают показания датчиков магнитометра и обмениваются ими. Данные датчиков используются для аутентификации ключей, сформированных по алгоритму Диффе-Хеллммана.

Магнитометрические данные, считанные с устройств ***A*** и ***B*** могут быть записаны как

$$B_A = T_{(Earth \to A)} B_{net},$$

$$B_B = T_{(Earth \to B)} B_{net},$$

где $T_{(Earth \to A)}$ и $T_{(Earth \to B)}$ – матрицы преобразования координат Земли в координаты устройств ***A*** и ***B***.

$$B_{net} = B_{Earth} + B_1 + B_2,$$

где B_{net} – магнитное поле Земли, B_1, B_2 – магнитные поля, создаваемые магнитами устройств ***A*** и ***B***.

На основе анализа приведенных выше методов сопряжения мобильных устройств была составлена сравнительная таблица (см. ниже). Каждый метод был оценен по трем характеристикам: требования к сопрягаемым устройствам, время, необходимое для их сопряжения, и вероятность ошибочной аутентификации устройств.

Из таблицы следует, что методы сопряжения, основанные на визуальном дополнительном канале, имеют самую низкую вероятность ошибки по сравнению с остальными методами, однако процесс аутентификации занимает больше времени, чем при использовании других дополнительных каналов. Недостатком методов, основанных на визуальном канале связи, также является то, что сопряжение устройств требует большого внимания пользователя и неприменимо для устройств, не оснащенных камерой [8]. Устройства, сопрягаемые при помощи акустического канала связи, должны

обладать динамиками и микрофонами. Так как данные методы восприимчивы к шуму окружающей среды, они показали высокий процент ошибочной аутентификации. Применение вибрационного канала связи для реализации процесса аутентификации требует наличия у мобильных устройств датчиков акселерометра. Сопряжение устройств с использованием данного метода с 90% вероятностью будет успешным и не займет много времени на реализацию. Недостатком вибрационного канала является необходимость выполнять пользователю встряхивания мобильных устройств в течение приблизительно 5 секунд. Сопряжение с использованием магнитометрического канала связи обеспечивает высокую скорость работы, низкую вероятность ошибочной аутентификации и позволяет минимизировать участие пользователя в процессе сопряжения устройств, что указывают на преимущество использования магнитометрического канала связи для аутентификации пользователей.

ТАБЛИЦА. Сравнительный анализ методов сопряжения мобильных устройств с использованием различных дополнительных каналов

Канал	Метод	Требования к устройствам		Среднее время сопряж.	Вероятн. ошибки
		Устройство А	Устройство В		
Визуальный	Seeing-is-Believing	Дисплей+ Камера	Дисплей+ Камера	26.9 с	5%
	VIC	Дисплей+ Камера	Дисплей+ Камера, Камера, Дисплей	17.0 с	5%
Акустический	Beep-Beep	Динамик+ Микрофон	Динамик+ Микрофон, Динамик, Микрофон	25.0 с	20%
	Loud-and-Clear	Динамик+ Микрофон	Динамик+ Микрофон	15.5.с	10%
Вибрационный	Smart-Its Friends	Акселерометр	Акселерометр	10.4	10%
Магнитометрический	MagPairing	Магнитометр	Магнитометр	4.5 с	7%

Список используемых источников

1. Gehrmann C. and Nyberg K. Security in personal area networks // Security for Mobility. 2004. PP. 191–230.

2. Saxena N. Secure device pairing based on a visual channel // IACR.2006.

3. McCune J. M. Seeing-is-believing: Using camera phonesfor human-verifiable authentication // IEEE Symposium onSecurity and Privacy. 2005.

4. Goodrich M. T., Sirivianos M., Solis J., Soriente C., Tsudik G., Uzun E. Using audio in secure device pairing. 2009. PP. 57–68.

5. Goodrich M. T., Sirivianos M., Solis J., Tsudik G., Uzun E. Loud and clear: Human-verifiableauthentication based on audio // IEEE ICDCS. 2006.

6. Holmquist L., Mattern F., Schiele B., Alahuhta P., Gellersen H.-W. Smart-its friends: A technique for users to easily establish connections between smart artefacts // Ubiquitous Computing, UbiComp. 2001. PP. 116–122.

7. Jin R., Shi L., Zeng K., Pande A., Mohapatra P., Mag Pairing: Pairing smartphones in close proximity using magnetometers // IEEE Transactions on information forensics and security. 2016. PP. 1304–1319.

8. Kumar A., Saxena N., Tsudik G., Uzun E., Caveat emptor: A comparative study of secure device pairing methods // IEEE International Conference on Pervasive Computing and Communications, PerCom. 2009.

УДК 004.75

ОСОБЕННОСТИ ФУНКЦИОНИРОВАНИЯ СОВРЕМЕННЫХ АВТОМАТИЗИРОВАННЫХ СИСТЕМ МОНИТОРИНГА ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ

В. Г. Иванов, Д. Д. Корякин

Военная академия связи имени Маршала Советского союза С. М. Буденного

Сегодня в условиях непрерывного развития и постоянного повышения сложности телекоммуникационных систем, обеспечение надежного функционирования инфокоммуникационных процессов и сервисов, позволяющих организовать эффективную работу пользователя, является важнейшей задачей администратора сети. Ввиду важности этого процесса необходим постоянный контроль за работой всей сети связи, которая включает в себя множество различного телекоммуникационного и серверного оборудования. Механизмы контроля нашли себя в автоматизированных системах мониторинга, использование которых позволяет в режиме реального времени отслеживать состояния доступности и производительности компонентов телекоммуникационной сети в независимости от архитектуры сети, анализировать и оптимизировать загрузку оборудования, а также прогнозировать возникновение чрезвычайных ситуаций и сигнализировать об обнаружении критических ошибок.

SNMP, мониторинг, агент.

Современные системы мониторинга основаны на запросных методах к компонентам сети. Специальные агенты собирают статистическую информацию о работе элементов сети и передают ее в центральную базу данных, после чего она обрабатывается модулями системы мониторинга. В состав системы мониторинга должны входить следующие компоненты: формиро-

вание отчетов, модуль управления SNMP, архив и консоль управления. Модуль формирования отчетов позволяет формировать из имеющихся накопленных статистических данных информацию для принятия управленческих решений. Модуль управления SNMP отвечает за сбор информации с агентов мониторинга и взаимодействие с системами управления. Архив позволяет упорядочить хранение статистической информации и организовать последующую работу с ней. Консоль управления реализует функции конфигурирования и управления системой. телекоммуникационных сетей делятся на активные и пассивные в зависимости от способа получения данных. Активные системы мониторинга посылают запросы к необходимым объектам наблюдения, получают и накапливают данные мониторинга. Наиболее популярным в системах данного типа является протокол SNMP (*Simple Network Management Protocol*). Широкое использование SNMP связана с тем, что его поддерживают производители различного сетевого оборудования и программного обеспечения. Пассивные системы обрабатывают и потоки трафика и собирают информацию о них без внедрения дополнительных пакетов в сеть [1]. Пассивные системы используются в биллинговых системах и системах анализа трафика.

На данный момент к системам удалённого мониторинга предъявляются следующие требования:

– мониторинг сетевых служб (SMTP, POP3, HTTP, NNTP, ICMP, SNMP);

– мониторинг состояния хостов (загрузка процессора, использование диска, системные логи) в большинстве сетевых операционных систем;

– поддержка удаленного мониторинга через шифрованные туннели SSH или SSL;

– веб-интерфейс для администрирования и настройки;

– простая архитектура модулей расширений (плагинов) позволяет, используя любой язык программирования по выбору (Shell, C++, Perl, Python, PHP, C# и другие), легко разрабатывать свои собственные способы проверки служб;

– параллельная проверка служб;

– распределенный мониторинг. Конфигурация младших узлов полностью контролируется старшими узлами, находящихся на более высоком уровне иерархии;

– отправка оповещений в случае возникновения проблем со службой или узлом (с помощью почты, пейджера, смс, или любым другим способом, определенным пользователем через модуль системы);

– возможность определять обработчики событий, произошедших со службами или узлами для проактивного разрешения проблем;

– возможность создавать карты сетей.

В основе любой системы управления сетью лежит элементарная схема взаимодействия агента с менеджером. На основе этой схемы могут быть построены системы практически любой сложности с большим количеством агентов и менеджеров разного типа.

Агент является посредником между управляемым ресурсом и основной управляющей программой-менеджером. Чтобы один и тот же менеджер мог управлять различными реальными ресурсами, создается некоторая модель управляемого ресурса, которая отражает только те характеристики ресурса, которые нужны для его контроля и управления. Например, модель маршрутизатора обычно включает такие характеристики, как количество портов, их тип, таблицу маршрутизации, количество кадров и пакетов протоколов канального, сетевого и транспортного уровней, прошедших через эти порты.

Менеджер получает от агента только те данные, которые описываются моделью ресурса. Агент же является некоторым экраном, освобождающим менеджера от ненужной информации о деталях реализации ресурса. Агент поставляет менеджеру обработанную и представленную в нормализованном виде информацию. На основе этой информации менеджер принимает решения по управлению, а также выполняет дальнейшее обобщение данных о состоянии управляемого ресурса, например, строит зависимость загрузки порта от времени.

Для получения требуемых данных от объекта, а также для выдачи на него управляющих воздействий агент взаимодействует с реальным ресурсом некоторым нестандартным способом. Когда агенты встраиваются в коммуникационное оборудование, то разработчик оборудования предусматривает точки и способы взаимодействия внутренних узлов устройства с агентом. При разработке агента для операционной системы разработчик агента пользуется теми интерфейсами, которые существуют в этой ОС, например, интерфейсами ядра, драйверов и приложений. Агент может снабжаться специальными датчиками для получения информации, например, датчиками релейных контактов или датчиками температуры.

Менеджер и агент должны располагать одной и той же моделью управляемого ресурса, иначе они не смогут понять друг друга. Однако в использовании этой модели агентом и менеджером имеется существенное различие. Агент наполняет модель управляемого ресурса текущими значениями характеристик данного ресурса, и в связи с этим модель агента называют базой данных управляющей информации – Management Information Base, MIB. Менеджер использует модель, чтобы знать о том, чем характеризуется ресурс, какие характеристики он может запросить у агента и какими параметрами можно управлять [2].

Главной причиной внедрения систем мониторинга является в увеличении количества сетевого оборудования и серверов, задействованных в инфраструктуре сети, увеличивается и количество проблем, требующих вмешательства и решения со стороны администратор.

Постоянный контроль работы локальной сети, составляющей основу любой корпоративной сети, необходим для поддержания ее в работоспособном состоянии. Контроль – это необходимый первый этап, который должен выполняться при управлении сетью. Ввиду важности этой функции ее часто отделяют от других функций систем управления и реализуют специальными средствами. Такое разделение функций контроля и управления полезно для больших и средних сетей, для которых установка интегрированной системы управления экономически целесообразна. Использование автономных средств контроля помогает администратору сети выявить проблемные участки и устройства сети, а их отключение или реконфигурацию он может выполнять в этом случае вручную.

Резюмируя, можно отметить, что мониторинг сетей является перспективным направлением развития ИТ-инфраструктуры и, несмотря на ряд проблем, возникающих при его внедрении, использование подобных решений обеспечит значительный рост эффективности использования аппаратного и программного обеспечения и снизит число критических сбоев в системах.

Список используемых источников

1. Новиков Ю. В., Кондратенко С. В. Локальные сети: архитектура, алгоритмы, проектирование. М. : Издательство ЭКОМ, 2001. 312 с.: ил.

2. Олифер В. Г., Олифер Н. А. Компьютерные сети. Принципы, технологии, протоколы. 3-е изд. СПб. : Питер, 2006. 958 с.: ил.

УДК 621.315

ОПРЕДЕЛЕНИЕ ЕМКОСТИ ВИТЫХ ПАР КАБЕЛЕЙ СКС

В. С. Иванов, О. Г. Патрик

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

В статье дается анализ различных методов расчета емкости витых пар кабелей СКС. Результаты расчета емкости сопоставляются с результатами измерений кабеля СКС типа UTP-4×2×0,5 категории 5е американской фирмы «Siemon».

структурированная кабельная система, неэкранированный кабель СКС, емкость витой пары.

Желание определить величину емкости симметричной цепи наиболее точным образом можно обнаружить у многих зарубежных и отечественных авторов, среди которых Ф. Люшен, М. Клейн, В. Н. Кулешов, Н. И. Миролюбов, А. В. Нетушил, К. М. Поливанов, Д. Л. Шарле и другие.

Сравнительно невысокая точность расчетов первоначальных формул была обусловлена тем, что в качестве изолирующего материала применялась кабельная бумага, которая в процессе изготовления кабелей подвергалась смятию. Это препятствовало точному определению геометрических размеров, изолированных жил и их местоположению в кабельном сердечнике.

Так, например, Ф. Люшен в расчетную формулу для парной скрутки ввел эмпирический, поправочный коэффициент α, равный 0,94:

$$C = \frac{\varepsilon_{r\ \text{экв}} \cdot 10^{-6}}{36 \cdot \ln(\alpha \cdot d_{\text{гр}} / d_0)}, \qquad (1)$$

где $\varepsilon_{r\ \text{экв}}$ – эквивалентное значение диэлектрической проницаемости изоляции токопроводящих жил, $d_{\text{гр}}$ – диаметр группы (пары), d_0 – диаметр неизолированной жилы.

У М. Клейна поправочный коэффициент равен 1,25:

$$C = \frac{0{,}0161 \cdot \varepsilon_{r\ \text{экв}} \cdot 10^{-6}}{\lg(1{,}25\frac{2d_1 - d_0}{d_0})} = \frac{\varepsilon_{r\,\text{экв}} \cdot 10^{-6}}{27\ln(1{,}25\frac{2d_1 - d_0}{d_0})},$$

где d_1 – диаметр изолированной жилы.

В отечественной практике наибольшее распространение получила формула, полученная В. Н. Кулешовым [1]:

$$C = æ\ \frac{\varepsilon_{r\,\text{экв}} \cdot 10^{-6}}{36\ln(\frac{2a}{d_0}\psi)}, \qquad (2)$$

где æ – коэффициент спиральности (скрутки), который учитывает реальную длину жил при скручивании жил в пару и в сердечник, по сравнению с длиной по кабелю; a – расстояние между центрами токопроводящих жил; ψ – поправочный коэффициент.

Эту формулу Кулешов получил, применяя метод зеркальных изображений проводников для кабеля, в котором в качестве экрана рассматривается решетчатый экран, образованный соседними токопроводящими жилами (рис. 1).

Поправочный коэффициент ψ для парной скрутки равен:

$$\psi = \frac{(d_{И} + d_1 - d_0)^2 - a^2}{(d_{И} + d_1 - d_0)^2 + d^2},$$

Чуть позже в отечественной литературе [2] появилась формула для расчета емкости между двумя проводниками (рис. 2), у которых электрические оси не совпадают с геометрическими:

$$C = \frac{2\pi\varepsilon_0}{\ln\left|\left(\eta_1 + \sqrt{\eta_1^2 - 1}\right)\left(\eta_2 + \sqrt{\eta_2^2 - 1}\right)\right|},$$

где $\eta_1 = x_1 / R_1$, $\eta_2 = x_2 / R_2$

При равенстве радиусов $R_1 = R_2 = R$ очевидно, что $x_1 = -x_2 = S/2R$ и значение емкости будет равно:

$$C = \frac{\pi\varepsilon_0}{\ln\left(\eta + \sqrt{\eta^2 - 1}\right)}, \qquad (3)$$

Аналогичная формула получена авторами [3, 4] при использовании метода конформных отображений (рис. 3).

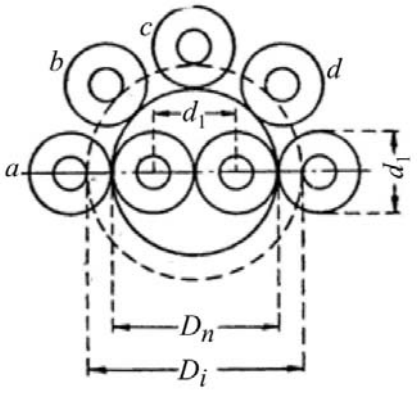


Рис. 1. Решетчатый экран, образованный соседними жилами

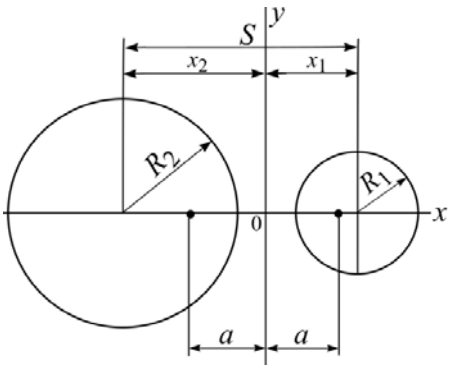


Рис. 2. Взаимное расположение проводников

$$C = \frac{2\pi\varepsilon_0}{\ln\left|\sqrt{h_1 / R_1^{\,2} - 1} + h_1 / R_1\right| \cdot \left|\sqrt{h_2 / R_2^{\,2} - 1} + h_2 / R_2\right|}, \qquad (4)$$

где $h_1 = 1/2D \cdot \left(D^2 + R_1^2 - R_2^2\right)$, $h_2 = 1/2D \cdot \left(D^2 + R_2^2 - R_1^2\right)$, D – расстояние между центрами проводников. При равенстве радиусов проводников формула (4) превращается в формулу (3).

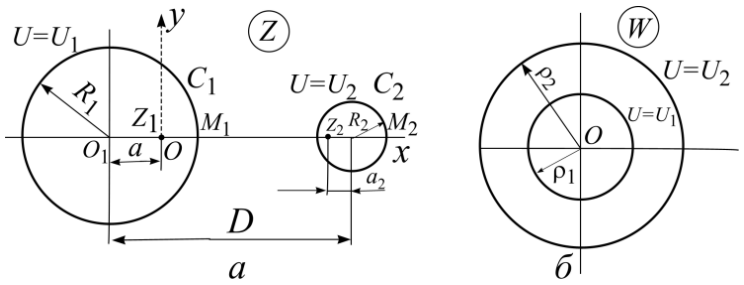


Рис. 3. Конформное отображение проводников в плоскости *W*

Представляет интерес формула для расчета емкости между проводами ВЛС, приведенная в [5]:

$$C = \frac{\pi\varepsilon_0}{\ln\left(\frac{a-r}{r}\right)}.$$

Если в качестве среды распространения использовать комбинацию воздуха и полиэтилена, как это имеет место в кабелях СКС, и учесть скрутку, то, очевидно, величину емкости можно рассчитать по следующей формуле:

$$C = æ\ \frac{\varepsilon_{r\,экв}\cdot 10^{-6}}{36\ln(\frac{a-r}{r})}, \qquad (5)$$

Эквивалентное значение относительной диэлектрической проницаемости обычно оценивается в результате учета объемов, занимаемых диэлектриками, в данном случае – это полиэтилен и воздух :

$$\varepsilon_{r\,экв} = \frac{\varepsilon_{r\,пэ}\cdot V_{пэ} + \varepsilon_{r\,в}\cdot V_{в}}{V_{пэ} + V_{в}},$$

Соотношение объемов можно заменить соотношением площадей, так как оно не зависит от длины.

Все дальнейшие вычисления емкости сделаны с использованием конструктивных размеров 4-парного неэкранированного кабеля категории 5е американской фирмы «Siemon», у которого диаметр неизолированной жилы равен 0,51 мм, а диаметр изолированной жилы – 0,92 мм.

Диаметр сердечника, в котом токопроводящие жилы одних пар попадают в междужильное пространство других, будет равен :

$$D_c = d_{п\ эк.} \times 2{,}41 = f_п\ d_1\ 2{,}41 = 3{,}42\ мм$$

где $d_{п\ эк.}$ – эквивалентный диаметр пары; $f_п$ – коэффициент, определенный теоретически и подтвержденный экспериментально, для несминаемой полиэтиленоаой изоляции равен 1,55 [6].

Площадь, занимаемая полиэтиленом, равна:

$$S_{пэ} = 8\frac{\pi}{4}\left(d_1^2 - d_0^2\right) = 6{,}28,\left(0{,}92^2 - 0{,}51^2\right) = 3{,}68 мм^2$$

Площадь, занимаемая воздухом:

$$S_в = \frac{\pi D_c^2}{4} - 8\frac{\pi d_1^2}{4} = \frac{3{,}14}{4}\left(3{,}42^2 - 8\cdot 0{,}92^2\right) = 3{,}87 мм^2$$

Окончательно $\varepsilon_{r\,экв}$ равно:

$$\varepsilon_{r\,экв} = \frac{2{,}3\cdot 3{,}68 + 1{,}0\cdot 3{,}87}{3{,}68 + 3{,}87} = 1{,}63$$

Коэффициент скрутки æ определяется как результат произведения коэффициента скрутки токопроводящих жил в пару $æ_{пары}$ и коэффициента скрутки при скручивании в сердечник – $æ_{серд}$ [3].

$$æ_{пары} = \sqrt{1+\left(\pi d_1 / h\right)^2},$$

где h – шаг скрутки пары.

$$æ_{серд} = \sqrt{1+\left(\pi 2{,}41 / H\right)^2},$$

где H – шаг скрутки в сердечник, для кабеля ф. «Siemon» его среднее значение равно 65 мм.

В таблице 1 приведены значения шагов скрутки в пару.

ТАБЛИЦА 1. Значения шагов скрутки

Цветовой код пары	Шаг скрутки, мм
Синий	10,7
Коричневый	22,3
Зеленый	13,8
Оранжевый	19,3

Результаты расчета коэффициента скрутки приведены в таблице 2.

ТАБЛИЦА 2. Результат расчета коэффициента скрутки

Цветовой код пары	$æ_{пары}$	$æ_{серд}$	$æ_{рез}$
Синий	1,031	1,0068	1,038
Коричневый	1,012	1,0068	1,019
Зеленый	1,026	1,0068	1,033
Оранжевый	1,014	1,0068	1,021

В таблице 3 приведены рассчитанные и измеренные значения емкости, последние заимствованы из [7].

ТАБЛИЦА 3. рассчитанные и измеренные значения емкости

Цветовой код пары	Коэфф. скрутки, $æ_{рез}$	Расчет по формуле (1)	Расчет по формуле (2)	Расчет по формуле (3)	Расчет по формуле (5)	Измер. значения
Синий	1.038	48,63	49,67	39,34	49,04	49,35
Коричневый	1,019	47,74	48,76	38,36	48,14	47,66
Зеленый	1,033	48,40	49,43	39,15	48,80	49,52

Цветовой код пары	Коэфф. скрутки, $æ_{рез}$	Расчет по формуле (1)	Расчет по формуле (2)	Расчет по формуле (3)	Расчет по формуле (5)	Измер. значения
Оранжевый	1,021	47,83	48,86	38,70	48,23	47,32
среднее	1,028	48,15	49,18	39,01	48,55	48,46

Анализируя результаты, представленные в таблице 3, необходимо отметить, что наилучшее совпадение результатов расчета с результатами эксперимента дают расчеты по формулам (1 и 5).

Список используемых источников

1. Кулешов В. Н. Теория кабелей связи: учебник. М. : Государственное издательство литературы по вопросам связи и радио, 1950. 420 с.

2. Нетушил А. В., Поливанов К. М. Основы электротехники. Часть третья. Госэнергоиздат, 1956. 191 с.

3. Смородинов Д. А. Оценивание рабочей емкости и эквивалентной диэлектрической проницаемости витой пары кабеля связи // Молодой ученый. 2013. № 4.С. 27–33.

4. Миролюбов Н. Н., Костенко М. В., Левинштейн М. В., Тиходеев Н. Н. Методы расчета электростатических полей. М. : Высшая школа, 1963. 415 с.

5. Шиниберов П. Я., Курбатов Н. Д., Сергеева К. К. Линии связи. М. : Связьиздат, 1962. 432 с.

6. Брискер А. С., Руга А. Д., Шарле Д. Л. Городские телефонные кабели. М. : Радио и связь, 1991. 207 с.

7. Суровцева О. Ф. Исследование характеристик передачи и взаимного влияния симметричных кабелей структурированных кабельных систем : дис. ... канд. техн. наук : 05.12.13 / Суровцева Ольга Федоровна; С.-Петерб. гос. ун-т телекоммуникаций им. М. А. Бонч-Бруевича. СПб., 2007. 122 с. : ил.

УДК 004.73

АНАЛИЗ СОВРЕМЕННЫХ ТЕХНОЛОГИЙ ПОСТРОЕНИЯ МУЛЬТИСЕРВИСНЫХ СЕТЕЙ

О. Б. Ильина[1], О. П. Купчиненко[1], О. И. Пантюхин[1], А. В. Скоропад[2]

[1]Военная академия связи имени Маршала Советского Союза С. М. Буденного
[2]Ленинградское отделение научно-исследовательского института радио (ЛО НИИР)

Технологии ATM, TCP/IP, MPLS, в том числе IP MPLS, приобретают все большую популярность для построения мультисервисных сетей. При этом технологии IP MPLS находят предпочтительное применение на сверхскоростных магистральных сетях,

а АТМ – на сетях доступа, взаимодействуя между собой на различных уровнях эталонной модели взаимодействия открытых систем и обеспечивая требуемое качество обслуживания.

мультисервисные сети, магистральные сети, сети доступа, качество обслуживания.

В начале нынешнего века ведущими операторами связи многих стран мира, в том числе и России, начато строительство сетей связи с использованием технологии коммутации информационных потоков по меткам MPLS (*MyltiProtocol Label Switching* – мультипротокольная коммутация по меткам), в том числе одной из её разновидностей, а именно IP MPLS (*Internet Protocol* – межсетевой протокол). Она получила массовое признание как перспективное «транспортное средство» для магистральных сетей и обусловила дальнейшую конкуренцию между технологиями ATM (*Asynchronous Transfer Mode* – асинхронный способ передачи) и TCP/IP (*Transmission Control Protocol* – протокол управления передачей) [1, 2].

Технологии ATM и MPLS в современных сетях связи выполняют одинаковую функцию, а именно создание слоя второго уровня эталонной модели взаимодействия открытых систем (ЭМВОС) [3] с установлением виртуальных соединений. Необходимость такого промежуточный слоя объясняется тем, что протоколом IP, который отлично справляется с функциями объединения сетей различных технологий, не предусмотрено установление соединений. Поэтому он принципиально не может решать задачи предоставления гарантированного уровня качества обслуживания QoS (*Qualiti Of Servise* – качество сервиса или услуг) из-за размытости путей следования трафика через сеть и невозможности влияния на эти пути, выбор которых осуществляется протоколами маршрутизации в соответствии с наименьшей метрикой. Модернизация протокола IP до технологии виртуальных соединений MPLS дополняет базовые возможности IP, позволяя направлять трафик по рациональным маршрутам и создавая основу резервирования пропускной способности для пользовательских потоков данных.

Анализ и сравнение технологий ATM и MPLS можно произвести по масштабируемости и качеству обслуживания.

Из-за различной масштабируемости технологий предполагается, что место MPLS будет в магистральной (транспортной) сети, а ATM – в сети доступа. Таким образом, в перспективном варианте построения сетей связи для MPLS по отношению к ATM отводится то же место, что и ATM к FR (*Frame Relay* – ретрансляция кадров) в существующих сетях. В технологии ATM имеется несколько ограничений, из-за которых ее масштабируемость не может выходить за определенные рамки. Если в момент создания возможности базовых механизмов ATM казались «безграничными», то се-

годня они уже сдерживают рост сетей. Самым принципиальным ограничением является фиксированный и очень небольшой размер ячейки – 53 байта. Такой размер был выбран для создания предсказуемых условий переноса чувствительного к задержкам голосового трафика через магистрали со скоростью 155 Мбит/с. Однако за последние годы порядок скоростей изменился. В настоящее время многие технологии, например, Packet over SDH (*Synchronous Digital Hierarchy* – синхронная цифровая иерархия), работают уже на скорости 10 Гбит/с, т. е. в 64 раза быстрее, чем 155 Мбит/с. Это значит, что допустимо использовании кадров с полем данных в 64 раза больше, что подтверждается практикой работы высокоскоростных каналов STM-64 (*Synchronous Transport Module of level* 64 – синхронный транспортный модуль 64-го уровня) в Internet, где применяются кадры с максимальным полем данных в 4500 байт.

Затраты вычислительной мощности любого пакетного коммутатора, независимо от поддерживаемой им технологии, пропорциональны количеству обрабатываемых пакетов (кадров, ячеек, «меток»), а не их размеру, поэтому коммутатору ATM приходится выполнять примерно в 100 раз большую работу, чем маршрутизатору IP, работающему с кадром размером в 4500 байт. При этом разница в скорости продвижения вследствие различий в размере ячеек и кадров не превышает наносекундных величин и не ощущается пользователями сети.

Одним из достоинств технологии MPLS по сравнению с ATM является ее способность использовать практически любой формат кадров существующих технологий второго уровня – ATM, FR, PPP (*Point-to-Point Protocol* – протокол «точка–точка»), Ethernet или любой иной, который может появиться в перспективе. Поэтому она имеет несколько разновидностей: ATM–MPLS, FR–MPLS, P–MPLS и E–MPLS, использующих соответственно ячейки ATM, кадры FR, пакеты PPP или Ethernet. Протокольная независимость IP MPLS обеспечивает ей высокую степень гибкости и масштабируемости, необходимую при работе на магистральной сети. Таким образом, стоимость переноса одного и того же объема данных с равной скоростью по магистрали MPLS и магистрали ATM всегда различна. Относительно меньшие затраты вычислительной мощности приводят к тому, что магистраль MPLS оказывается экономичней.

Масштабируемость означает также поддержку большого количества пользовательских потоков. Экономичность подразумевает возможность передачи через магистраль многочисленных потоков без необходимости слежения за каждым из них, т. е. агрегированно. При этом механизмы агрегирования MPLS более гибки и могут быть автоматизированы. Если коммутатор ATM «не видит» ничего, кроме информации своего второго уровня, т. е. номера виртуального соединения/пути (VCI/VPI), то коммутирующий

маршрутизатор MPLS, называемый LSR (*Label Switching Router* – маршрутизатор, коммутирующий пакеты по меткам), имеет доступ к информации как того же второго уровня, и кроме того, так и третьего (IP-адреса), и четвертого (порты TCP/UDP), а часто и прикладного уровня. Следовательно, администратор может написать несколько правил агрегирования с учетом разных признаков трафика, в том числе и высокоуровневых, и предоставить дальнейшую работу LSR. Еще одним хорошим «масштабируемым» свойством MPLS является неограниченное число уровней иерархии меток и, соответственно, агрегирования путей, вместо двух уровней ATM.

Сеть с технологией ATM может контролировать параметры QoS «из конца в конец» для каждого отдельного виртуального соединения, обеспечивая высокую степень выполнения соглашений об уровне сервиса. Неспособность MPLS поддерживать QoS подобным образом является пока ее уязвимым местом и главной причиной сохранения ATM на магистрали. Но поддержка QoS не встроена жестко в MPLS. Исходя из этого, сетевым интеграторам предоставляется возможность применять те из имеющихся механизмов QoS, которые лучше всего отвечают потребностям сети.

Одним из таких механизмов является дифференциальное обслуживание разнотипного трафика (*DiffServ*). Механизм разработан для сетей IP и ориентирован на работу с несколькими агрегированными классами трафика, а не отдельными пользовательскими соединениями, как в ATM. Именно такая технология подходит для работы на магистральной сети. В качестве альтернативного механизма может использоваться объединение техники инжиниринга трафика MPLS с DiffServ. Этот механизм получил название «DiffServ Aware Traffic Engineering». Он предусматривает прокладку в сети IP MPLS агрегированных путей LSP (*Label Switching Pass* – путь при коммутации по метке) двух типов – для чувствительного к задержкам трафика и для остального. В результате весь пользовательский трафик сводится всего к двум классам, так что вместо информации о параметрах QoS тысяч виртуальных соединений (подход ATM), устройствам LSR достаточно запоминать параметры только двух LSP по каждому интерфейсу. Такое существенное сокращение обеспечивает высокую масштабируемость решения и сохраняет поддержку QoS. Но при данном подходе к соблюдению QoS пользователь может оказаться в ситуации, когда при получении сервиса IP MPLS неизвестно, как его реализовал оператор, каким образом он поддерживает соблюдение параметров QoS и обеспечивает ли вообще.

С ATM таких проблем нет. У всех производителей QoS реализуется примерно однотипно в соответствии со стандартами. Более того, ATM дает пользователю возможность проконтролировать качество виртуального соединения, а для MPLS такого рода стандартные средства отсутствуют. Что же касается отсутствия в MPLS ATM-подобных механизмов раздельной

поддержки QoS, существует парадоксальное мнение разработчиков, что для работы на высокоскоростной магистрали они и вовсе не нужны.

Все сказанное справедливо только для высокоскоростных трактов. Если рассматривать магистральные сети с трактами до 155 Мбит/с, то ситуация изменяется, и ATM в данном случае выглядит предпочтительнее. Для управления трафиком на низкоскоростных каналах механизмы поддержки QoS в MPLS подходят плохо. Здесь как раз нужны тонкие методы обслуживания очередей ATM, поскольку они обеспечивают соблюдение параметров QoS для каждого виртуального соединения в отдельности. Только в этом случае оператор может гарантировать клиентам, что обещанные в SLA средние скорости трафика, пульсации и уровни задержек будут соблюдены.

Исходя из проведенного анализа можно сделать вывод, что в будущем применение MPLS на сверхскоростной магистрали более перспективный вариант, чем ATM. При этом за ATM остаются сети доступа, где его применение вполне обоснованно.

При внедрении этой архитектуры возникает проблема взаимодействия сетей доступа ATM с магистралью IP MPLS. Сегодня существует два подхода к обеспечению такого взаимодействия – на третьем и втором уровнях ЭМВОС.

Вариант взаимодействия на третьем уровне известен под названием MPLS VPN (*Virtual Private Network* – виртуальные частные сети) третьего уровня. При этом в сети доступа в качестве технологии второго уровня может использоваться ATM, а поверх нее работает протокол IP со своей адресацией. В случае, если в сети доступа используются другие технологии второго уровня (*Ethernet*, FR), их адресная информация также отбрасывается при поступлении в магистраль и не учитывается при прохождении через нее.

Сеть доступа может взаимодействовать с магистралью IP MPLS и на втором уровне. При этом протоколы третьего уровня, например, IP, вообще не участвуют во взаимодействии. Поэтому при организации взаимодействия на третьем уровне такой трафик нужно обязательно инкапсулировать в пакеты IP, что приводит к большим накладным расходам, а в данном варианте он инкапсулируется непосредственно в кадры или ячейки второго уровня, что, соответственно, уменьшает затраты.

Если в сети доступа применяется ATM, то виртуальное соединение не заканчивается на входном устройстве магистрали, а прозрачным образом проходит через туннель MPLS и продолжается на выходе из магистрали в сеть доступа со стороны узла назначения.

Описанные схемы взаимодействия ATM и MPLS дополняют друг друга. Их совместное применение позволяет передавать через магистраль MPLS любой трафик, как IP, так и отличный от него.

Одновременная поддержка в магистральных коммутаторах ATM и IP MPLS дает возможность операторам реализовать еще одну схему их взаимодействия – смешанную. Собственно, это даже не схема, а стратегия постепенной миграции магистрали ATM к магистрали IP MPLS. По мере установки в сеть ATM все большего количества коммутаторов нового поколения с поддержкой, в том числе и MPLS, оператор сможет увеличить и количество путей LSP между пограничными устройствами, не отказываясь в то же время от уже работающих виртуальных соединений ATM. При этом производители таких коммутаторов рекомендуют операторам начать с перевода на MPLS не требовательного к качеству обслуживания трафика, для которого оператор не обязан гарантировать пользователям каких-либо количественных характеристик QoS. И только накопив опыт работы с MPLS, следует обратиться к переводу на пути LSP других классов трафика, в том числе и чувствительных к задержкам, передающихся сегодня с помощью соответствующих служб ATM.

Таким образом, модернизация протокола IP до технологии виртуальных соединений MPLS позволяет создавать современные мультисервисные сети.

Список используемых источников

1. Олифер В. Г., Олифер Н. А. Компьютерные сети. Принципы, технологии, протоколы: учебник для вузов. 3-е изд. СПб. : Питер, 2006. 958 с.

2. Таненбаум Э. Компьютерные сети. 4-е изд. СПб. : Питер, 2003. 992 с.

3. Крукк Б. И., Попантонопуло В. Н., Шувалов В. П. Телекоммуникационные системы и сети: учебное пособие. В 3-х томах. Том 1. Современные технологии / под ред. профессора Шувалова В. П. Изд. 3-е, испр. и доп. М. : Горячая линия-Телеком, 2003. 647 с.

УДК 371.39

ИСПОЛЬЗОВАНИЕ МОДЕЛИ РАША ДЛЯ ОЦЕНКИ КАЧЕСТВА ЗНАНИЙ ОБУЧАЕМЫХ

О. Б. Ильина[1], О. П. Купчиненко[1], О. И. Пантюхин[1], А. В. Скоропад[2]

[1]Военная академия связи имени Маршала Советского Союза С. М. Буденного
[2]Ленинградское отделение научно-исследовательского института радио (ЛО НИИР)

Одной из основных технологий проверки качества в образовании является тестирование. В настоящее время наиболее часто используются статистические методы тестирования. В статье исследуется применение однопараметрической модели Раша

для оценки эффективности тестов, показывается использование данной модели для различных вариантов тестовых заданий.

однопараметрическая модель, тестирование, трудность задания, уровень подготовленности.

Согласно государственной программе Российской Федерации «Развитие образования» на 2013–2020 гг. одной из ключевых приоритетных задач является обеспечение государственных гарантий – доступности и равных возможностей получения полноценного образования, достижение нового, современного качества профессионального образования. Основные усилия по реализации программы сегодня сосредоточены на увеличении роли информационных технологий.

На сегодняшний день основной технологией проверки качества в образовании является тестирование. Тестирование, как средство обучения и контроля знаний, в образовательных процессах используется давно. Однако в последнее десятилетие наблюдается явный рост популярности тестовых проверок при оценке качества знаний, что связано с информатизацией образовательных технологий и повсеместной компьютерной обеспеченностью учебного процесса.

Тестирование имеет ряд преимуществ по сравнению с классическими формами проверки качества знаний. Это возможность автоматизировать процесс тестирования с помощью персональных компьютеров, что влечет удобство использования тестовых материалов, снижение трудоемкости, исключение ошибок при проверке, объективность оценивания, широкий спектр тестовых заданий по сравнению с классическими узкими экзаменационными вопросами. Существенно повышает информативность контроля знаний адаптивное тестирование [1].

Многообразие тестов, используемых в различных методиках преподавания, ставит вопрос об их эффективности, т. е. адекватности теста уровню обучаемого, эффективности его использования и т. п.

В последнее время роль статистических методов тестирования неуклонно возрастает. Значительную популярность среди них приобрел метод однопараметрической модели Раша, названный в честь датского математика Георга Раша.

Статистическая обработка результатов тестирования на основе модели Раша обладает важными достоинствами, среди которых необходимо отметить следующие.

Модель Раша превращает измерения, сделанные в дихотомических (т. е. имеющих только два возможных значения) и порядковых шкалах, в линейные измерения. В результате качественные данные анализируются с помощью количественных методов. Это позволяет использовать широкий спектр статистических процедур.

Оценка трудности тестовых заданий не зависит от выборки испытуемых, на которых она была получена. Оценка уровня знаний испытуемых так же не зависит от используемого набора тестовых заданий. Пропуск данных для некоторых комбинаций (испытуемый – тестовое задание) не является критическим. Кроме того, модель Раша характеризуется наименьшим числом параметров: один параметр уровня знаний для каждого испытуемого и только один параметр трудности для каждого задания [2].

Модель Раша опирается на понятия «трудность задания» и «уровень подготовленности». Так, одно задание считается более трудным, чем другое, если вероятность правильного ответа на первое задание меньше, чем на второе, независимо от того, кто их выполняет. Аналогично, более подготовленный обучающийся имеет большую вероятность правильно ответить на все задания, чем менее подготовленный.

Благодаря простой структуре модели существуют удобные вычислительные процедуры для проверки адекватности модели для всего набора тестовых результатов, для каждого испытуемого, для каждого задания и для каждого конкретного ответа.

Модель применяется для анализа дихотомических переменных, что как нельзя лучше подходит к тестам, в которых можно обозначить правильный ответ на вопрос как 1, а неправильный – как 0.

После проведения теста можно составить матрицу, в строчках которой были бы испытуемые, в столбцах – вопросы теста, а на их пересечении – баллы (1 или 0), полученные испытуемым за ответ на тот или иной вопрос. Подобная матрица не зависит ни от числа вопросов в тесте, ни от количества обучаемых, что делает первоначальное применение модели практически универсальным и в высшей степени нетрудоемким. Первичный балл испытуемого получается в результате подсчета числа правильных ответов (т. е. суммы баллов в каждой строке). Первичный балл задания можно получить, суммируя в столбцах число правильных ответов на задание всеми испытуемыми. Чем больше правильных ответов на задание, тем легче оно оказывается для данной группы испытуемых. Если разделить полученный первичный балл задания на общее число заданий, то можно перейти к вероятности правильных p и вероятности неправильных q ответов [3].

Рассмотрим применение модели Раша на конкретном примере. Пусть тест состоит из K различных заданий бинарного типа (испытуемый получает 1, если ответил правильно, и 0 при неверном ответе) и его выполняют N обучающихся. В результате получается матрица ответов $A_{n,k}$, состоящая из N_i строк и K_j столбцов:

$$A_{n,k} = (a_{ij}).$$

Число b_i, равное сумме баллов в i-ой строке, называется первичным баллом i-го испытуемого и равно числу правильных ответов:

$$b_i = \sum_{j=1}^{k} a_{ij}.$$

Уровни подготовленности участников *A* и *B* обозначим через S_A и S_B, а трудность заданий – через *t* (на самом деле все задания имеют разный уровень трудности t_k). В модели Раша соотношение уровней подготовленности участников имеет следующий вид:

$$\frac{S_A}{S_B} = \frac{p_{At}\, q_{Bt}}{q_{At}\, p_{Bt}}, \quad (1)$$

$$q_{At} = 1 - p_{At}, \quad q_{Bt} = 1 - p_{Bt},$$

где p_{At} и p_{Bt} – вероятность выполнения задания уровня трудности *t* соответственно участниками *A* и *B*, q_{At} и q_{Bt} – вероятности невыполнения задания уровня трудности *t* соответственно участниками *A* и *B*.

Анализ выражения (1) показывает, что оно верно для любого уровня трудности заданий и любой пары участников тестирования. Пусть какое-либо задание имеет трудность *t* = 1 и необходимо сравнить трудности двух заданий. В модели Раша уровень трудности определяется как отношение вероятности q_{1t} того, что некоторый стандартный участник испытания с единичным уровнем подготовки *S* = 1 не выполнит данное задание к вероятности p_{1t} его выполнения:

$$t = \frac{1-p_{1t}}{p_{1t}}.$$

Единичный уровень подготовки и единичная трудность задания в модели Раша связаны между собой. Используя выражение:

$$\frac{S_A}{S_B} = \frac{p_{A1}\, q_{B1}}{q_{A1}\, p_{B1}} = \frac{p_{A1}}{(1-p_{A1})} \times \frac{(1-p_{B1})}{p_{B1}}$$

и, предположив, что уровень подготовленности участника *B* является единичным $S_B = 1$, получим следующее выражение:

$$S_A = \frac{p_{At}\, q_{1t}}{q_{At}\, p_{1t}} = \frac{p_{At}}{(1-p_{At})} \times \frac{(1-p_{1t})}{p_{1t}} = \frac{p_{At}}{(1-p_{At})} \times t. \quad (2)$$

Уравнение (2) связывает уровень трудности некоторого задания и уровень подготовленности некоторого участника с вероятностью правильного выполнения задания и справедливо для заданий любого уровня трудности. Анализ уравнения (2) показывает, что вероятность *P*(*S, t*) того, что участник с уровнем подготовки *S* правильно выполнит задание трудности *t*, выражается следующей формулой:

$$P(S,t) = \frac{S}{S+t} = \frac{1}{1+\frac{t}{S}}. \quad (3)$$

Вероятность $P(S, t)$ называется функцией успеха. Из выражения (3) видно, что функция успеха зависит только от отношения t к S. Поэтому модель Раша называется однопараметрической и использует шкалу отношений.

После определения новых переменных:

$$\ln S = \theta, \qquad S = \exp(\theta),$$

$$\ln t = \delta, \qquad t = \exp(\delta),$$

выражение (3) можно переписать в виде:

$$P(\delta, \theta) = \frac{1}{1+\exp(\delta-\theta)}. \qquad (4)$$

Формула (4) является основным уравнением однопараметрической логистической модели Раша. Единица измерения δ и θ называется логитом. При одном логите ($\delta_0 = 1$ и $\theta_0 = 1$) вероятность успеха $P(\delta, \theta) = 0{,}5$, т. е. вероятность выполнения стандартного задания стандартным участником должна быть равна 0,5 (рис.).

Модель Раша позволяет сделать один очень важный вывод: чем выше уровень подготовки участника, тем больше вероятность выполнения задания любого уровня трудности. Параметры δ и θ называют латентными параметрами, т. к. они не измеряются непосредственно в процессе тестирования.

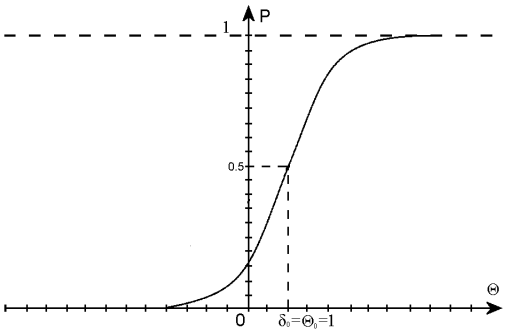


Рисунок. Характеристическая кривая трудности задания

Таким образом, достоинством модели Раша является ее аддитивность, т. е. вероятность успеха зависит только от разницы между уровнем подготовленности и трудностью задания. Вместе с тем модель Раша требует наиболее тщательного подбора заданий, т. к. накладывает жесткие ограничения на форму характеристических кривых.

Список используемых источников

1. Авраменко В. С., Купчиненко О. П., Пантюхин О. И. Адаптивное тестирование при автоматизации контроля знаний // Актуальные проблемы инфотелекоммуникаций в науке и образовании. V международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 3 т.; Т. 2. / под ред. С. В. Бачевского. СПб.: СПбГУТ, 2016. С. 213–217.

2. Челышкова М. Б. Теория и практика конструирования педагогических тестов: учебное пособие. М. : Логос, 2002. 432 с.

3. Гмурман В. Е. Теория вероятностей и математическая статистика. М. : Высшая школа, 1997. 359 с.

УДК 004.056

РАЗВЕРТЫВАНИЕ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА НА ОС ASTRA LINUX ДЛЯ ОБЕСПЕЧЕНИЯ ПОДДЕРЖКИ PKI

А. С. Исаков, М. М. Ковцур

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

В настоящие время распространено использование операционных систем семейства Windows для обеспечения поддержки Инфраструктуры Открытых Ключей в аккредитованных Удостоверяющих Центрах 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 описаны недостаточно в современной литературе. В данной статье описывается развёртывание УЦ на базе ОС Astra Linux.

инфраструктура открытых ключей, удостоверяющий центр, сертификат, astra linux.

Основной вопрос, связанный с использованием средств электронной цифровой подписи, к которым предъявляются требования по высокой отказоустойчивости, заключается в повышенных мерах обеспечения информационной безопасности при обращении 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 развертывания удостоверяющих центров (УЦ) в среде именно Astra Linux.

Для реализации этой задачи необходимо развернуть удостоверяющий центр на Astra Linux для обеспечения поддержки Инфраструктуры Открытых Ключей (рис. 1) [1, 2] по выдаче подписанных сертификатов.

Для развёртывания УЦ на базе ОС Astra Linux был сделан выбор в пользу УЦ на TinyCA. К особенностям развёртывания УЦ TinyCA на этой ОС можно отнести следующие:

- необходим смонтированный образ ОС [3];
- openssl v1.0.1k и выше;
- требуется защита каталога УЦ.

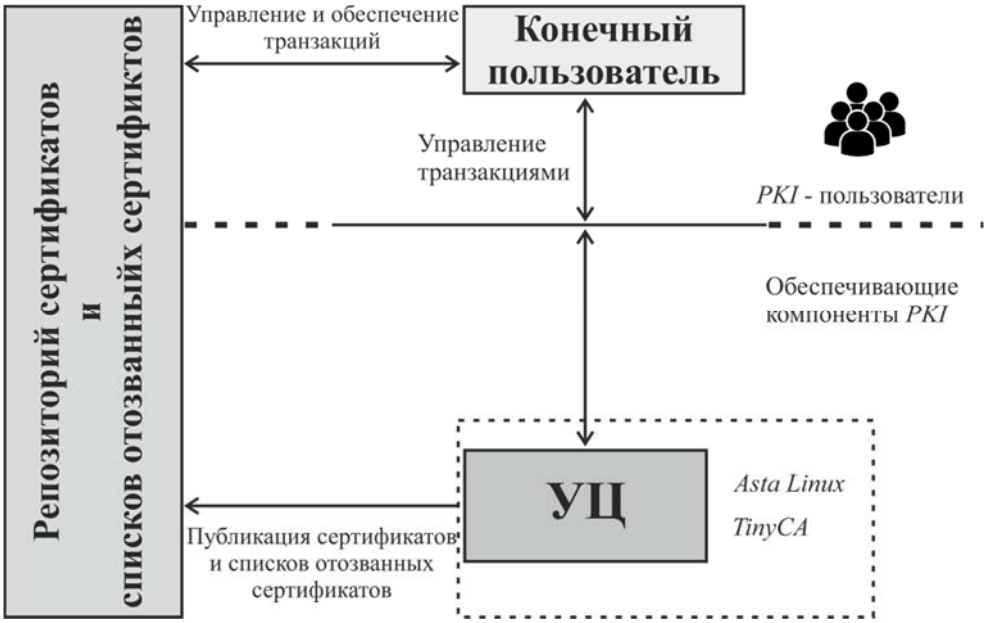


Рис. 1. Инфраструктура открытых ключей на базе ОС Astra Linux

TinyCA решает задачи управления сертификатами. Интерфейс TinyCA (рис. 2) обеспечивает расширенные функции по выпуску сертификатов, среди которых стоит отметить [4]:

– поддержка неограниченного количества УЦ: возможность работать с несколькими УЦ (выбор производится при открытии приложения или с помощью элемента интерфейса);

– возможность создания и управления иерархической древовидной структурой корневого и подчинённых УЦ;

– создание и аннулирование сертификатов в формате X.509, выпускаемых по шаблонам S/MIME, SSL Client, SSL Server;

– импорт и обработка запросов на выпуск сертификатов;

– экспорт сертификатов в форматы pem, der, pkcs # 12 и текстовый формат;

– интеграция в УЦ любых криптопровайдеров, имеющих стандартизованный программный интерфейс (в т. ч. соответствующих требованиям национальных стандартов на СКЗИ [5]).

Структура взаимодействия программных модулей и интерфейса ПО показана на рис. 3, она состоит из:

1. Графический интерфейс GUI.

2. Ядро скрипта обработки запросов и взаимодействия графического интерфейса ПО TinyCA с ПО OpenSSL – CA.pl.

3. Подключаемые компоненты ПО OpenSSL.

4. Конфигурационные файлы ПО TinyCA.

5. Файлы журнала регистрации событий работы УЦ.

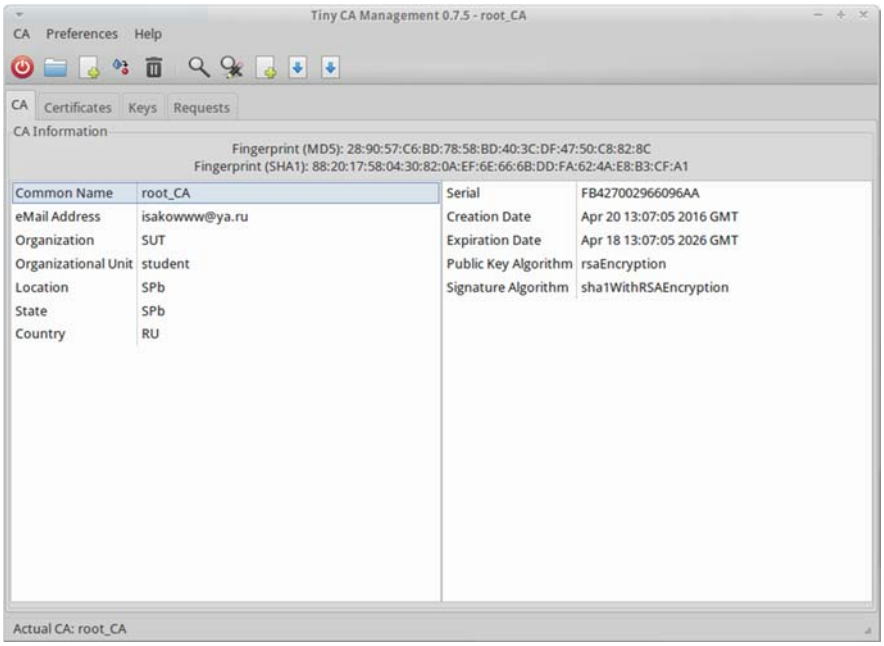


Рис. 2. Графический интерфейс TinyCA

Последовательность развертывания УЦ с использованием ПО TinyCA состоит из следующих действий:

1. установка и первоначальная настройка ПО TinyCA согласно эксплуатационной документации;

2. создание корневого УЦ путем выбора соответствующего пункта в интерфейсе TinyCA и настройки полей его сертификата. При этом УЦ выпускает свой самоподписанный сертификат, после чего УЦ считается развёрнутым.

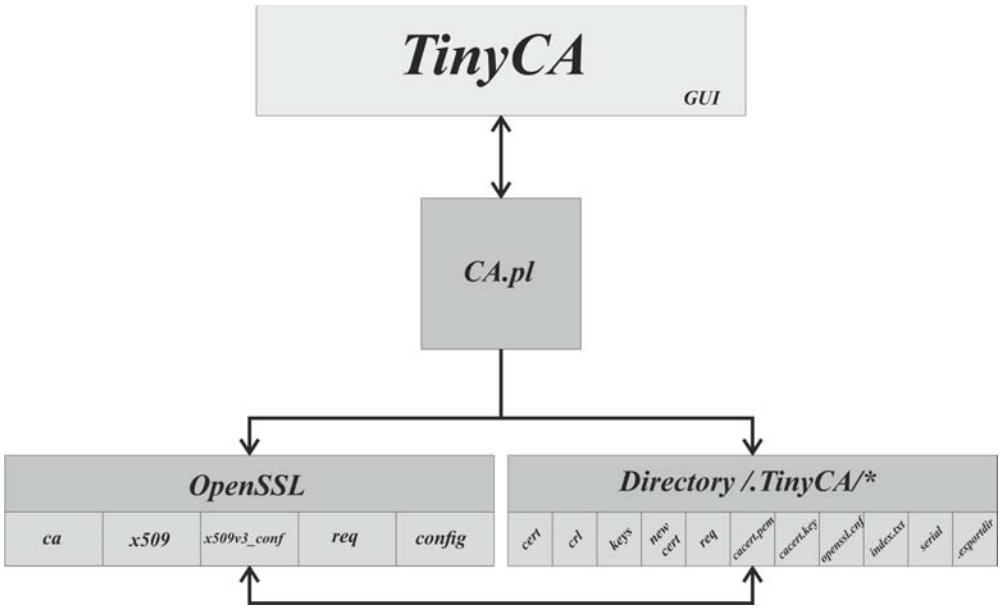


Рис. 3. Структура взаимодействия программных модулей и интерфейса ПО

Для выпуска сертификата пользователя необходимо создать запрос с помощью утилиты certmgr.msc Windows и экспортировать его на съемный носитель для дальнейшей его передачи и импорта в TinyCA.

Для создания сертификата открытого ключа в TinyCA необходимо импортировать ранее выполненный запрос сертификата, на основе которого будет выпущен сертификат открытого ключа пользователя, сформировавшего запрос в УЦ TinyCA. После выпуска сертификата пользователя он импортируется в хранилище сертификатов ОС Windows.

Как видно из рис. 4, выпущенный сертификат был сформирован путем подписания на секретном ключе УЦ TinyCA пользовательского запроса в соответствии с требованиями стандарта X.509 [6].

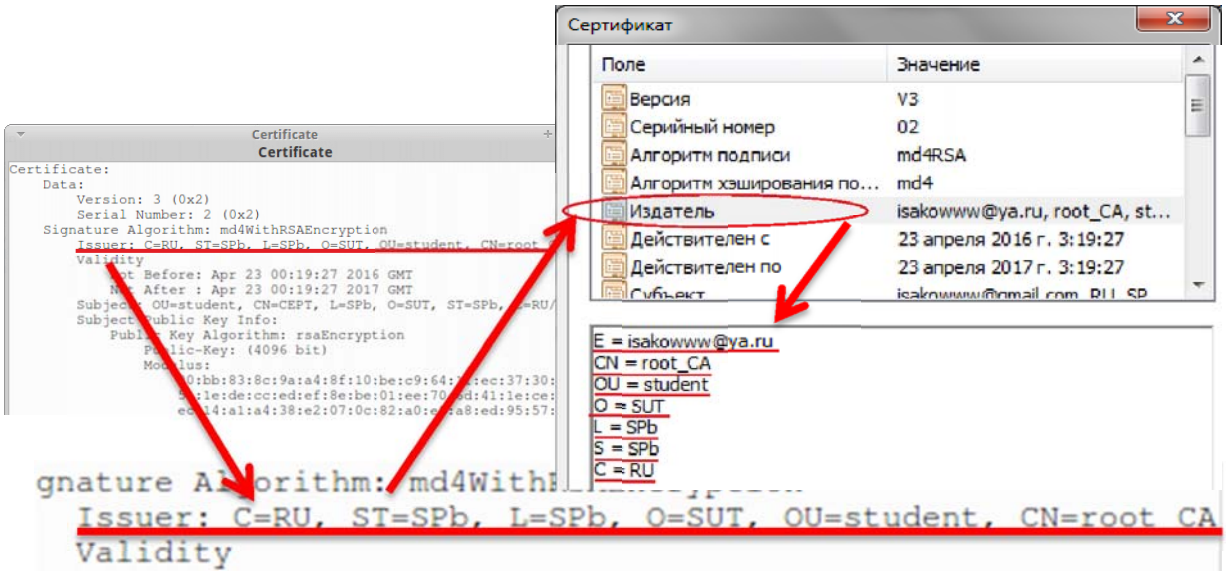


Рис. 4. Демонстрация подписанного сертификата в TinyCA и в certmgr Windows

В заключение стоит отметить, что TinyCA позволяет выпускать сертификаты, соответствующие стандарту X.509, открытые ключи, ЭЦП [7], обрабатывать запросы на сертификаты, формировать базы открытых ключей и списки отозванных сертификатов, что соответствует большинству задач, выполняемых на Windows УЦ.

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. Официальный сайт AstraLinux [Электронный ресурс]. Режим доступа: // http://astra-linux.ru/ (дата обращения: 10.12.2016).

4. Stephan Martin TinyCA – OpenSSL Front end [Электронный ресурс]. Режим доступа: // http://tinyca.sm-zone.net/ (дата обращения: 10.12.2016).

5. Ковцур М. М., Павлюкович М. В. Методика организации аккредитованного удостоверяющего центра // Актуальные проблемы инфотелекоммуникаций в науке и образовании. V международная научно-техническая и научно-методическая конференция: сб. науч. ст. СПб. : СПбГУТ, 2016. С. 417–421.

6. Recommendation ITU-T X.509 | ISO/IEC 9594-8 defines frameworks for public-key certificates and attribute certificates.

7. Небаева К. А., Чумаченко С. А. Роль электронных цифровых подписей в электронном документообороте // Актуальные проблемы инфотелекоммуникаций в науке и образовании. IV Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 2 томах. СПб : СПбГУТ, 2015. Т. 1. С. 377–379.

УДК 004.056.55

ВАРИАЦИОННОЕ ШИФРОВАНИЕ НА ОСНОВЕ КРИПТОГРАММЫ ТАМАН ШУД

Д. Е. Каблуков

Всероссийский научно-исследовательский институт радиоаппаратуры

В данной статье рассмотрен вариант расшифровки криптографической загадки, связанной с убийством неизвестного – Таман Шуд. Проанализировано частотное упоминание букв в зашифрованном тексте и предложен вариант развития событий, а также доказательства и возможный убийца. На основе данных расшифровки предложен алгоритм вариационного кодирования – нового вида создания высокостойких текстов для использования в передаче сообщений.

шифрование, криптография, защита информации.

Историческая справка

1 декабря 1948 года, тело человека было найдено на пляже в Австралии. Он был одет в костюм с намеренно отрезанными этикетками. Этот факт предполагает, что кто-то пытался скрыть свою личность. Ранние попытки определить, кем он был, не увенчались успехом. Полиции удалось придумать несколько возможных теорий, каждая из которых в конечном итоге была опровергнута.

Летом 1949 г., инспекторы обнаружили скрытый карман внутри штанов мужчины. В кармане был кусок бумаги, который гласит: "Tamam Shud", что означает «окончание» на персидском языке.

На сегодняшний день личность загадочного человека остается неизвестной. Даже причина смерти не определена. Исследователи до сих не

оставляют попытки взломать его. На самом деле, новое исследование определило одну вещь, которая почти наверняка верна: таинственный человек был отцом (незаконнорождённого) сына Неназванной медсестры [1, 2].

Расшифровка

Код (рис. 1) подвергается некоторой интерпретации. Совершенно очевидно, что есть строка текста, который была зачёркнута. Есть также несколько неоднозначных букв, которые описываются следующим образом:

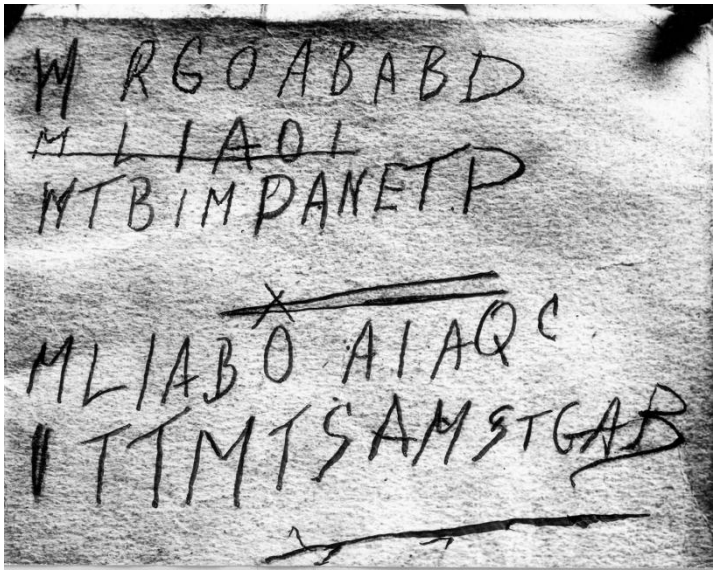


Рис 1. Изображение найденного шифра

Первая буква первой и второй линий (не считая перечёркнутую линию) выглядит так, как будто это может быть либо *M* или *W*.

Существует крест на вершине O (это может указывать на ошибку, и, следовательно, обесценить характер).

Третий по последнему письму выглядит как G, но может быть C, как горизонтальная линия, которая является частью следующего символа. Пятая буква последней строки выглядит как S, но с линией, проходящей через середину. Это не согласуется с другой S.

Каждая из этих односимвольных неясностей представлена погрешностями на графике (рис. 2) распределения частотности (для S с линией, проходящей через него за исключением случаев, у нас нет никакой альтернативной теории о том, что персонаж). Как вы можете видеть в частотном участке ниже, неоднозначность первой буквы первой и второй линий (M или W) представлена зеленым, неоднозначность первой буквы в последней строке (I или V) представлена в желтый и неоднозначность третьего по последней букве (G или C) представлен в фиолетовый цвет. Эти цвета будут храниться в соответствии в настоящем докладе. Следует отметить,

что ровно два зеленых участков должны быть включены и ровно один желтый и один фиолетовый должен быть включен в любой интерпретации кода.

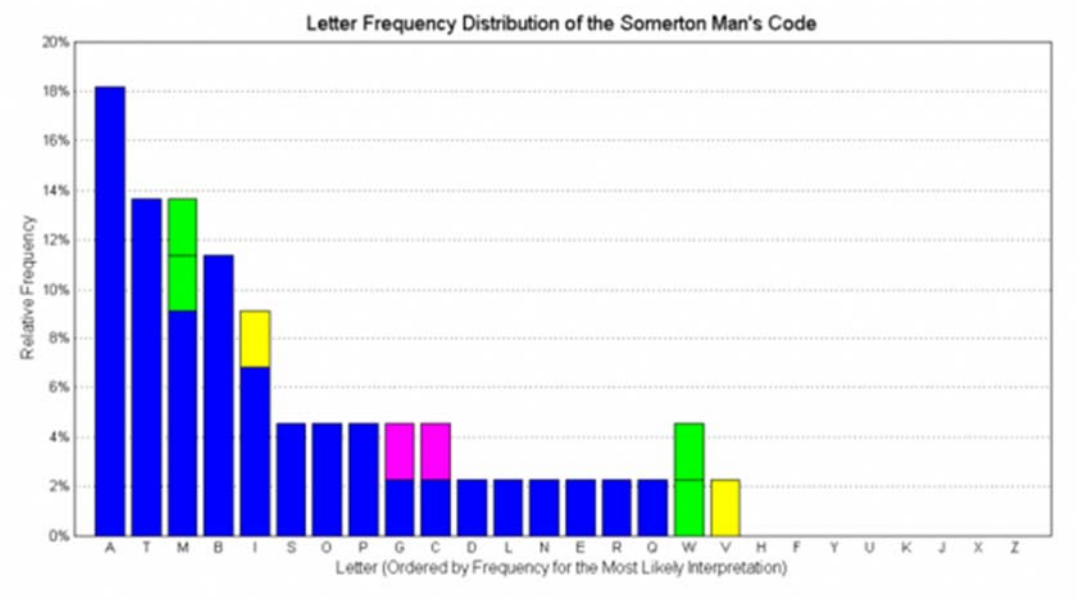


Рис 2. Частотный анализ встречаемости букв

В процессе работы был сделан вывод, что наиболее вероятной, последовательность символов (из чистого первого наблюдения, рис. 2), которая должна выглядеть следующим образом:

Первая строка: WRGOABABD
Вторая строка: WTBIMPANETP
Третья строка: MLIABOAIAQC
Четвертая строка: ITTMTSAMSTGAB
Зачёркнутая линия: MLIAOI

regaf
Alef B: Alef B that's me. I'm Lam. Yes Alef
Lam: Yes me.
I'm but Alef none tape me?
I'm: Lam Yes, Alef B.
Alef: Yes. Alef go for cheap
Yes, that's me. I'm too seen Alef.
Me: i'm seen to go for Alef B.

Regaf – Регулярные силы авиации.
Alef B: Alef B, это я. Я Lam. Да Alef
Лам: Да, меня.
Я, но Алеф не записывал меня?
Я: Lam Да, Alef B.

Alef: Да. Alef продался задёшево.
Да, это я. Я тоже видел Alef.
Я: Я видел, иду за Alef B.
Alef B – Альфред Боксолл.
вав – голос после того, как голос.

Из текста можно сделать вывод, что здесь содержится переписка 3-х человек, один из которых – убитый. Alef B – Альберт Боксолл, вероятно познакомившийся во время войны с немцем с позывным Lam и с убитым, вероятно русским, судя по форме его ушей, что относит его к 3 % населения Земли, проживающим, в основном на Кавказе. Также о связи свидетельствует тот факт, что сын медсестры Неназванной, знакомой с Боксоллом имел точно такое же отклонение, передающееся по наследству. Боксолл, Лам и убитый собирали информацию около военной базы в Австралии, где Великобритания в то время проводила новые испытания самолётов. В то же время после убийства были раскрыты несколько советских агентов, что также доказывает реалистичность версии. Вероятнее всего, убитый был отравлен Ламом, так как по некоторым свидетельствам убитого принесли на это место, что также объясняет начищенные ботинки без песка. В последствии был убит адвокат в Сингапуре, у которого была такая же версия книги. Вероятно, преступники думали, что можно использовать её как ключ, но так как в книге нет ключа, тот адвокат оказался случайной жертвой.

Использование в шифровании

По аналогии данный метод шифрования можно использовать в радиотехнике и современной криптографии. В шифре Таман Шуд используется фарси и транскрипционные аналогии. Таким образом с помощью использования различных алфавитов со сменой с определённой периодичностью можно шифровать сообщения.

Таким образом можно уменьшать размер сообщения и увеличивать криптостойкость. Как пример можно взять древнеславянский алфавит и шифровать тексты с помощью него.

Список используемых источников

1. Stateline South Australia, «Somerton Beach Mystery Man», Transcript, Broadcast 27 March 2009. Accessed 27 April, 2009.
2. The Advertiser, «Somerton Mystery Clue», 15 January 1949 (англ.)

Статья представлена научным руководителем, доктором технических наук В. Т. Яковлевым.

УДК 654.027

МЕТОДИКА ФОРМИРОВАНИЯ МАРШРУТОВ ПЕРЕДАЧИ ИНФОРМАЦИИ В ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ

А. К. Канаев, М. М. Лукичев

Петербургский государственный университет путей сообщения Императора Александра I

Вопросы маршрутизации потоков информации в телекоммуникационной сети являются не простыми. Правильно подобранный метод маршрутизации обеспечивает более эффективное функционирование телекоммуникационной сети. В работе предложен подход для получения требуемого числа рациональных маршрутов, учитывающий разработанную процедуру маршрутизации.

телекоммуникационная сеть, многопутевая маршрутизация.

При построении и эксплуатации современных систем связи одним из важнейших элементов является определение маршрутов прохождения потоков информации между узлами сети. Совокупность всех маршрутов, представленная на физическом графе сети, непосредственно определяет потоковую структуру, которая однозначно определяет физическую возможность реализации потребностей в пропускной способности всех клиентов данной транспортной сети связи [1, 2].

С целью обеспечения эффективности распределения ресурсов пропускной способности, либо обеспечения отказоустойчивости телекоммуникационных сетей целесообразно применять метод многопутевой маршрутизации [3, 4]. Суть метода сводится к нахождению кратчайших маршрутов между рассматриваемыми корреспондирующими парами. После нахождения кратчайшего маршрута любым известным методом [5, 6] линии связи, через которые проходит данный маршрут исключаются из сети, после чего на оставшемся подграфе сети производят аналогичную операцию до тех пор, пока не выполнится условие надежности либо эффективности.

Однако указанный выше подход имеет ряд недостатков. К наиболее существенному можно отнести возможность потери нескольких маршрутов небольшой протяжённости или стоимости при определении и удалении первым кратчайшего маршрута на графе сети, что приводит к снижению эффективности функционирования телекоммуникационной сети в целом либо, в ряде случаев, к невозможности построения требуемого числа маршрутов.

Тем не менее, в работе предложен подход для получения требуемого числа рациональных маршрутов путем минимизации интегральной суммы

длин или веса входящих в маршруты линий связи в рассматриваемой корреспондирующей паре. Для этого разработана процедура, позволяющая получить множество всех возможных маршрутов рассматриваемой корреспондирующей пары, а также определить общую длину или вес линий связи входящих в каждый маршрут. После выполнения данной операции, на множестве маршрутов для рассматриваемой корреспондирующей пары определяется такое подмножество, которое бы удовлетворяло следующим требованиям:

– количество маршрутов в подмножестве должно соответствовать введенному требованию исходя из нормативного значения по надежности доставки информации;

– линии и/или узлы телекоммуникационной сети, используемые в маршрутах не должны повторяться в данном подмножестве, для построения независимых маршрутов, либо допускается использование определенного числа повторов для построения зависимых маршрутов;

– сумма длин или весов линий связи в данном подмножестве маршрутов должна быть минимизирована.

Разработанный подход обеспечивает эффективность использования ресурсов телекоммуникационной сети при поддержании требований по безотказности функционирования для заданных корреспондирующих пар, а также дает возможность использовать зависимые маршруты. Тем не менее, в сравнении с классическим подходом, вычислительная сложность разработанного метода существенно выше, что обеспечивает его применения в части решения задач планирования и проектирования на сетях связи, однако не позволяет, в данный момент, использовать его в динамической маршрутизации.

Список используемых источников

1. Алиев Т. И., Никульский И. Е., Пяттаев В. О. Моделирование и анализ подуровня агрегирования мультисервисной телекоммуникационной сети // Техника связи. 2009. № 2. С. 12–18.

2. Канаев А. К., Сахарова М. А. Нейросетевая модель управления трафиком СПД с применением регулятора с предсказанием // 69-я научно-техническая конференция, посвященная Дню радио. Труды конференции. 2014. С. 203–204.

3. Вишневский В. М. Теоретические основы проектирования компьютерных сетей. М. : Техносфера, 2003. 512 с.

4 Канаев А. К., Сахарова М. А. Моделирование процессов обработки потоков IP-пакетов с различными типами информационных составляющих на основе глубокого анализа трафика // Бюллетень результатов научных исследований. 2014. № 3 (12). С. 85–93.

5. Афанасьев А. П., Гринберг Я. Р., Курочкин И. И. Равномерные» алгоритмы последовательного заполнения потоковой сети потоками продуктов // Труды ИСА РАН. 2005. Т. 14.

6. Малашенко Ю. Е, Новикова Н. М. Суперконкурентное распределение потоков в многопродуктовых сетях // Дискретный анализ и исследование операций. 1997. Т. 4, № 2. С. 34–54.

УДК 654.027

МОДЕЛЬ РАСПРЕДЕЛЕНИЯ ТРАФИКА В СЕТИ СЛЕДУЮЩЕГО ПОКОЛЕНИЯ, УЧИТЫВАЮЩАЯ ПОДДЕРЖАНИЕ ПОКАЗАТЕЛЕЙ КАЧЕСТВА ОБСЛУЖИВАНИЯ

А. К. Канаев, М. М. Лукичев

Петербургский государственный университет путей сообщения Императора Александра I

Определение значений параметров телекоммуникационных сетей, характеризующих качество обслуживания, имеет большую сложность. Представленная в работе имитационная модель телекоммуникационной сети позволяет воспроизвести процесс её функционирования и рассчитать значения параметров, важных с точки зрения качества обслуживания

телекоммуникационная сеть, имитационное моделирование, маршрутизация.

Развитие современных телекоммуникационных сетей связи неразрывно связано с построением рациональной их структуры, для обеспечения требуемых экономических и надежностных показателей. При этом основной функцией транспортной сети остается выполнение множества требований к выделению ресурсов пропускной способности, что соответствует задаче о многопродуктовой потоковой сети [1]. Однако, с развитием сетевой инфраструктуры, все чаще требуется определить не только физическую реализуемость множества требований канального ресурса на известном графе сети, но и основные параметры качества обслуживания при передаче информации соответствующего клиента. Сам процесс определения указанных параметров для телекоммуникационных сетей имеет большую вычислительную и алгоритмическую сложность, из-за значительного количества входных потоков нагрузок. В данных условиях, наиболее приемлемым способом определения параметров качества обслуживания транспортной сети с многопродуктовыми потоками можно считать имитационное моделирование.

Разработка имитационной модели, в рамках представленной работы, включает разработку адекватных моделей исследуемых систем для решения

задач анализа и синтеза сложных сетевых структур, для которых трудно однозначно определить влияние внешних и внутренних факторов. В процессе моделирования решались задачи разработки модели, анализа свойств и выработки рекомендаций по модернизации, существующей или проектированию новой сети [2, 3]. При этом для получения результата, который с достаточной точностью будет отображать реальные процессы в современных транспортных сетях, были учтены факторы, такие как характер входного трафика, способы обработки его узлами сети, с учетом воздействия на них нагрузок других клиентов, принципы формирования маршрутов, а также другие факторы, влияющие на распределение потоков в транспортных сетях.

Кроме этого, для построения адекватной имитационной модели, были определены механизмы обработки пакетов на узле сети. Для этого сформируются маршруты прохождения для каждой корреспондирующей пары путем использования любых известных алгоритмов маршрутизации: Дейкстры [1], Беллмана-Форда [2], Диница [4] и др. Следующим этапом формируются таблицы маршрутизации для каждого узла сети, в которой содержится информация об интерфейсе, в который необходимо передать пакет с требуемым назначением (*next hop*). Таким образом, на каждом узле сформирована таблица, позволяющая перенаправлять пакеты по маршруту от узла источника к узлу приемнику.

После выполнения всех вышеуказанных этапов, формализуется алгоритм работы имитационной модели, которая в общем виде состоит из: генераторов нагрузки, узлов графа сети и его ребер. Результатом работы имитационной модели является определение загрузки каждого ребра сети связи, а также математическое ожидание задержки, ее среднеквадратичное отклонение для каждой конкретной корреспондирующей пары.

Подводя итог, следует отметить, что имитационная модель позволяет воспроизвести процесс функционирования телекоммуникационной сети с сохранением логической структуры и связей между элементами в условиях распределения между ними различных видов трафика. Это позволяет использовать разработанную имитационную модель на стадиях проектирования и модернизации существующих телекоммуникационных сетей.

Список используемых источников

1. Малашенко Ю. Е, Новикова Н. М. Суперконкурентное распределение потоков в многопродуктовых сетях // Дискретный анализ и исследование операций. 1997. Т. 4. № 2. С. 34–54.

2. Вишневский В. М. Теоретические основы проектирования компьютерных сетей. М. : Техносфера, 2003. 512 с.

3. Канаев А. К., Лукичев М. М., Муравцов А. А. Синтез потоковой структуры транспортной сети связи с использованием имитационного моделирования // Известия Петербургского университета путей сообщения. 2015. № 2 (43). С. 105–111.

5. Канаев А. К., Лукичев М. М. Сравнительный анализ алгоритмов построения потоковой структуры телекоммуникационной сети // 69-я научно-техническая конференция, посвященная Дню радио. Труды конференции. 2014. С. 206–208.

УДК 621.396

ПОДХОДЫ К ТЕСТИРОВАНИЮ МОДЕЛЬНОЙ ЛЕТАЮЩЕЙ СЕТИ НА БАЗЕ БПЛА

Р. В. Киричек, М. И. Савенко

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

Одним из приложений Интернета вещей являются летающие сенсорные сети. Такие сети состоят из двух сегментов: наземного и летающего. Летающий сегмент образуется на базе БПЛА общего пользования. На базе модельной летающей сети проводятся экспериментальные исследования и тестирование. Результаты таких исследований могут быть использованы при проектировании летающих сенсорных сетей для различных целей и задач.

летающие сенсорные сети, методика испытаний, тестирование.

В настоящее время развитие сетей связи происходит с учетом концепции Интернета вещей и гетерогенности сетей связи [1, 2, 3]. Одним из достаточно новых приложений Интернета вещей являются летающие сенсорные сети [4, 5].

Прежде чем говорить о разработке летающей сенсорной сети необходимо ввести понятие что это такое.

Летающая сенсорная сеть на базе БПЛА (ЛСС) – один, или несколько летательных аппаратов, взаимодействующих как, между собой, так и с наземными сегментами (рис.).

Поскольку все взаимодействия и связи в такой структуре строго беспроводные, а ко всему прочему зависят от скорости и погодных условий, в отличии от привычных типов сетей, то и гарантированность доступности узлов, и качество связи будет обеспечиваться сложнее. В силу таких особенностей, для построения летающей сенсорной сети необходимо разработать как модель типовой ЛСС, так и методы испытаний, с целью максимально точно исследовать параметры сети на соответствие стандартам.

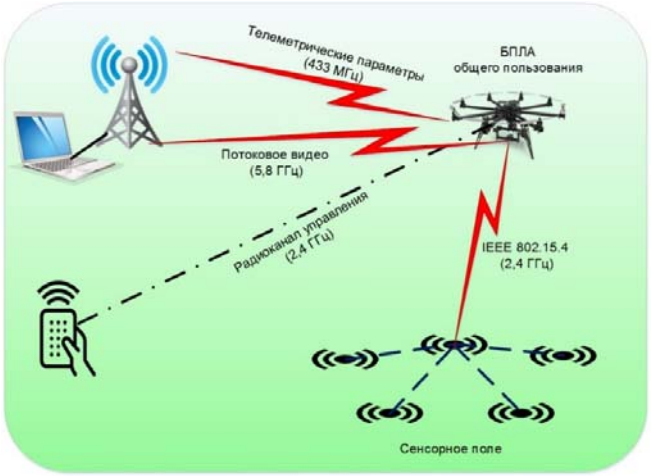


Рисунок. Схема взаимодействия элементов летающей сенсорной сети

Данная схема отображает основополагающие узлы и системы. Следовательно, необходимо обеспечить их безотказную работу и взаимосвязь. В таблице приведены основные проблем, которые могут возникнуть в ходе эксплуатации ЛСС.

ТАБЛИЦА. Основные подсистемы узлов ЛСС, отказы и их последствия

	Задержки	Потери пакетов	Потеря соединения
Потоковое видео с камеры БПЛА (5,8 ГГц)	Помехи при просмотре потокового видео на наземной станции.	Помехи при просмотре потокового видео на наземной станции.	Отсутствие визуального контроля движения БПЛА по заданному маршруту, неспособность преодолевать препятствия на пути.
Канал радиоуправления (2,4 ГГц)	Невыполнение команд по изменению курса движения или высоты. Возможность столкновения с препятствием.	Возможность столкновения с препятствием.	Выход БПЛА из строя.
Канал взаимодействия летающего и наземного сегмента (2,4 ГГц)	Увеличение количества необслуживаемых сенсорных узлов	Неполные и ошибочные данные, полученные с сенсорных полей.	Отсутствие передачи данных с сенсорных полей.
Канал передачи телеметрических параметров (433 МГц)	Предоставление информации о параметрах полета БПЛА с задержками.	Краткие прерывания в передаче данных о параметрах полета БПЛА.	Неспособность контролировать параметры полета (возможен только визуальный контроль)

Что бы убедиться в том, что ЛСС работает должным образом, необходимо провести ряд испытаний и тестирование на соответствие существующей нормативной базе, характерной для беспроводных сетей связи. На базе лаборатории Интернета вещей СПбГУТ была разработана модельная летающая сенсорная сеть [6, 7, 8, 9]. Ниже приводится перечень видов тестирования, которые проводились согласно разработанной методике [10, 11, 12, 13]:

1. Тестирование летающего сегмента сенсорной сети.

Первый тест-это тест на исследование сходимости летающего сегмента при выходе из строя одного или нескольких БПЛА и определение минимального времени для реконфигурации сети.

– цель теста: необходимо протестировать летающий сегмент на сходимость при выходе из строя БПЛА при различных архитектурах построения сети и определить время, необходимое для восстановления сети;

– тестовая процедура:

- ✓ организовать летающий сегмент ЛСС в двух структурах (все БПЛА одинаковы по функциональности, когда имеется головной узел);
- ✓ удаленно вывести из строя один или несколько БПЛА;
- ✓ зафиксировать время, которое потребуется для восстановления функционирования летающего сегмента.

– результаты: в результате теста необходимо определить способность к сходимости летающего сегмента и получить минимальное время для восстановления сети.

2. Тестирование периода опроса наземного сегмента и сбора с него данных.

Следующим шагом определяется период сбора данных с сенсорных узлов.

– цель теста: определить период опроса сенсорных узлов (как часто проводить тестирование?);

– тестовая процедура:

- ✓ установить соединение БПЛА с наземным сегментом;
- ✓ определить максимальную нагрузку и энергоэффективность узлов;
- ✓ рассчитать промежуток времени, спустя который проводить повторный сбор данных с сенсоров, используя полученные данные о нагрузке и энергоэффективности узлов.

– результаты: в результате теста необходимо определить период времени, спустя который можно будет повторять повторный сбор данных.

3. Тестирование качества передачи данных с наземного сегмента.

Следующая процедура-подсчет коэффициента битовых ошибок. Проводится на физическом уровне.

– цель теста: определить коэффициент битовых ошибок (*BER*) при передачи данных с наземного сегмента.

– тестовая процедура:

- ✓ инициировать передачу данных между сенсорным узлом наземного сегмента сети и БПЛА, выполняющего роль летающего сегмента, в условиях среды, приближенных к идеальным;
- ✓ оценить параметр *BER* при передаче данных.

– результаты: в результате теста будут получены следующие параметры: время теста, общее количество переданных бит, общее количество бит с ошибкой, а также их соотношение.

Параметр коэффициента битовых ошибок рассчитывается по формуле:

$$\mu = \frac{n}{N},$$

где n – количество принятых бит с ошибкой, N – общее количество принятых бит.

4. Тестирование дальности связи с летающим сегментом.

– цель теста: необходимо определить максимально возможное расстояние, при котором будет возможна передача данных с сенсорного узла на удаленную базу данных.

– тестовая процедура:

- ✓ установить соединение БПЛА с сенсорным узлом;
- ✓ организовать передачу данных с сенсорного узла группе БПЛА, которые будут по цепочке передавать полученные данные;
- ✓ определить максимально возможное расстояние, при котором будет достоверная передач данных без потерь.

– результаты: в результате теста необходимо определить максимальное расстояние для передачи данных без потерь.

Вышеуказанный ряд тестов фактически является тестовой спецификацией, которая может быть использована для комплексного тестирования ЛСС. Результат таких испытаний – выявленные отклонение сети от работы в штатном режиме, а также соответствие нормам проектирования, производительности и безопасности.

Список используемых источников

1. Кучерявый А. Е., Прокопьев А. В., Кучерявый Е. А. Самоорганизующиеся сети. СПб. : Любавич, 2011. 310 с.

2. Кучерявый А. Е. Интернет Вещей // Электросвязь. 2013. № 1. С. 21–24.

3. Киричек Р. В., Парамонов А. И., Прокопьев А. В., Кучерявый А. Е. Эволюция исследований в области беспроводных сенсорных сетей // Информационные технологии и телекоммуникации. 2014. № 4 (8). С. 29–41.

4. Кучерявый А. Е., Владыко А. Г., Киричек Р. В., Парамонов А. И., Прокопьев А. В., Богданов А. И., Дорг-Гольц А. А. Летающие сенсорные сети // Электросвязь. 2014. № 9. С. 2–5.

5. Кучерявый А. Е., Владыко А. Г., Киричек Р. В. Летающие сенсорные сети – новое приложение интернета вещей // Актуальные проблемы инфотелекоммуникаций в науке и образовании. IV международная научно-техническая и научно-методическая конференция: сборник научных статей в 2 томах. СПб. : СПбГУТ, 2015. Т. 1. С. 17–22.

6. Kirichek R., Koucheryavy A. Internet of Things laboratory test bed//Lecture Notes in Electrical Engineering. 2016. Vol. 348. PP. 485–490, DOI: 10.1007/978-81-322-2580-5_44.

7. Koucheryavy, A., Vladyko, A., & Kirichek, R. State of the art and research challenges for public flying ubiquitous sensor networks // In Conference on Smart Spaces – Springer International Publishing, 2015. pp. 299–308.

8. Kirichek, R., Vladyko, A., Paramonov, A., Koucheryavy, A.: Software-Defined Architecture for Flying Ubiquitous Sensor Networking. In: 19th International Conference on Advanced Communication Technology (ICACT), pp. 158–162 (2017).

9. Kirichek, R., Vladyko, A. Zakharov, M., Koucheryavy, A.: Model Networks for Internet of Things and SDN. In: 18th International Conference on Advanced Communication Technology (ICACT), pp. 76–79. IEEE (2016).

10. Kirichek R., Kulik V. Long-Range Data Transmission on Flying Ubiquitous Sensor Networks (FUSN) by Using LPWAN Protocols // In Communications in Computer and Information Science, 2016, vol. 678, pp. 442–453. DOI: 10.1007/978-3-319-51917-3_39.

11. Kirichek R., Paramonov A., Koucheryavy A. Flying ubiquitous sensor networks as a quening system // in Proc. 17th ICACT, pp. 127–132, 2015. DOI: 10.1109/ICACT.2015.7224771.

12. Kirichek R., Paramonov A., Vareldzhyan K. Optimization of the UAV-P's motion trajectory in public flying ubiquitous sensor networks (FUSN-P) // In ser. Lecture notes in computer science, vol. 9247, pp. 352–366, 2015. DOI: 10.1007/978-3-319-23126-6_32.

13. Кучерявый А. Е., Владыко А. Г., Киричек Р. В. Теоретические и практические направления исследований в области летающих сенсорных сетей // Электросвязь. 2015. № 7. С. 9–11.

УДК 004.738

СЕМАНТИЧЕСКИЙ MQTT-ШЛЮЗ ДЛЯ LoRaWAN

Р. В. Киричек, В. Д. Фам

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

В данной статье представлены результаты исследования сематического MQTT-шлюза для беспроводной технологии LoRA. Для проведения исследования были

разработаны структурная схема сетевого взаимодействия и программная архитектура для семантического MQTT-шлюза. В качестве аппаратной платформы рассматривается модуль Semtech SX1276 и микрокомпьютер Raspberry Pi 3, который получает данные от удаленных LoRa-узлов и передает данные в Интернет по протоколу MQTT. Протокол MQTT является наиболее распространенным на сегодняшний день для устройств Интернета Вещей. В ходе эксперимента определяется задержка, загрузка центрального процессора и загрузки оперативной памяти, которые, в свою очередь, зависят от количества обслуживаемых LoRa-узлов.

Интернет Вещей, протокол, MQTT, LoRaWAN, семантический шлюз.

Развитие концепции Интернета вещей [1, 2, 3] диктует необходимость появления новых технологий передачи данных для устройств с низким энергопотреблением. Фактически в 2014–2016 гг. был создан новый класс сетей LPWAN (*Low-power Wide-area Network*) – энергоэффективная сеть дальнего радиуса действия. Одним из представителей данного класса является технология LoRa [3, 4, 5, 6], которая появилась в 2015 г. и была представлена компанией Semtech. Данная технология ориентирована на передачу данных на дальние расстояния 1–20 км. Используя данную технологию можно передавать телеметрические данные от устройств с низким энергопотреблением и работающим от одного комплектов элементов питания до 10 лет. Технология LoRa работает на частоте 433 МГц (Азия), 868 МГц (Европа) и 915 МГц (США). С учетом этих характеристик беспроводная технология LoRa очень подходит для Интернета Вещей [4, 5, 7].

В сети LoRaWAN доступ к Интернету осуществляется с помощью шлюза, в частном случае такой шлюз является LoRa-узлом и подключается к Интернету по Wi-Fi или Ethernet. Протокол MQTT (*Message Queue Telemetry Transport*) [8, 9], который является одним из популярных протоколов Интернета Вещей, используется в этом шлюзе для передачи информаций от LoRa-узлов к Брокеру и для получения информаций от него. Схема взаимодействия между узлами и шлюзами показана на рис. 1.

Ввиду того, что для передачи данных к Брокеру используется протокол MQTT шлюз называется MQTT-шлюзом. В ходе натурного эксперимента в лаборатории Интернета вещей СПбГУТ был разработан шлюз на основе микрокомпьютера Raspberry Pi 3 Model B с LoRa-модулем, подключенным через интерфейс UART [10]. На микрокомпьютере предустановлена операционная система Raspbian, поэтому можно разрабатывать сценарии работы шлюза на многих языках программирования. Протокол MQTT представляется протокол обмена сообщениями издатель-подписчик (*publish/subsribe*). Издатель (*publisher*) – это MQTT-клиент публикует данные, а подписчик (*subsciber*) – это MQTT-клиент подписывает на каналы (топики). В этом слу-

чае MQTT-шлюз играет в роль клиента, который может публиковать и подписаться на топики Брокера. Шлюзы тоже могут сообщаться между собой через Брокер. Принцип работы шлюза представляется на рис. 2 (см. ниже).

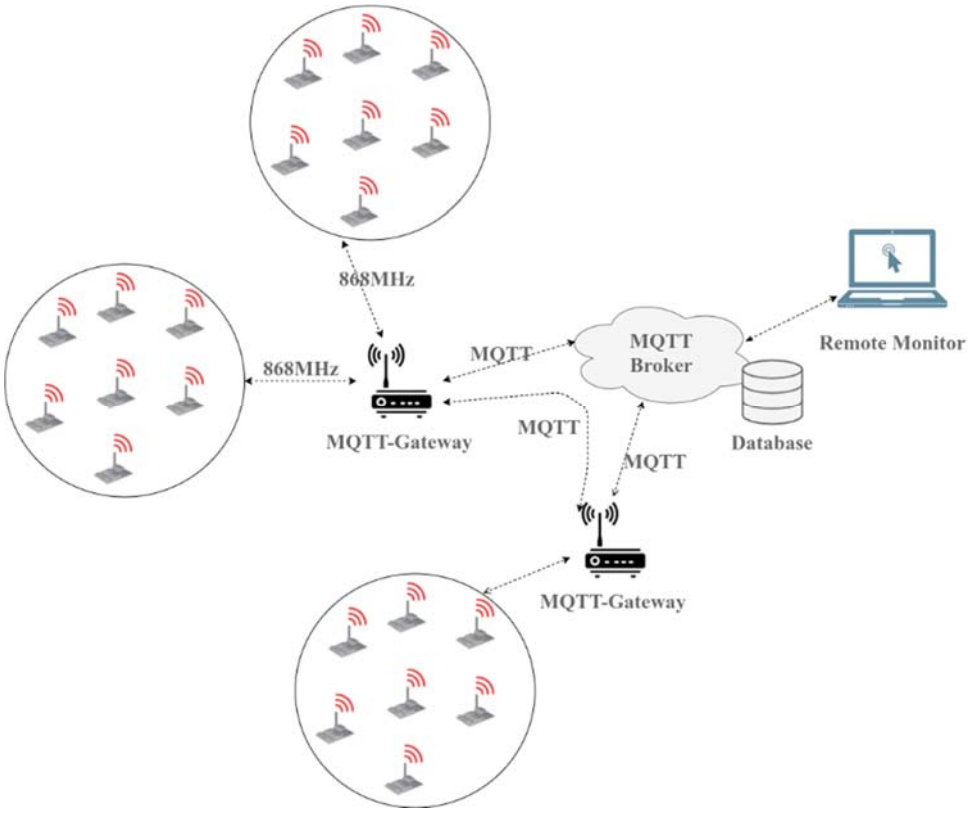


Рис. 1. Схема взаимодействия между узлами и шлюзами

LoRa-узлы передают сообщения к шлюзу по форматам:

<ID>/<action>/<topic>/<value>

<ID> – идентификатор узла, которые подтверждает, что узел находится в этой сети.

<action> – могут быть “pub”, “sub”, “unsub”.

С учетом данного формата сообщений, шлюз распознает, что узел с заданным <ID> хочет публиковать (*sub*) данные <value>, подписаться (*sub*) или не подписаться (*unsub*) на этот топик (<*topic*>). Если один *LoRa*-узел хочет опубликовать данные на топик “temp”, то ему нужно передать сообщения со своим идентификатором и данными по формату “<id>/pub/temp/<data>” к Брокеру. А если LoRa-узел хочет подписаться на топик “humidity”, то этот узел будет передавать один раз к Брокеку сообщение со своим идентификатором “<id>/sub/humidity”. После этого Брокер подписывается на топик “humidity”, когда данные “humidity” появляются, Брокер сразу передает эти данные LoRa-узлу. И соответственно с <action> = “unsub”, когда LoRa-узел хочет остановить подписку.

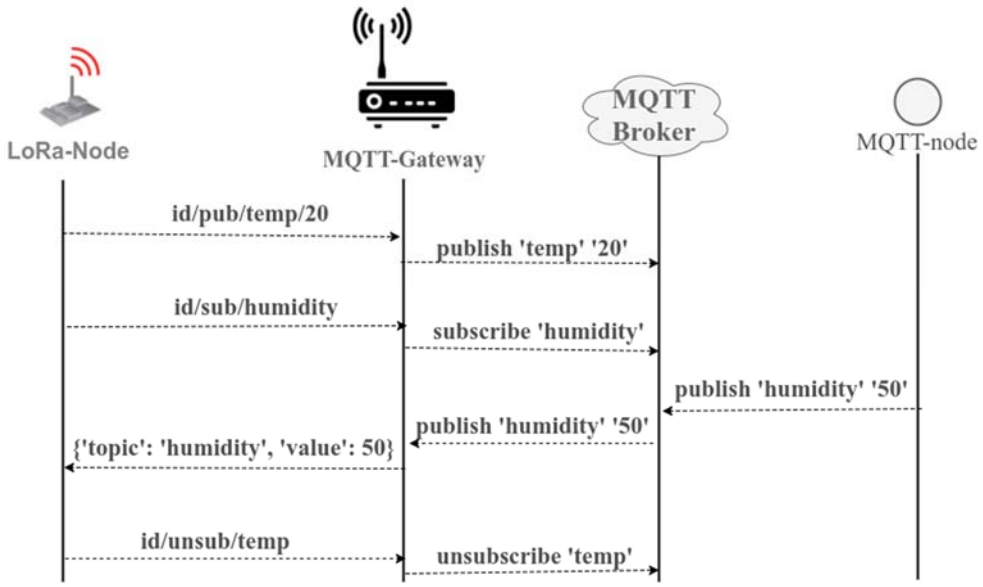


Рис. 2. Принцип работы MQTT-шлюза

В ходе исследования были рассмотрен параметр временени обработки сообщения шлюзом при получении сообщений от LoRa-узла и Брокера. При проведении эксперимента измерили время обработки 100 сообщений. В течении получения 100 сообщений измеряли время от момента получения до момента публикации сообщения, переданных LoRa-узлом к Брокеру, и время от момента получения сообщения Брокера до момента передачи их LoRa-узлам. График изменения времени в зависимости от количества испытаний приведен на рис. 3. На графике видно, что шлюз быстро обрабатывает сообщения, когда получает их от Брокера и передает LoRa-узлам. А при перенаправлении данных от LoRa-узла к Брокеру, шлюз тратит больше времени.

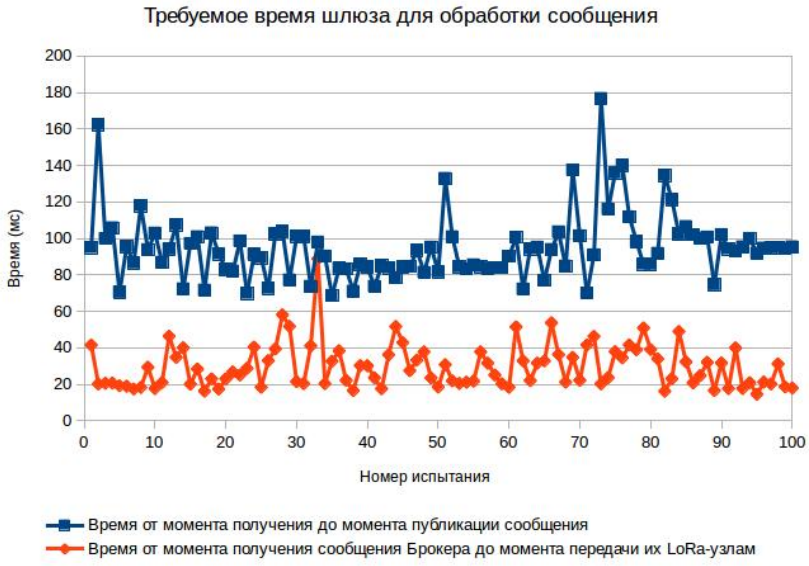


Рис. 3. Время обработки сообщения шлюзом

В ходе тестирования шлюза рассматривались параметры загрузки процессора и оперативной памяти шлюза. На базе лабораторного стенда были проведены эксперименты с 10 обслуживаемыми узлами (клиентами). Полученные зависимости представлены на рис. 4. На графике видно, что на шлюзе низкая загрузка оперативной памяти и загрузка процессора (в среднем составляет от 25 % до 35 %). Такая загрузка характерна для шлюза в процессе работы. На основе проведенного исследования можно сделать вывод, что шлюз обслуживает LoRa-узлы без перегрузок в пределах функциональных характеристик.

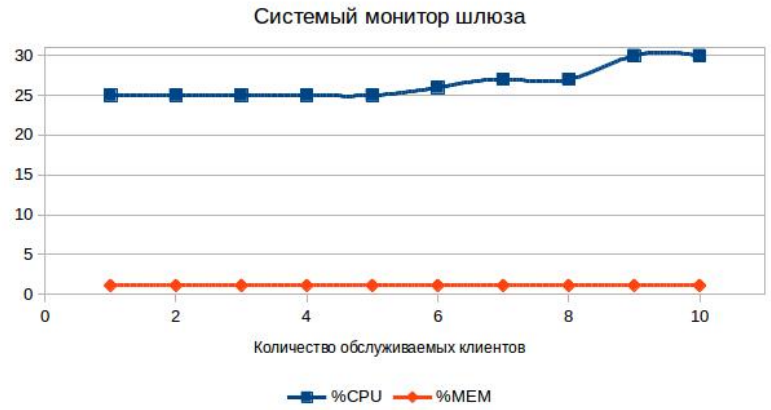


Рис. 4. Параметры загрузки процессора и оперативной памяти шлюза

В статье рассмотрены результаты исследования MQTT-шлюза для сети LoRaWAN. Для исследования шлюза были разработан лабораторный стенд, а также программное обеспечение MQTT-шлюза для сети LoRaWAN. В результате исследования было установлено, что шлюз обеспечивает взаимодействие сенсорных узлов на базе технологии LoRa с Брокером MQTT. По результатам тестирования шлюза установлено, что время обработки сообщения измеряется в мс и при использовании MQTT-шлюза загрузка оперативной памяти, а также загрузка процессора незначительная. Можно сделать вывод, что испытываемы шлюзы походят для использования в инфраструктуре «Умных городов».

Список используемых источников

1. Кучерявый А. Е., Прокопьев А. В., Кучерявый Е. А. Самоорганизующиеся сети. СПб. : Любавич, 2011. 310 с.
2. Кучерявый А. Е. Интернет Вещей // Электросвязь. 2013. № 1. С. 21–24.
3. Киричек Р. В., Парамонов А. И., Прокопьев А. В., Кучерявый А. Е. Эволюция исследований в области беспроводных сенсорных сетей // Информационные технологии и телекоммуникации. 2014. № 4 (8). С. 29–41.
4. Semtech, “LoRaWAN Specification v1.0”, Jan. 2015.
5. Гимранов Р. Р., Киричек Р. В., Шпаков М. Н. Технология межмашинного

взаимодействия LoRa // Информационные технологии и телекоммуникации. 2015. № 2 (10). С. 62–73.

6. Kirichek R., Kulik V. Long-Range Data Transmission on Flying Ubiquitous Sensor Networks (FUSN) by Using LPWAN Protocol // Communications in Computer and Information Science, 2016. Vol. 678. PP. 442–453. DOI: 10.1007/978-3-319-51917-3_39.

7. Kirichek R. The Model of Data Delivery from the Wireless Body Area Network to the Cloud Server with the Use of Unmanned Aerial Vehicles // Proceedings of 30th European Conference on Modelling and Simulation Proceedings – ECMS. 2016. PP. 603–606. DOI: 10.7148/2016-0603.

8. MQTT V3.1 Protocol Specfication. International Business Machines Corporation (IBM) Eurotech. 2015. PP. 1–2.

9. Киричек Р. В., Фам В. Д., Юльчиева Л. О. Исследование протоколов взаимодействия интернета вещей на базе лабораторного стенда // Информационные технологии и телекоммуникации. 2016. № 1. С. 55–67.

10. Kirichek R., Koucheryavy A. Internet of Things laboratory test bed // Lecture Notes in Electrical Engineering. 2016. Vol. 348. PP. 485–490. DOI: 10.1007/978-81-322-2580-5_44.

УДК. 621.391

КОНЦЕПТУАЛЬНЫЙ ПОДХОД К ИССЛЕДОВАНИЮ ИНФОКОММУНИКАЦИОННОЙ СЕТИ

А. А. Киселев[1], М. А. Сазонов[2]

[1]ПАО «Интелтех»
[2]Военная академия связи имени Маршала Советского Союза С. М. Буденного

В работе представлен методологический подход рассмотрения инфокоммуникационной сети в рамках системного анализа. Содержательная часть статьи посвящена раскрытию неформальных, содержательных признаков системы: расчленимости, целостности, связанности и неаддитивности.

системный анализ, системный подход, инфокоммуникационная сеть.

В наше время есть понимание необходимости применения системного подхода к решению проблем различного характера, но далеко не всегда есть понимание, каким образом использовать этот подход на практике [1].

За основу комплексного, всестороннего исследования организации инфокоммуникационной сети (ИКС) выбран системный анализ.

Объектом системного анализа выступает ИКС, которую необходимо создать (спроектировать, спланировать) или модернизировать, с целью предоставления услуг абонентам (потребителям) с заданным качеством.

При этом рассматриваемая сеть является общим, обобщающим случаем ИКС.

В настоящее время общепринято, что неформальными, содержательными признаками системы являются: расчленимость, целостность, связанность и неаддитивность [1, 2].

Изучаемый объект расчленим, если существует возможность выделить в нем фиксированное число составных частей первого уровня, а в них части второго уровня и так далее вплоть до последнего уровня, состоящего из неделимых далее частей. Составные части представленного таким образом объекта, кроме частей последнего уровня, называются подсистемами. Части последнего или низшего уровня принято именовать элементами. Элементы и подсистемы обозначаются обобщающим термином «компоненты».

Понятие «уровень» употребляется в системном анализе в четырех значениях [1]:

1. Уровень трактуется в организационном плане (уровни-эшелоны).

2. Уровнем фиксируется определенная общность законов функционирования (уровни-страты).

3. Понятием уровня выражается точка зрения исследователя на различные аспекты изучаемой системы (уровни-слои).

4. Определением уровня часто выражается оценочная характеристика анализируемого объекта или явления (уровни-оценки).

Тогда уровни представления для ИКС можно записать в виде упорядоченной последовательности (кортежа):

$$Y_{\text{ИКС}} = \langle Y_{\text{Э}}, Y_{\text{Ст}}, Y_{\text{Сл}}, Y_{\text{О}} \rangle,$$

где $Y_{\text{Э}}$ – уровни-эшелоны, $Y_{\text{Ст}}$ – уровни-страты, $Y_{\text{Сл}}$ – уровни-слои, $Y_{\text{О}}$ – уровни-оценки.

С этой точки зрения ИКС можно представить в виде следующих уровней-эшелонов (рис. 1).

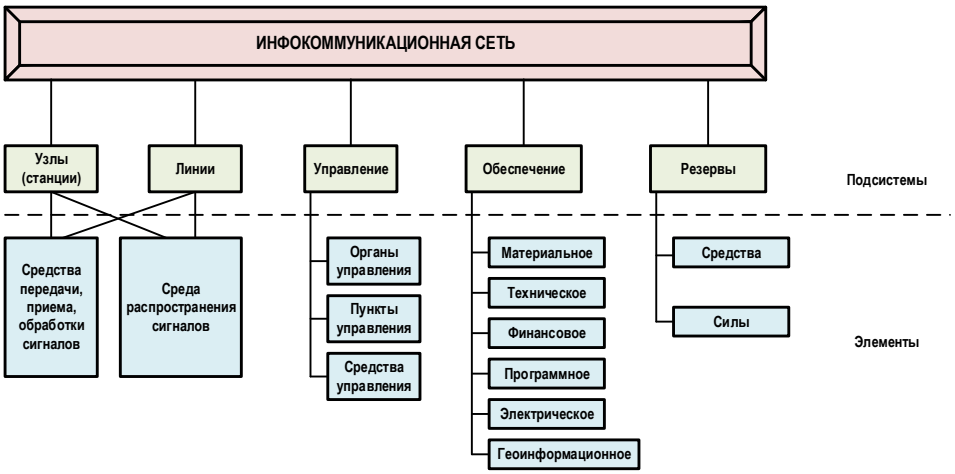


Рис. 1. Организационное представление инфокоммуникационной сети

ИКС собственно и является системой, которая подлежит описанию и дальнейшему исследованию. В свою очередь она включает подсистемы: узлов (станций), линий, управления, обеспечения, резервов.

Таким образом, признак расчленимости ИКС с точки зрения организационного построения можно представить в виде:

$$Y_{\text{Э}} = \left\langle Ps_{\text{с}}, Ps_{\text{л}}, Ps_{\text{у}}, Ps_{\text{о}}, Ps_{\text{р}} \right\rangle,$$

где $P_{S\text{с}}$ – подсистема узлов (станций), $P_{S\text{л}}$ – подсистема линий связи, $P_{S\text{у}}$ – подсистема управления, $P_{S\text{о}}$ – подсистема обеспечения, $P_{S\text{р}}$ – подсистема резервов.

С позиций общности законов функционирования, единства пространственно-временной топологии и субстанционального построения определенных компонентов системы ИКС может рассматриваться на различных уровнях (социальном, экономическом, информационно-управленческом, технологическом и т. п.). Имеющиеся на сегодняшний день представления о ИКС [3, 4] позволяют ее стратифицировать по следующим уровням (рис. 2): по категориям ($St_{\text{кат}}$); по территориальному делению и назначению ($St_{\text{тд}}$); по функциональному признаку ($St_{\text{фп}}$); по типу присоединяемых абонентских терминалов ($St_{\text{ат}}$); по выполнению требований по устойчивости, безопасности ($St_{\text{уст}}$); по количеству служб электросвязи ($St_{\text{сэ}}$); по виду коммутации ($St_{\text{ком}}$); по технологии распределения информации ($St_{\text{ри}}$); по характеру среды распространения сигнала ($St_{\text{ср}}$); по месту на рынке ($St_{\text{р}}$); по обеспечению функционирования ($St_{\text{ф}}$); по уровням взаимодействия ($St_{\text{вз}}$); по функциональным областям управления ($St_{\text{фо}}$); по признакам передаваемого сообщения ($St_{\text{пс}}$); по виду программного обеспечения ($St_{\text{впо}}$); по уровню программного обеспечения ($St_{\text{упо}}$); по виду информационного фонда ($St_{\text{иф}}$); по виду базы данных ($St_{\text{бд}}$); по виду системы управления базами данных (СУБД) ($St_{\text{субд}}$); по назначению услуг($St_{\text{усл}}$); по важности услуг ($St_{\text{вусл}}$); по характеру использования услуг ($St_{\text{хусл}}$); по группам пользователей (абонентам) ($St_{\text{аб}}$), т. е.:

$$Y_{\text{Ст}} = \left\langle \begin{matrix} St_{\text{кат}}, St_{\text{тд}}, St_{\text{фп}}, St_{\text{ат}}, St_{\text{уст}}, St_{\text{сэ}}, St_{\text{ком}}, St_{\text{ри}}, St_{\text{ср}}, St_{\text{р}}, St_{\text{ф}}, St_{\text{вз}}, \\ St_{\text{фо}}, St_{\text{пс}}, St_{\text{впо}}, St_{\text{упо}}, St_{\text{иф}}, St_{\text{бд}}, St_{\text{субд}}, St_{\text{усл}}, St_{\text{вусл}}, St_{\text{хусл}}, St_{\text{аб}} \end{matrix} \right\rangle.$$

Следующим представлением ИКС являются уровни-слои. Они отражают отношение исследователя к данному объекту, фиксируя способы познания его характеристик, глубину проникновения в сущность изучаемого объекта. Зачастую слоями называют структурные компоненты системы, выделенные по временному признаку или по типу решаемых задач. С этих позиций для ИКС можно выделить следующие слои: прогнозирование, проектирование (планирование) и управление:

$$Y_{\text{Сл}} = \left\langle Sl_{\text{пр}}, Sl_{\text{пл}}, Sl_{\text{упр}} \right\rangle,$$

где $Sl_{пр}$ – слой прогнозирования, $Sl_{пл}$ – слой проектирования (планирования), $Sl_{упр}$ – слой управления.

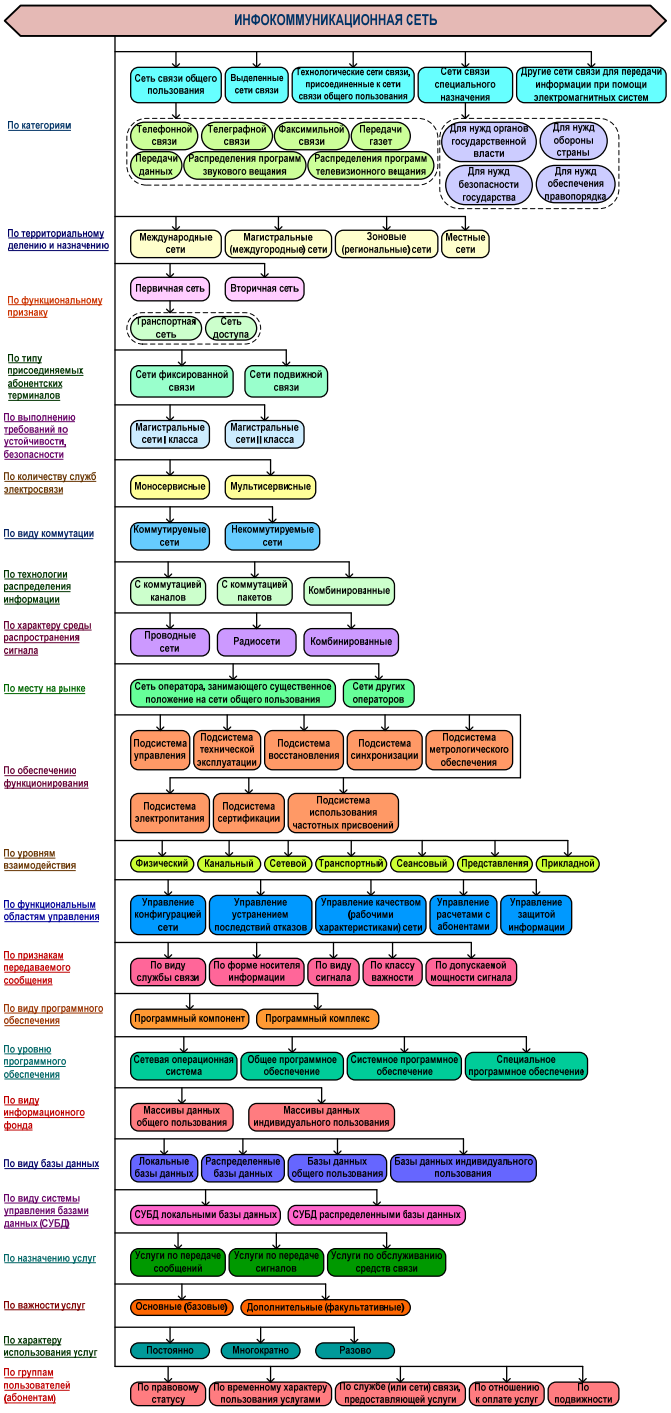


Рис. 2. Стратификация инфокоммуникационной сети по уровням

Четвертым значением понятия «уровень» является оценочная характеристика анализируемого объекта или явления. В этом случае, как правило, оперируют двумя важными характеристиками: качеством предоставления услуг и эффективностью функционирования ИКС:

$$Y_{\text{О}} = \left\langle O_{\text{икс}}, O_{\text{пцф}}, O_{\text{у}} \right\rangle,$$

где $O_{\text{икс}}$ – оценочная характеристика ИКС, $O_{\text{пцф}}$ – оценочная характеристика процесса функционирования ИКС, $O_{\text{у}}$ – оценочная характеристика услуги, предоставляемой ИКС.

Следующим содержательным признаком системы является целостность. Она исторически выступает родовым признаком системы.

Формальное содержание этого признака заключается в следующем.

Объект, состоящий из нескольких выделенных частей, обладает целостностью, если [1, 2]:

а) в нем в результате взаимодействия частей образуется новое качество (общесистемное свойство), отсутствующее у частей;

б) каждая составная часть приобретает иные качества (системные свойства компонентов) по сравнению с качествами, присущими этим же частям вне данного объекта.

Таким образом, признак целостности отражает особенности не всякого, а определенного вида целого, такого, где достаточно выражено единство и где обязательно имеются выделенные части, влияющие друг на друга. Простое механическое вычленение какого-либо объекта из такого целого приводит к тому, что в итоге получается другой объект.

Третьим, содержательным признаком системы, является связность. Связанность для ИКС следует рассматривать как признак, свидетельствующий о том, что целостные свойства сети и особые свойства ее частей формируются за счет межкомпонентных (внутриуровневых и межуровневых) отношений, связей и взаимодействий.

Заключительный признак системы – неаддитивность проявляется в том, что свойства изучаемого объекта невозможно свести к свойствам его частей, а также вывести лишь из них. Этот признак в несколько иной интерпретации можно выразить формулой: если изучаемый объект представляется в данном исследовании как система, то при любом способе разделения такого объекта на части невозможно выявить его целостные свойства.

Таким образом, ИКС, показана как система, так как она идентифицируется по признакам расчленимости, целостности, связанности и неаддитивности, а само исследование относится к классу системных, так как оно процедурно строится без нарушения положений этих признаков.

Представленный подход системного описания ИКС в теоретической и практической областях выступает основой, базой для проектирования (планирования), как ИКС в целом, так и отдельных ее элементов.

Список используемых источников

1. Новосельцев В. И. и др. Теоретические основы системного анализа / под ред. В. И. Новосельцева. М. : Майор, 2006. 592 с.

2. Петухов Г. Б., Якунин В. И. Методологические основы внешнего проектирования целенаправленных процессов и целеустремленных систем. М. : АСТ, 2006. 504 с.

3. Федеральный закон «О связи» от 07.07.2003 г. № 126-ФЗ (с изменениями на 6 июля 2016 года).

4. Булгак В. Б. и др. Концептуально-целевые основы развития и общие организационно-технические положения. Руководящий документ. Книга 1. М. : ЦНТИ «Информсвязь», 1996. 247 с.

УДК 65.011.56

ПОДХОД К ВНЕДРЕНИЮ КОНЦЕПЦИИ CEM В РАМКАХ ДОМЕНА ASSURANCE КАРТЫ TAM

С. В. Кисляков, А. А. Кормановская

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

Customer Experience Management – концепция, включающая в себя совокупность методов, процессов и технологий, которые позволяют отслеживать, измерять и управлять впечатлениями клиента при взаимодействии с компанией-оператором связи. Одним из важнейших аспектов, формирующих положительный клиентский опыт, является грамотная организация процессов взаимодействия с клиентом в различных точках его контакта с компанией, в частности в рамках домена Assurance карты TAM. В докладе рассматривается подход к внедрению концепции CEM в системы OSS-среды, относящиеся к домену Assurance, на примере процессов современного оператора связи.

Customer Experience, Customer Experience Management, TAM, OSS/BSS, Assurance.

С каждым днем на рынке телекоммуникации конкуренция между операторами связи усиливается, и для любой компании одной из первостепенных задач является работа по удержанию клиентов и их лояльностью. Чтобы компания была высококонкурентной, ей необходимо не только грамотно организовать процесс общения с клиентом, но и уделить огромное внимание решениям задач по управлению клиентским опытом. С помощью этих решений можно снизить отток клиентов, и, несомненно, преумножить доходы копании. Вследствие чего, применение концепции Customer Experience Management в специфике оператора связи набирает большую популярность.

Понятие клиентский опыт – Customer Experience (CE) складывается из множества факторов, и представляет собой совокупность впечатлений, желаний и ощущений, которая возникает на протяжении всего жизненного цикла клиента – Customer Lifecycle. На каждом этапе жизненного цикла клиентский опыт (CE) может быть, как положительным, так и отрицательным,

но в любом случае CE будет влиять на лояльность и отток клиентов в будущем [1]. Поэтому компании оператора связи необходимо уметь отслеживать, анализировать и влиять на клиентский опыт. Для решения этих задач существует концепция Customer Experience Management (CEM) – управление клиентским опытом, которая описывает подход в качественном обслуживании клиента, обеспечивает управление эмоциональным опытом клиента, а также увеличивает его ценность у оператора связи. CEM можно применить в точках взаимодействия клиента с компанией. И цель оператора – добиться того, чтобы клиент был доволен в каждой точке взаимодействия, и превзойти его ожидания.

Поиск точек взаимодействия начинается с тщательного анализа процесса, который происходит в компании оператора связи. Чтобы проанализировать процесс, необходимо изучить системы, в которых он происходит. Для этого рассмотрим один из стандартов TM Forum, а именно карту приложений в области телекоммуникаций – Telecom Application Map (TAM), которая описывает функции систем и приложений в IT-ландшафте оператора связи [2]. TAM разделена на функциональные домены, базирующиеся на бизнес-процессах, которые определены в карте eTOM. Выделяют девять доменов:

1. Маркетинг и продажи (*Market_Sales Domain*).
2. Продукт (*Product Domain*).
3. Клиент (*Customer Domain*).
4. Услуги (*Service Domain*).
5. Ресурс (*Resource Domain*).
6. Поставщики и партнеры (*Supplier_Parther Domain*).
7. Предприятие (*Enterprise Domain*).
8. Кросс-доменные приложения (*Cross Domain*).
9. Интеграционная инфраструктура (*Integration Infrastructure Domain*).

Кроме того, карта TAM разделена на вертикальные группы, которые отвечают за конкретные процессы:

1. Стратегия, Инфраструктура и Продукт (*Strategy, Infrastructure and Product*) – отвечает за планирование, разработку стратегии и управление жизненным циклом продукта и инфраструктуры [2].

2. Готовность к работе и эксплуатационная поддержка (*Operation Support and Readiness*) – отвечает за создания условий и обеспечение готовности для эффективного выполнения групп Fulfillment, Assurance и Billing.

3. Продажа/Обработка заказов (*Fulfillment*) – отвечает за своевременное выполнение заказа и оповещение клиентов о ходе его выполнения.

4. Управление качеством (*Assurance*) – отвечает за обеспечение качества услуги и технического обслуживания. А также обрабатывает жалобы клиентов, информирует их о возможных перерывах связи и следит за своевременным устранением возникшей проблемы.

5. Биллинг (*Billing*) – занимается решение проблем, возникающих во время оплаты услуг, и отвечает на запросы клиентов, которые касаются начисления оплаты.

На пересечении рассмотренных доменов и групп располагаются системы. При этом если анализировать процессы в этих системах, можно найти огромное количество точек взаимодействия с клиентом. Эти точки будут появляться на протяжении всего процесса, который затрагивает сразу несколько систем, однако оператор связи не всегда знает, что с ними делать. В связи с этим компания не знает, что о ней думает клиент, нет возможности влиять на лояльность клиента, а также происходит неэффективное взаимодействие с клиентом.

Для решения этих проблем необходимо использовать концепцию CEM, которая при внедрении в среду оператора связи поможет управлять CE.

На данный момент можно выделить два основных подхода реализации концепции CEM в общей OSS/BSS среде оператора связи:

– внедрение CEM, как отдельной самостоятельной системы;

– реализация концепции CEM, как набора инструментов к существующим решениям;

Рассматривая первый подход – внедрение CEM, как отдельной самостоятельной системы, потребуется решения важной задачи, а именно как подобная система должна вписываться в общую среду оператора связи. Система CEM должна выступать единым накопителем данных о CE, как количественных, так и качественных от всех систем OSS/BSS комплекса оператора связи, анализируя и используя CE для решения прикладных задач в дальнейшем. Исследуя функциональную архитектуру системы, можно выделить уровни: агрегации (*Data Aggregation*), анализа (*Analytics*), взаимодействия с клиентом (*Customer Interaction Management*) и прикладной уровень (*Application*). Функциональная структура CEM – комплекса представлена на рис. 1.

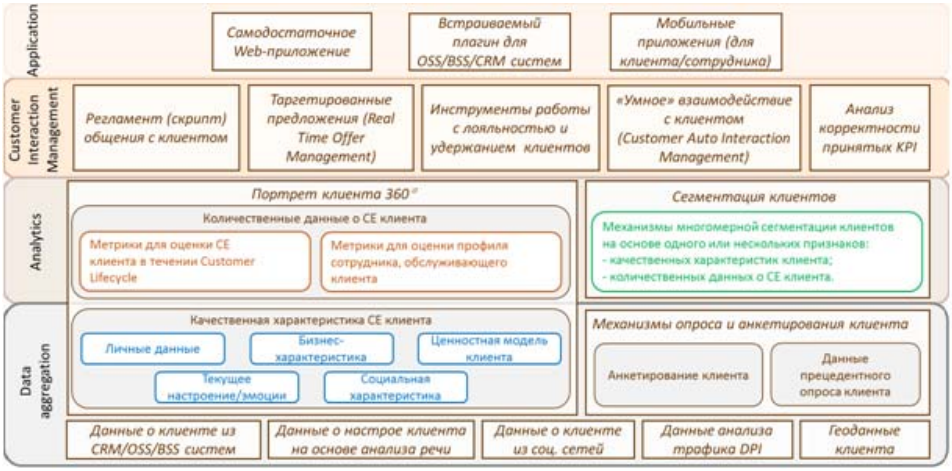


Рис. 1. функциональная структура CEM – комплекса

Data Aggregation – уровень агрегации данных реализует различные механизмы получения информации о клиенте и обработки полученной информации.

Analytics – уровень анализа. На уровне анализа строятся аналитические метрики, которые позволяют оценить уровень CE клиента и его удовлетворенность от используемого сервиса.

Customer Interaction Management – уровень взаимодействия с клиентом реализует инструменты и прикладные механизмы, которые позволяют отлеживать CE и влиять на него, на основе полученных данных при каждом взаимодействии клиента с компанией.

Application – уровень приложений определяет, в каком виде будут представлены инструменты, реализующие на предыдущих уровнях, конечному пользователю.

Второй подход – реализация концепции CEM, как набора инструментов к существующим решениям. Данный подход потребует доработок в различных системах OSS/BSS комплекса оператора, что усложняет их поддержку и функционирование [1]. При внедрении CEM, как набора инструментов выделяют такие подсистемы как:

1. CAIM (*Customer Auto Interaction Management*) – подсистема управления «умным» автоматизированным взаимодействием с клиентом.

2. CEM – FB (*Customer Experience Management – Feedback*) – подсистема сбора прецедентной обратной связи. Решения, реализуемые с помощью данной подсистемы, направлены на изучение мнения клиента о разных аспектах взаимодействия с компанией на различных этапах жизненного цикла.

3. CEM–метрики. Подсистема, позволяющая стоить многомерную аналитику CE на основе данных из других систем. Помимо стандартных метрик клиентского опыта (NPS, CSI, FCR) существует возможность рассчитывать метрики, стандартизованные TM Forum.

4. CEM-Sales&Targeting – подсистема событийной поддержки продаж на основе знаний CE и продуктовой линейки компании. Решения, реализуемые с помощью этой подсистемы, направлены на поддержку продаж в рамках различных ситуаций взаимодействия сотрудников компании с клиентом.

5. Скрипт взаимодействия с клиентом. Подсистема позволяет построить процесс общения сотрудника компании и клиента за счет регламента, который формируется на основе портрета клиента, его текущего отношения к компании и конкретной ситуации.

Данные инструменты и плагины можно внедрить в проекции на процессы, которые определены в группе Assurance. Рассмотрим процесс от регистрации клиентского инцидента до закрытия, последовательность процесса представлена на рис. 2.

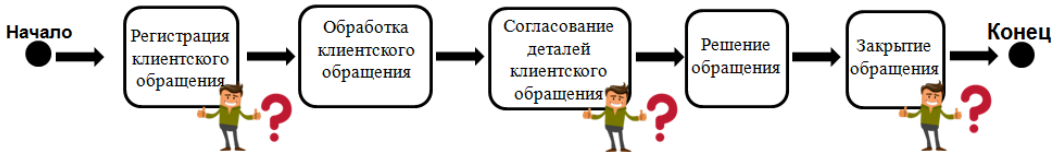


Рис. 2. Процесс у оператора связи

В рассмотренном процессе выделено три точки взаимодействия с клиентом, в этих точках можно применить рассмотренные выше инструменты (рис. 3). Используя эти инструменты, оператор сможет отслеживать, анализировать и влиять на СЕ.

Рис. 3. Применение инструментов концепции CEM в процессе оператора связи

Стоить отметить, что внедрение CEM, как набора инструментов является менее трудоемкой задачей, но такая реализация не позволит использовать весь функционал CEM.

В заключении хотелось бы сказать, что при внедрении концепции CEM в среду современного оператора связи компания сможет построить персонализированный подход к каждому клиенту, снизить стоимость клиент-ориентированных транзакций, получить сверх выгоду в рамках каждого клиентского события, а также превзойти ожидания клиента от предоставляемого сервиса и компании в целом. В свою очередь, внедрение подобного CEM – комплекса в среду оператора связи дает бесспорное конкурентное преимущество на современном рынке телекоммуникаций.

Список используемых источников

1. Акишин В. А., Кисляков С. В., Феноменов М. А. Функциональная архитектура CEM-комплекса для внедрения в IT-ландшафт крупного оператора связи // T-Comm: Телекоммуникации и транспорт. 2016. Том 10. № 10. С. 12–16.

2. Самуйлов К. Е., Чукарин А. В., Яркина Н. В. Бизнес-процессы и информационные технологии в управлении современной инфокоммуникационной компанией. М. : Альпина Паблишер, 2016. 515 с.

3. TM FORUM. GB929. Application-framework. (TAM) R16.5 TM Forum; October 2016.

УДК 65.011.56

ИССЛЕДОВАНИЕ МОДЕЛЕЙ ВЗАИМОДЕЙСТВИЯ ОПЕРАТОРА СВЯЗИ И IOT

С. В. Кисляков, Н. С. Плетнева

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

В статье рассматриваются модели коммуникации IoT, основные модели взаимодействия оператора с окружением интернет вещей, приводится анализ их особенностей на основе рассмотрения существующих методологий рынка Интернет вещей. Актуальность данной темы обусловлена стремительным ростом популярности различных «умных» устройств, подключенных к Интернету, и отсутствием процессов и основной бизнес-модели на рынке Интернет вещей.

Интернет вещей, IoT, оператор связи, бизнес-модель, монетизация, QoS.

Интернет вещей расширяет привычное представление об Интернете за счет применения новых подключений между «умными» вещами, пользователями и вещами, ЦОД и вещами [1]. Глобальная сеть Internet of Things охватывает огромное количество компонентов: линии связи, сетевые шлюзы, маршрутизаторы, IoT-платформы, взаимодействие которых возможно благодаря многообразию стандартов и протоколов [1].

Разная пропускная способность, разный уровень подключения и разные типы устройств – всё это разнообразие вариантов использования соединенных устройств требует особенных запросов на подключение, которым не свойственны универсальные способы эксплуатации [1].

К тому же сегодня еще не найден общий язык общения IoT-устройств, но существует множество платформ и стандартов, конкурирующих между собой.

Несмотря на это, IoT рынок стремительно растет и развивается. Аналитики Gartner подсчитали, что к концу 2017 г. по всему миру будет насчитываться 8,4 млрд. подключенных к сети устройств. По сравнению с прошлым годом их количество вырастет на 31 %. Предполагается, что к 2020 г. число IoT-устройств достигнет 20,4 млрд штук. По итогам 2017 г. объем рынка Интернета вещей в денежном выражении составит 1,7 трлн долл. против 1,4 трлн долл. в 2016 г. [2].

Таким образом, от Интернета вещей ожидают, как минимум, удвоения прибыли всего ИТ-рынка.

– Сегодня IoT активно продвигают по всем информационным каналам. Но несмотря на это, он все еще не растет стремительными шагами и не забрал с рынка сколько-нибудь существенную часть возможной прибыли, обозначенной ранее.

Есть ряд проблем, возникающих перед «интернетизацией» вещей [1, 2, 3]:

– Разнообразие.

Стандартизация интерфейсов, к которым могут подключаться все соединенные «вещи», – чрезвычайно трудная задача. «Вещи» интегрируются с разнообразными платформами и приложениями, а также с физическими «вещами», что требует конкретной бизнес-логики.

Трудность разработки бизнес-модели для IoT состоит из-за множества различных типов подключенных объектов и устройств и отсутствия единых стандартов.

– Незрелость инноваций.

Незрелость относится к текущему «беспорядку» новых компонентов и технологий. На сегодняшний день основу IoT составляют еще не созревшие и не стандартизированные продукты и услуги, большинство из которых имеет модульную структуру, поэтому требуют дополнительных инженерных работ для интеграции в области приложений.

– Неструктурированная экосистема.

Отсутствие определенных базовых структур и управления, роли заинтересованных сторон и логики также влияют на несогласованность в регулировании бизнеса и трудность создания бизнес-модели.

Но все же сегодня уже существуют определенные бизнес-модели, согласно которым функционирует рынок IoT.

Многие из моделей рассчитаны на распространение продуктов бесплатно и получение прибыли в отдаленном будущем.

Для монетизации операторам предлагается воспользоваться несколькими моделями, а именно:

1) Модель превращения оператора в «трубу» [3]:
   - тарификация за трафик или за подключение IoT-датчиков к сети:
     - ✓ тариф за разовое использование;
     - ✓ лимитный тариф;
     - ✓ оплата за результат;
   - тарификация upfront за подключение к услуге IoT, без привязки к периоду, на все время жизни датчика.
2) Модель превращения оператора в «умную трубу»:

– тарификация не только объема трафика IoT, но и управляемых качественных характеристик, таких как гарантированная доступность необходимой емкости канала с возможностью его динамического изменения, задержка сигнала, джиттер и др.

3) Модель «оператор не труба»:

– эффективным решением проблемы монетизации IoT для оператора и сервис-провайдера может стать формирование экосистемы взаимодействующих между собой сервисов, создающих добавленную стоимость
– еще одной перспективной моделью для оператора может стать модель реселлера с созданием добавочной стоимости путем обеспечения характеристик QoS, напрямую зависящих от сети

Самым простым способом монетизации рынка IoT является тарификация за трафик или подключение. Это связано с тем, что на сегодняшний день основной двигатель IoT – это операторы связи.

Но при такой модели бизнеса возникает ряд дополнительных вопросов, требующих определенных затрат (правильная установка, аутентификация датчиков, биллинг и проч.), что сильно тормозит массовое внедрение IoT-решений.

Также на протяжении нескольких последних лет просматривается тенденция распространения интересов оператора во всех звеньях цепочки создания стоимости на IoT-рынке.

Однако такая бизнес-модель утратила себя и уже не может развиваться в существующем виде. Это требует пересмотра стратегий операторов в области IoT и трансформации их бизнеса.

«Распад» цепочки ценности предоставит новые возможности для операторов. Операторы смогут концентрироваться на определенном виде деятельности (например, обеспечение безопасности или решения для управления оборудованием), а не выбирать: предоставлять исключительно услуги связи или цельного конечного решения для различных вертикалей рынка [4].

За Интернетом вещей будущее. Крупные ИТ-компании мира конкурируют между собой в создании наиболее универсальных IoT-платформ, сервисов и устройств. Интернет вещей повсюду. Ежедневные новые подключения девайсов вызывают дополнительную нагрузку на сети. Наблюдая за данным процессом, операторы понимают, что при наличии необходимой инфраструктуры, программного обеспечения и клиентов в ближайшем будущем направление IoT займет лидирующие позиции в телеком-индустрии [5]. Поэтому так важно разработать стандарты, предусмотреть новые способы ведения бизнеса и найти работающую бизнес-модель.

Список используемых источников

1. Роуз К., Элдридж С., Чапин Л. Интернет вещей: краткий обзор // The Internet Society (ISOC) 2015.
2. Райли Д., Кринер М. NGOSS: построение эффективной системы поддержки и эксплуатации сетей для операторов связи : пер. с англ. М. : Альпина Бизнес Букс, 2007. 192 с. ISBN 978-5-9614-0632-0.
3. 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.
4. Internet Society. [Электронный ресурс]. – Режим доступа: https://www.internetsociety.org/iot (дата обращения 15.03.2017).
5. IoT [Электронный ресурс]: – Режим доступа: https://iot.ru/ (дата обращения 02.03.2017).

УДК 004.046

ФОРМИРОВАНИЕ ТРЕБОВАНИЙ К ФУНКЦИОНАЛЬНОСТИ СОВРЕМЕННОЙ СИСТЕМЫ УПРАВЛЕНИЯ НЕИСПРАВНОСТЯМИ НА СЕТЯХ СВЯЗИ

С. В. Кисляков, В. В. Савич

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

С развитием инфокоммуникационных технологий с одной стороны и с ростом конкуренции среди операторов связи с другой, решение задачи управления неисправностями на сетях Fault Management требует новых подходов, а, следовательно, возникают новые функциональные требования к функциональности FM-систем.

В статье приведены результаты анализа стандартизованных ассоциацией TM Forum программных и бизнес-функций FM, обозначены новые проблемы в управлении неисправностями. На основе анализа сформулированы требования к функциональности современной FM-системы.

На основе выполненного анализа и выявленных требование к системе, предложена к обсуждению функциональная архитектура комплексной системы FM. Также, предложены варианты развития системы для повышения качества управления неисправностями.

Fault management, устранение неисправностей, проактивный мониторинг, функциональная модель.

Задача поддержки работоспособности сетевого и ИТ-оборудования и услуг связи является одной из ключевых в работе оператора связи. Традиционно работы по устранению неисправностей начинаются после обращения пользователя или сигнала соответствующей подсистемы. То есть оператор связи реагирует на информацию о проблеме/инциденте постфактум.

К сожалению, для обслуживания крупной сети такой реактивный (постфактум) подход во многих случаях оказывается недостаточно эффективным: в какой-то момент количество сообщений о неисправностях начнёт увеличиваться лавинообразно, что приведёт (вероятно) к отказу критичных сетевых сервисов. Такой подход несёт ещё один «минус», заключающийся в том, что клиент «видит» сбой, он о сбое знает, а это отчасти снижает рейтинг оператора связи в глазах клиента.

Исходя из сказанного, требуется найти решение, позволяющее эффективнее поддерживать работоспособность сетевых ресурсов и при этом минимизировать информированность клиента о сбоях. Последнее предполагает следующее: нужно спрогнозировать сбой/аварию и устранить источник или результат без участия клиента, чтобы клиент даже не знал о случившейся проблеме.

Существуют определённые модели (FCAPS, ITIL, TMN и т. д.), описывающие задачу поддержки IT-инфраструктуры в целом или сетевой инфраструктуры в частности. Рекомендуется использовать такие модели как базовые и необходимые в ИТ-комплексе оператора, в которых система управления неисправностями и методы мониторинга являются одними из ключевых компонентов.

В документации TM Forum [1, 2, 3] описывается набор рекомендованных функций, «опорных точек» для начала разработки Fault Management (FM-система) и характеризуется как реактивная система (рис. 1), то есть система, которая начинает обрабатывать сигнальное сообщение, поступившее от оборудования только в момент попадания его в систему. Решение проблем (реакция) начинается, когда они уже возникли и были оценены администратором (анализ).

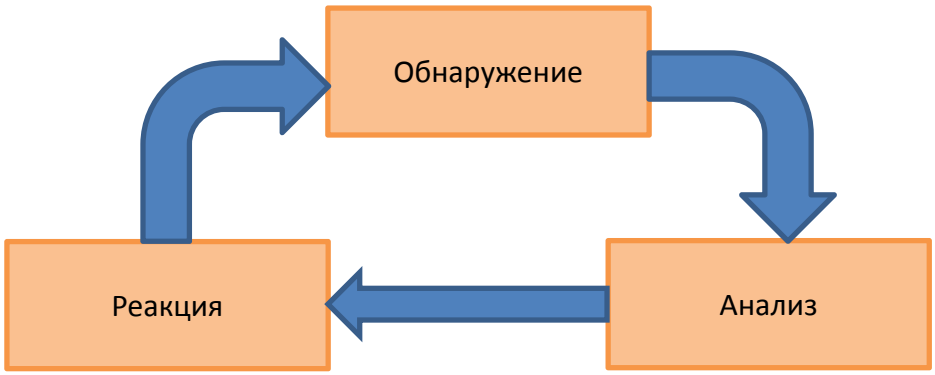


Рис. 1. Реактивная система Fault Management (по TMF)

Ниже приведен краткий перечень рекомендованных TM Forum функций базовой системы FM:

1. Основные функции управления сигнальными сообщениями:

1.1. Сбор сигнализационной информации, поступающей из сети.

1.2. Визуализация в виде информационных сообщений для последующего анализа оператором.

2. Пассивный подход мониторинга:

2.1.Получение сообщений о событиях.

2.2.Группировка сигнальных сообщений.

3. Ведение истории событий и логирование.

4. Информирование диспетчеров о неисправности.

Наличие такой системы, несомненно, упрощает работу сетевого инженера. Однако, что происходит за время, прошедшее от факта поломки оборудования до окончательного восстановления работоспособности элемента сети? В течение этого времени оборудование простаивает, ухудшается качество услуги или она полностью отсутствует. Оператор несет убытки, снижается уровень лояльности клиента, которые сам начинает обращаться к оператору по проблеме.

Уйти от описанных проблем реактивного подхода можно, если реализовать подход проактивного мониторинга, сделав его частью комплекса FM-комплекса. При таком подходе система сможет отыскать возможные и самые незначительные неполадки, которые способны стать причиной (или потенциальной причиной) отказа работоспособности и своевременно перераспределить ресурсы сети.

Проактивный мониторинг следует теперь рассматривать как основной инструмент поддержки корпоративных сетей, благодаря которому становится возможным оперативное определение и устранение причин возникающих неполадок, прогнозирование поведения системы и выявление «слабых» мест, а также грамотное распределение системных ресурсов сети.

В результате расширения функциональности FM проактивным мониторингом – комплексная система (рис. 2, 3) должна представляет собой набор функций, которые обнаруживают, коррелируют и диагностируют неисправности в телекоммуникационной сети, осуществляют хранение отчетной информации в базе знаний событий. Работа такой системы должна сопровождаться проведением последовательных диагностических тестов, исправлением ошибок, фиксированием условий и сохранением информации о причинах их возникновения, а также локализации и отслеживания неисправностей. При возникновении неисправности или каком-либо событии, сетевое устройство будет посылать уведомление диспетчеру для информации.

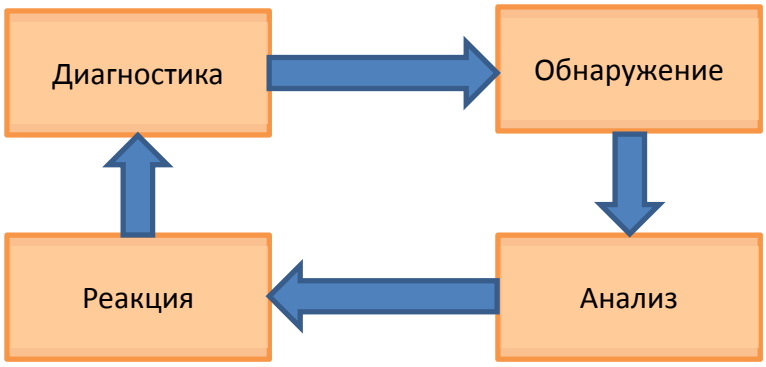


Рис. 2. Функциональная модель комплексной системы управления неисправностями

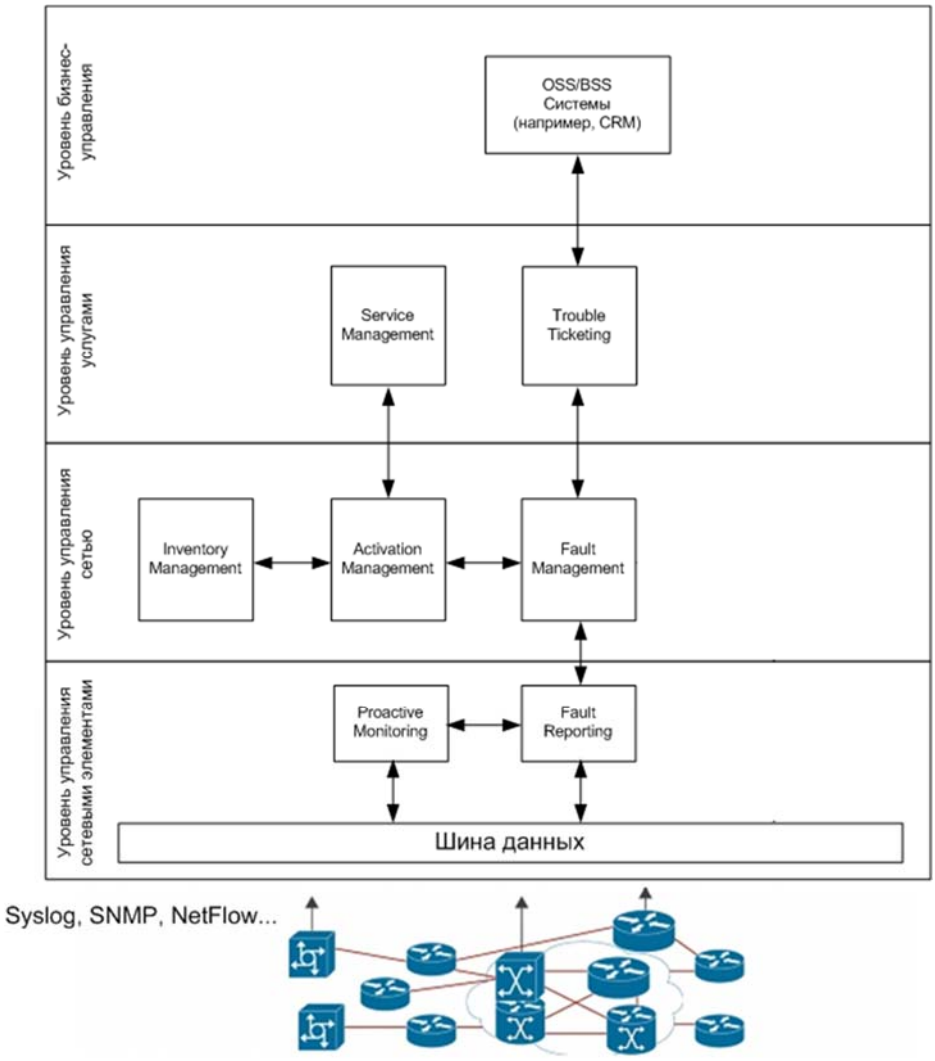


Рис. 3. Информационная архитектура взаимодействия систем комплексной FM-системы

Опираясь на представленную выше функциональную архитектуру взаимодействия систем, важно отметить, что FM-системы имеет возможность как ручной регистрации (например, с помощью системы *Trouble ticketing*, по обращению клиента, зарегистрированному в CRM), так и автоматиче-

ской, путем сбора информации с сетевого оборудования. Рассмотрим процессы детально. Если представить источники обмена сетевой информацией, как единую шину данных, то все сигнальные сообщения, поступающие с нее в комплексную систему управления должны быть обработаны FM и отсеяны ошибки.

Проактивный мониторинг (*Proactive monitoring*) несет важную, но все-же вспомогательную роль в регистрации предупреждений о возможных авариях. Система должна обнаруживать причины, которые могут привести к возможным неисправностям оборудования с помощью выполнения диагностических тестов. Если тесты не предусмотрены в программном обеспечении производителя оборудования, то типы и сценарии тестирования должны быть определены и разработаны инженерами поддержки сети.

Интеграция с системами класса Inventory (учет ресурсов, IM) и Activation management (активация ресурсов и услуг, AM) должна давать возможность выделять поврежденное оборудование для дальнейшей оценки зоны повреждения, поиска, затронутого аварией другого сетевого оборудования и услуг, к которым нарушен доступ.

Вся информация о неисправностях (по итогу проделанных операций в системах *inventor*y и *activation*) должна быть повторно обработана и классифицирована в FM и затем передана в систему учета событий Trouble ticketing, где специалисты смогут оценить неисправность (или предупреждение, поступившее от системы проактивного мониторинга) и принять решение об ее устранении.

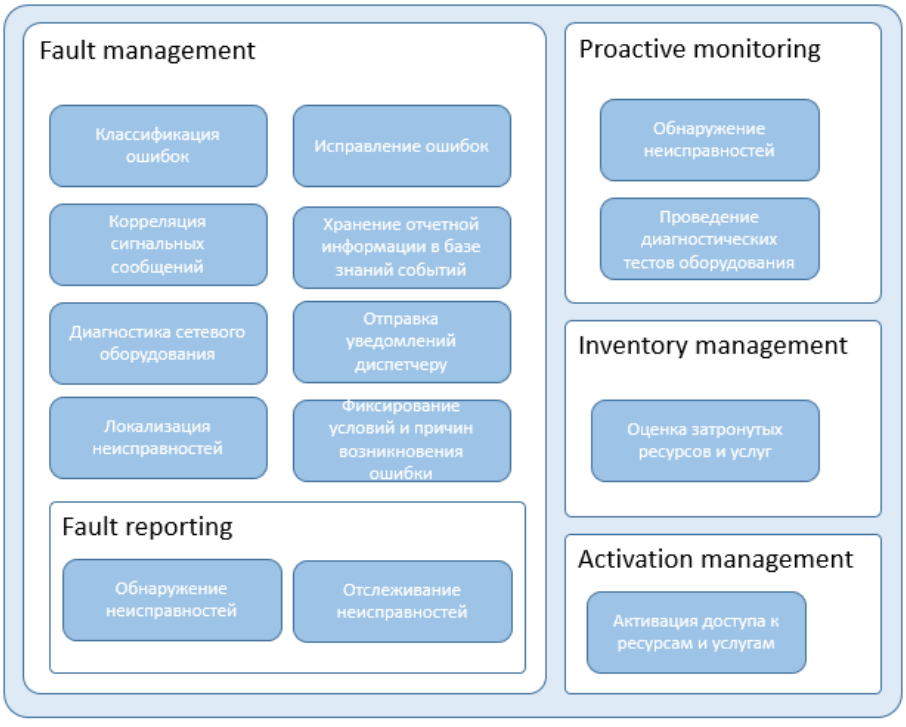


Рис. 4. Функции комплексной системы управления неисправностями

После устранения неисправности на оборудовании данные о проведенных диагностических тестах должны быть собраны FM и зафиксированы в системе учета событий в виде отчета с целью ведения истории и передачи на последний этап жизненного цикла события (от возникновения сообщения о неисправности до подтверждения об устранении). Оператором системы управления выполняется подтверждение о решении проблемы, доступ к услугам, попавшим в зону аварии, должен быть активирован системой AM.

Качество комплексной системы управления неисправности (рис. 4) во многом зависит от систем проактивного мониторинга.

Предложенная система мониторинга позволит предотвращать отказы сетевого оборудования и избегать лишних затрат – как денежных, так и временных. Такой мониторинг гарантирует долгосрочную службу сети и стабильный доступ к ее услугам.

Список используемых источников

1. 3GPP SA5 – TM Forum TIP Fault Management Harmonization : TR183, TM Forum, май 2013. Версия 1.3. 44 с.

2. End-to-end Virtualization Management: Impact on E2E Service Assurance and SLA Management for Hybrid Networks : IG1127, TM Forum, май 2015. Версия 15.0.0, 23 с.

3. Resource Trouble Management (RTM) - DDP BA : TMF518_RTM, TM Forum, сентябрь 2011. Версия 1.2, 87 с.

УДК 004.056

ПРОЕКТИРОВАНИЕ И РЕАЛИЗАЦИЯ ПРОТОТИПА СИСТЕМЫ ЦЕНТРАЛИЗОВАННОГО СБОРА, ХРАНЕНИЯ И ОБРАБОТКИ СИСТЕМНЫХ ЖУРНАЛОВ

С. А. Кобзев, А. А. Кулешов, И. А. Ушаков

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

В статье рассмотрены технологии и архитектурные решения, на основе которых разработан программный прототип системы сбора, хранения и анализа телеметрических данных различных компонентов информационных систем, а также по сформировавшимся критериям для характерной технической задачи проведен сравнительный анализ с решениями сторонних производителей.

Elastic Stack, Elasticsearch, Logstash, Kibana, сравнительный анализ систем сбора, хранения и анализа системных журналов.

В современных информационных системах постоянно растет количество подключенных к сетям устройств, увеличивается сложность сетевых топологий, в связи с этим все более актуальной становится задача контроля и мониторинга событий различного характера в информационных системах для оперативного решения проблем безопасности, и выявления потенциально уязвимых мест в части параметров обслуживания, а также ошибок в конфигурации системы. Особенно актуальна тематика определения аномалий и корреляционного анализа на множестве системных событий для проактивного выявления событий нарушения информационной безопасности. Для решения обозначенных задач применяются различные системы сбора, хранения и анализа данных системных журналов и телеметрических данных от различных источников – технических и программных средств информационных систем.

К прототипу системы сбора и аналитики данных, используемому для целей исследования моделей и алгоритмов определения событий безопасности, предъявляются следующие основные технические требования:

1) Гибкость системы в части источников данных, обеспечиваемая за счет модульной архитектуры (возможность обеспечить сбор информации от различных источников для централизованного анализа и мониторинга).

2) Эластичность системы – распределением нагрузки (предпочтительно использование внешних стандартных сервисов распределения нагрузки).

3) Поддержка развитого API и возможность эффективной интеграции собственных алгоритмов в движок аналитики Системы.

4) Минимизация операционного времени на развертывание и настройки инфраструктуры, сервисов и других системных задач, не относящихся к предмету исследования.

5) Реализация механизмов отказоустойчивости и высокой доступности на программном уровне (предпочтительно микросервисная архитектура, обеспечивающая удобную контейнеризацию/виртуализацию).

6) Поддержка горизонтального масштабирования для компонентов и системы в целом.

7) Распространенность на рынке и активное сообщество пользователей.

Для решения поставленной задачи был проведен анализ существующих на современном рынке коммерческих и открытых решений.

Одним из наиболее популярных решений подобного рода является коммерческий программный продукт Splunk Enterprise [1]. Данный продукт – платформа операционной аналитики для сбора и анализа машинных данных, основанный на парадигме MapReduce с автоматической балансировкой нагрузки. Такой подход дает возможность наращивать производительность за счет добавления типовых серверов, что обеспечивает горизонтальную

масштабируемость и отказоустойчивость системы. Имеет документированный RESTful API и SDK для популярных языков. Платформа обрабатывает данные любого формата. Splunk является коммерческим продуктом, с закрытым исходным кодом, что ограничивает и замедляет развитие API и делает масштабирование системы платным.

Еще одно распространенное коммерческое решение – ManageEngine EventLog Analyzer [2], имеющее схожие достоинства и недостатки решения конкурента – Splunk Enterprise. Продукт EventLog Analyzer поддерживает распределение нагрузки с использованием внутреннего сервиса. Алгоритмы, методы и основа платформы не доступны на программном уровне, а вся настройка и работа производится с помощью API, который развивается исключительно ManageEngine в зависимости от нужд платежеспособного потребителя, что уменьшает гибкость системы.

В 2014 г. компания Cisco Systems опубликовала исходный код решения OpenSOC – основанное на экосистеме Apache Big Data open source решение для создания собственного центра мониторинга киберугроз [3]. К сожалению, адаптированная под задачи high-load архитектура решения Apache Metron имеет свойство плохого обратного масштабирования – для построения простейшей системы (например, для задач обучения, как в нашем случае) необходимо развертывание большого количества компонентов системы и ресурсоемких сервисов, которые не будут использоваться. В условиях задач и среднестатистических ресурсов учебного прототипа просто невозможно обеспечить загрузку данными от источников, под которую рассчитано данное решение, одновременно с этим компоненты решения требуют достаточно много человеческих ресурсов на развертывание и конфигурирование. Безусловно проект Apache Metron заслуживает внимания в случае необходимости решения задач, ориентированных именно на обслуживание высоконагруженных и распределенных информационных систем.

Одним из самых производительных из открытых программных продуктов, специализирующихся на решении обозначенных задач является Graylog [4]. Это бесплатная система централизованного сбора, хранения и анализа информации часто используемая в среде DevOps команд.

В 2016 г. разработчики продукта объявили об отказе от компонента mongodb, необходимого для хранения логов и настроек всей системы в целом. Произошло это из-за частых сбоев модуля и потреблении большого количества памяти. Было принято решение на смену mongodb использовать компонент Elasticsearch. Стоит учесть, что несмотря на частые обновления Graylog и развитое сообщество пользователей, интеграция актуальных версий Elasticsearch в проект требует много времени. Доказательство этому то, что на 2017 г. последняя версия Graylog 2.1.1 работает только с Elasticsearch версии 2.3.5, являющейся устаревшим.

Основываясь на результатах анализа имеющихся в индустрии средств был выбран комплекс программного обеспечения Elastic Stack [5].

Рассмотрены основные составляющие Elastic Stack, которые были использованы в проекте:

Elasticsearch – распределенное, поисковое и аналитическое ядро системы, поддерживающее архитектурный стиль REST API и передачи данных через JSON. Централизованно хранит поступающие в него данные. Поддерживает кластерную архитектуру, позволяя безболезненно масштабировать систему. Ядро Elasticsearch выполняет в реальном времени поиск по большим объемам разнотипных структур данных – документов. Документ – базовая единица информации, которая может быть индексирована. Документы выражаются в JSON формате. Имеет развитый API, в список поддерживаемых языков для взаимодействия входят: Java, Python, .NET, Groovy, JavaScript, PHP и многие другие популярные языки.

Logstash – программный конвейер обработки данных, одновременно собирает данные из множества различных источников, первично обрабатывает их, и отправляет в подсистему хранения. Имеет встроенный синтаксический анализатор, позволяющий нормализовать разнотипные данные, производить определение географических координат по IP, обрабатывать информацию различных источников, в независимости от формата и структуры.

Kibana – программный компонент, реализующий функционал визуализации и навигации в комплексе ПО Elastic Stack. Представляет данные в виде настраиваемой интерактивной панели индикаторов в реальном времени. Реализует большое количество встроенных настраиваемых виджетов – гистограммы, графы, карты и другие стандартные инструменты. Имеет развитый API.

Beats – набор программ коллекторов данных с низкими требованиями к ресурсам, устанавливаемых на клиентских устройствах для сбора системных журналов и файлов. Имеется широкий выбор коллекторов, а также возможность написать свой коллектор.

Прототип разрабатывается с целью в будущем быть базой SIEM системы, поэтому необходимо обеспечить широкий охват доступной информации для анализа. На данный момент поддерживается сбор событий протокола syslog, журналов событий Windows, телеметрии оборудования, ОС и сервисов, а также информации о потоках сетевого трафика из протокола netflow/sflow, с помощью filebeat, winlogbeat, metricbeat, packetbeat соответственно [6]. В будущем, при необходимости отправки специфичных данных, возможно написание собственных Beat-коллекторов на основе предоставленной библиотеки libbeat, и развитого API.

Для обработки и доставки данных в Elastic Stack используется конвейер Logstash. Он разделен на три основных функциональных блока (*plugins*): input, filter, output.

В функциональном блоке Input plugin указывается конкретный источник событий, который будет считываться Logstash конвейером.

Блок Filter plugin выполняет промежуточную обработку события. Это позволяет структурировать данные, извлекая только необходимую информацию, например, дату, время, IP-адрес, код ошибки и т. д. и сохраняя их в структуры данных, отправляет далее в output plugin для последующей передачи в Elasticsearch.

В Output plugin указывается дальнейший маршрут обработки документов в JSON-формате. Это окончательных этап конвейера. В прототипе данные передаются в подсистему аналитики и хранения – Elasticsearch.

Для обеспечения отказоустойчивости и доступности в прототипе, была дополнена выше приведенная схема.

При превышении скорости входящих событий над скоростью обработки данных конвейер Logstash начинает отбрасывать события. В случае реализованного прототипа подсистема конвейерной обработки на базе Logstash была разделена на два отдельных программных сервиса:

1) Сервис приема данных от источников событий beats, с последующей отправкой в буфер massage broker.

2) Сервис приема из буфера, дальнейшая обработка, и отправка в Elasticsearch.

Модуль Elasticsearch output plugin настроен на автоматическую балансировку нагрузки на множество узлов в Elasticsearch кластере. При отказе одного из узлов, поток данных не прерывается, что позволяет исключить единую точку отказа. Это обеспечивает высокую доступность кластера, и маршрутизацию трафика к активным узлам кластера.

Также в Elastic Stack есть возможность балансировки нагрузки между узлами системы, осуществляемая с помощью сервера nginx.

В прототипе был развернут кластер Elasticsearch. В терминологии Elastic Stack кластер представляет собой набор узлов (серверов), которые хранят в себе всю информацию и предоставляют возможность индексирования и поиска по всем узлам. В терминологии ELK Набор структур-документов, имеющих какие-либо похожие характеристики, называется индексом, используются стандартные подходы. Для удобства индексы разделяют на типы – документы имеющие общие поля.

Потенциально индекс может увеличиваться до больших размеров, превышающих физические возможности узла. Для решения этой проблемы индекс делят на несколько частей называемых осколками (*shards*). Это позволяет распределять данные на несколько узлов, а также распределить и распараллелить операции с осколками, что увеличивает производительность

и пропускную способность. Для предотвращения сбоев и обеспечения механизма отказоустойчивости, Elasticsearch позволяет делать копии осколков индекса, которые называются репликами. Осколок и его реплика никогда не располагаются на одном узле. Это также позволяет масштабировать поиск и пропускную способность, так как поиск происходит по всем репликам параллельно.

Kibana – это платформа для аналитики и визуализации, основанная на открытом исходном коде, разработанная специально для работы с Elasticsearch. Позволяет искать, просматривать и взаимодействовать с данными, хранящимися в индексах Elasticsearch. Обеспечивает возможность расширенного анализа и визуализации данных в виде различных графиков, таблиц и карт.

В статье приводится анализ современных решений, реализующих сбор, хранение и анализ системных событий и телеметрических данных, таких, как Splunk Enterprise, ManageEngine EvenLog Analyzer, GrayLog, Apache Metron и Elastic Stack. На основе критериев поставленной задачи, было выбрано решение Elastic Stack и на его базе реализован прототип системы для исследовательских целей. Способность данного решения собирать хранить быстро структурировать и анализировать данные любого типа, эластичность и программная расширяемость системы, предоставляют широкие возможности для дальнейшей разработки продуктов в сфере безопасности, мониторинга и контроля информационных систем [7]. Решение Elastic Stack имеет огромный потенциал, о чем свидетельствует его популярность в рамках индустрии.

Список используемых источников

1. Carasso D. Exploring Splunk. Splunk Inc., 2012 [Электронный ресурс]. URL: https://www.splunk.com/web_assets/v5/book/Exploring_Splunk.pdf (дата обращения 11.01.2017).

2. Quick Start Guide [Электронный ресурс] // ManageEngine Inc., 2017. URL: https://download.manageengine.com/products/eventlog/eventlog-analyzer-quickstart-guide.pdf (дата обращения 11.01.2017).

3. Дубровин Н. Д., Ушаков И. А., Чечулин А. А. Применение технологии больших данных в системах управления информацией и событиями безопасности // Актуальные проблемы инфокоммуникаций в науке и образовании. V Международная научно-техническая и научно-методическая конференция: сборник научных статей в 2 томах. СПб.: СПбГУТ, 2016. Т. 1. С. 348–353.

4. Graylog Documentation [Электронный ресурс] // Graylog Inc., 2017. URL: https://media.readthedocs.org/pdf/graylog2-docs/1.0/graylog2-docs.pdf (дата обращения 11.01.2017).

5. Gormley C., Tong Z. Elasticsearch: The Definitive Guide. Y O'Reilly Media, 2015.

6. Lightweight Data Shippers [Электронный ресурс] // Elastic Inc., 2017. URL: https://www.elastic.co/products/beats (дата обращения 11.01.2017).

7. Андрианов В. И., Красов А. В., Липатников В. А. Иновационное 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.

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

УДК 003.056

О НЕКОТОРЫХ ОСОБЕННОСТЯХ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

А. В. Козачок, Е. В. Кочетков

Академия Федеральной службы охраны Российской Федерации

В последнее время вопросы защиты информации, обрабатываемой на объектах критической информационной инфраструктуры, становятся все более актуальными. В настоящей работе рассмотрены основные нормативно-правовые акты, регламентирующие требования по обеспечению безопасности обработки информации для таких объектов, также некоторые особенности реализации мер защиты информации объектов критической информационной инфраструктуры применительно к системам реального времени.

критическая информационная инфраструктура, информационная безопасность.

На текущем уровне научно-технического прогресса невозможно представить дальнейшее развитие общества и государства без повсеместного внедрения информационных технологий во все сферы государственного управления и жизнеобеспечения общества, в том числе и при построении автоматизированных систем управления технологическими процессами (АСУ ТП).

Сложность сопровождения и модернизации существующих АСУ ТП, построенных на основе проприетарных протоколов и технологий, требует унификации и стандартизации используемых решений. При этом внедрение информационных технологий без рассмотрения вопросов информационной безопасности приводит к появлению ранее неизвестных угроз.

Глобализация информационно-вычислительных сетей позволяет удаленно оказывать влияние на элементы сетевой инфраструктуры, к которой

можно отнести современные АСУ ТП, то есть становится кибероружием, способным нарушить нормальное функционирование объектов критической инфраструктуры не только в информационной сфере, но и в реальной жизни, что может привести к катастрофическим последствиям и даже гибели людей.

Защита критической информационной инфраструктуры (КИИ) государства относится к стратегическим целям обеспечения информационной безопасности в области государственной и общественной безопасности [1].

Согласно определению объектов КИИ, представленному в [2], все объекты можно разделить на две группы:

– информационные системы, информационно-коммуникационные сети органов государственной власти;

– информационные системы, информационно-коммуникационные сети, АСУ ТП, функционирующие в оборонной, топливной, атомной, ракетно-космической, горнодобывающей, металлургической, химической промышленности, области здравоохранения, транспорта, связи, кредитно-финансовой сфере.

Вопросы обеспечения информационной безопасности объектов первой группы в значительной степени проработаны, так как они непосредственно или косвенно касаются защиты конфиденциальной информации и государственной тайны. В то время как особое внимание к вопросам обеспечения информационной безопасности объектов второй группы стало уделяться относительно недавно после ряда инцидентов, связанных с нарушением нормального функционирования объектов под управлением АСУ ТП [3].

Основными законодательными актами, регламентирующими обеспечение безопасности КИИ в Российской Федерации, являются:

– Доктрина информационной безопасности Российской Федерации [1] (определяет национальные интересы в информационной сфере, к которым относится устойчивое и бесперебойное функционирование критической информационной инфраструктуры в мирное время, в период непосредственной угрозы и в военное время);

– Проект федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации» [2] (устанавливает организационные и правовые основы обеспечения безопасности критической информационной инфраструктуры Российской Федерации в целях ее устойчивого функционирования при проведении в отношении нее компьютерных атак, основные принципы государственного регулирования в указанной сфере, определяет полномочия органов государственной власти Российской Федерации. Затрагиваются вопросы централизованного мониторинга инцидентов информационной безопасности на объектах КИИ. Одним из важных

принципов обеспечения информационной безопасности критической информационной инфраструктуры является приоритет предотвращения компьютерных инцидентов перед устранением их последствий);

– приказ ФСТЭК России «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды» [4] (в этом документе устанавливаются требования к обеспечению защиты информации, на объектах КИИ под управлением АСУ ТП. Они определяют характеристики штатного режима функционирования, при котором обеспечивается соблюдение проектных пределов значений параметров выполнения целевых функций в условиях воздействия угроз безопасности информации, а также снижения вероятности незаконного вмешательства в процессы функционирования автоматизированных систем управления критически важных объектов.);

Следует также учитывать, что в АСУ ТП зачастую информация передается в режиме реального времени, предъявляются высокие требования по доступности и целостности [5]. Проведенный анализ требований по защите информации в автоматизированной системе управления [4] показал, что реализация ряда требований на практике может привести к потере доступности и нарушению штатного режима функционирования за счет применения средств:

– «Антивирусной защиты».

– «Обнаружения (предотвращения) вторжений».

Согласно описанию требований по антивирусной защите, средства антивирусной защиты (САВЗ) должны не только обеспечивать обнаружение любой информации, способной нанести вред АСУ ТП, но и соответствующим образом реагировать в случае ее обнаружения. В современных САВЗ используются методы сигнатурного, эвристического и поведенческого анализа. Все они принципиально не позволяют добиться полной защиты от вредоносных программ, таким образом, всегда существует вероятность как пропуска цели, так и ложного срабатывания. В качестве реакции САВЗ на обнаружение признаков вредоносного кода может быть, как оповещение оператора о подозрительной активности, так и полная блокировка процесса, поведение которого с точки зрения САВЗ является подозрительным или с высокой степенью соответствует вредоносной активности. При этом заблокированная программа может быть легитимной, к примеру, средством удаленного управления технологическим процессом, которая подверглась заражению вредоносным кодом. Блокирование такой программы может произойти в произвольный момент времени, а отсутствие доступа оператора

к управлению технологическим процессом может нарушить режим штатного функционирования АСУ ТП в целом.

Любые действия, направленные на несанкционированный доступ к ресурсам АСУ ТП или оказание на нее воздействий, должны быть не только обнаружены, но и обеспечена соответствующая реакция по их предотвращению в рамках обеспечения требования по обнаружению (предотвращению) вторжений. Поскольку применяемые в системах обнаружения вторжений (СОВ) механизмы определения аномального поведения аналогичны механизмам, применяемым в САВЗ, в таких системах также возможны ошибки первого и второго рода. В свою очередь, ответной реакцией СОВ на вторжение может быть блокирование:

– соединения;

– учетных записей пользователей;

– узла компьютерной сети.

При всех видах блокировки возможно закрытие каналов управления между программным обеспечением и оконечным технологическим оборудованием. Аномальная сетевая активность может быть вызвана как настоящим вторжением во внутреннюю сеть АСУ ТП, так и непредвиденными особенностями телекоммуникационного оборудования. То есть ложное срабатывание в СОВ может привести к потере доступности некоторых сегментов внутренней сети, что может повлечь нарушение штатного режима функционирования всей АСУ ТП.

Обеспечение безопасности КИИ является одним из стратегических направлений деятельности государства. Переход при проектировании АСУ ТП от проприетарных протоколов к открытым, а также интеграция в глобальные информационно-вычислительные сети создает новые угрозы информационной безопасности объектам критической инфраструктуры. При этом реализация некоторых предъявляемых мер защиты информации в АСУ ТП не всегда гарантировано обеспечивает непрерывность штатного функционирования технологического процесса и доступность циркулирующей информации. Ложные срабатывания средств обеспечения защищенности информационной инфраструктуры могут привести к нарушению свойств доступности в отношении всей АСУ ТП, что может привести к катастрофическим последствиям. В связи с этим требуется разработка новых подходов и методов, позволяющих обеспечить информационную безопасность в сетях АСУ ТП с учетом особенностей функционирования таких систем.

Список используемых источников

1. Указ Президента Российской Федерации от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации».

2. Проект Федерального закона N 47571-7 «О безопасности критической информационной инфраструктуры Российской Федерации».

3. Аналитический центр компании «Panda Security SL» Критическая инфраструктура: кибер-атаки на основы современной экономики [Электронный ресурс]. URL: http://www.pandasecurity.com/mediacenter/pandalabs/whitepaper-critical-infrastructure/ (дата обращения 07.03.2017).

4. Приказ ФСТЭК России от 14.03.2014 N 31 «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды».

5. Кондратенко А. А. ИБ в ключевых системах информационной инфраструктуры. От теории к практике // Connect! Мир связи: Наука. Бизнес. Управление. 2013, № 9.

УДК 004.021

ЭКСПЕРИМЕНТАЛЬНОЕ ИССЛЕДОВАНИЕ СТЕГОСИСТЕМЫ С ПЕРЕДАЧЕЙ СИГНАЛОВ ПО АУДИО КАНАЛУ В УСЛОВИЯХ ВНЕШНИХ ПОМЕХ

В. И. Коржик, И. В. Кропивко

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

Исследуется стегосистема с использованием эхо-сигналов с их передачей по аудио каналу в условиях внешних помех. Показано, что при адекватном выборе параметров стегосистемы вложенная информация может быть достоверно извлечена даже при условии присутствия внешних шумов (речь и музыка). Расстояние между передатчиком (мегафон) и приемником (портативный микрофон) может быть порядка 10–30 метров. Данный метод может быть использован для передачи секретной информации во время проведения собраний на открытом воздухе или для вложения цифровых «водяных знаков» для предотвращения пиратского копирования музыкальных работ.

стегосистема, эхо-сигналы, кепстральный анализ, акустические шумы.

Стеганография – это семейство методов, при помощи которых некоторая дополнительная информация погружается в основное сообщение (так называемое покрывающее сообщение) при сохранении хорошего качества покрывающего сообщения.

В работе были исследованы методы построения такой стегосистемы, параметры которой позволяли бы передавать скрытую информацию с помощью аудиосигнала через акустическую среду. Данную стегосистему можно

применять при передаче скрытой информации с помощью аудиосигналов, которые будут воспроизводиться с помощью мегафона. Также данный метод возможен для использования в качестве цифрового водяного знака с целью сохранения прав собственности на аудио продукцию, к примеру, на концертных выступлениях. Схема работы, исследуемой стегосистемы, изображена на рис. 1.

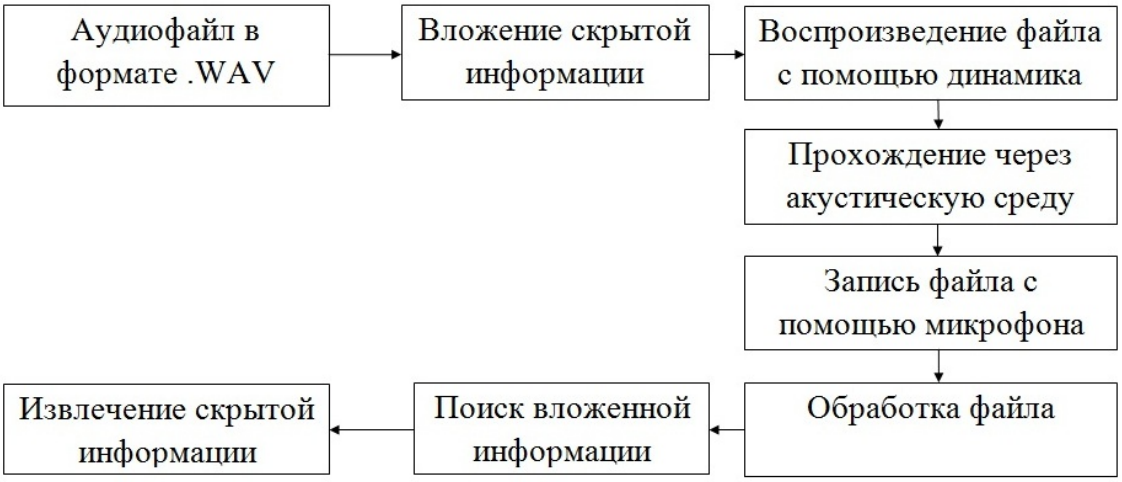
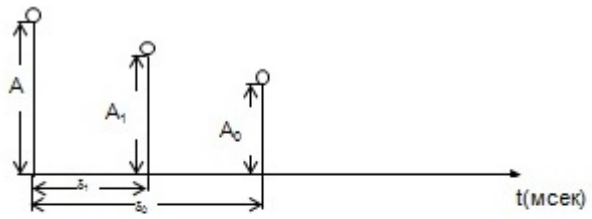


Рис. 1. Схема работы аудио стегосистемы

В качестве используемого метода вложения в исследуемой стегосистеме предлагается использовать метод, основанный на эхо-сигналах [1]. Он заключается в добавлении «эхо» (сдвинутого по времени сигнала) к основному аудио сигналу. При этом данная «добавка» воспринимается человеком не как добавление аддитивного шума, а как появление дополнительной звуковой «окраски» (рис. 2).



A – амплитуда исходного сигнала,
A_1 – амплитуда эхо сигнала, соответствующая вложению «1».
A_0 – амплитуда эхо сигнала, соответствующая вложению «0».
δ_1 – задержка эхо-сигнала, соответствующая вложению «1».
δ_0 – задержка эхо-сигнала, соответствующая вложению «0».

Рис. 2. Параметры вложения информации с использованием эхо-сигналов

В качестве метода обнаружения подобной стегосистемы предлагается использовать кепстральный метод приема [2]. Основная идея кепстрального анализа заключается в том, что свёртка двух сигналов ($x(n) = S(n) * h_b(n)$) соответствует сумме их кепстремов:

$$\tilde{x}(n) = \tilde{S}(n) + \tilde{h}_b(n), \quad n = 1,2,\ldots,$$

где $S(n)$ – исследуемый аудиосигнал, h_b – отклик фильтра на вложенный бит $b = (0,1)$, «~» – означает представление в виде кепструме.

При этом корреляционный прием сигналов, основанный на кепстреме, определяется следующей известной формулой:

$$\sum_n \hat{x}(n) \cdot \hat{h}_0(n) \underset{b=1}{\overset{b=0}{\gtrless}} \sum_n \hat{x}(n) \cdot \hat{h}_1(n).$$

Одним из ключевых факторов при выборе данного метода извлечения является тот факт, что в кепстральной области не имеет значения абсолютное значение амплитуды сигнала, которое меняется на протяжении всего сигнала и мешает выбрать порог для правила решения с использованием автокорреляционной функции [3].

В ходе исследования был проведен следующий эксперимент. В три различных аудиосигнала было произведено вложение с использованием эхо-сигналов с одними и теми же параметрами вложения (глубина вложения 0,9; задержка сигнала – 32 и 37 отсчетов; количество бит, использующихся для вложения одного информационного бита – 10000). Затем аудиосигнал проходил через акустическую среду, причем сначала в среде не было явных источников акустического шума, а затем они были добавлены согласно схеме, представленной на рис. 3. В качестве шумов использовались записи шума толпы и музыкального произведения.

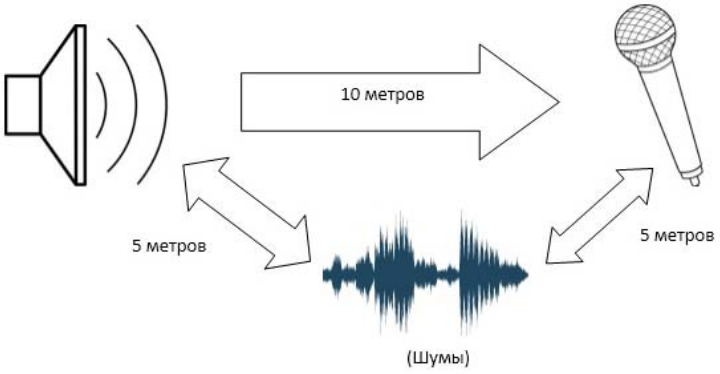


Рис. 3 Схема эксперимента с акустическими шумами

После прохождения акустической среды аудиосигнал с вложенной информацией подвергался кепстральному анализу. Результаты эксперимента

представлены в таблицах 1–3 (аббревиатуры в таблицах – музыкальные файлы: Champions League – CL, Queen We Are The Champions – QWATC).

ТАБЛИЦА 1. Результаты исследования при удалении источника и приемника на расстояние в 10 метров при отсутствии шума

Расстояние в 10 метров без помех	CL	QWATC	Pen
Вероятность ошибки (%)	0,4	2,8	2,8
Максимальный уровень сигнала (дБ) при приеме	–13,20	–9,68	–6,88
Среднеквадратичный уровень сигнала (дБ) при приеме	–36,12	–28,16	–26,58

ТАБЛИЦА 2. Результаты эксперимента при использовании шума толпы в качестве внешних помех

	CL	QWATC	Pen
Кол-во ошибок после акустической среды	3	15	12
Вероятность ошибки (%)	1,2	6	4,8
Максимальный уровень сигнала (дБ) при приеме	–10,10	–4,64	–7,18
Среднеквадратичный уровень сигнала (дБ) при приеме	–30,10	–25,24	–26,58

ТАБЛИЦА 3. Результаты эксперимента при использовании музыки в качестве внешних помех

	CL	QWATC	Pen
Кол-во ошибок после акустической среды	24	38	40
Вероятность ошибки (%)	9,6	15,2	16
Максимальный уровень сигнала (дБ) при приеме	–10,32	–7,18	–6,02
Среднеквадратичный уровень сигнала (дБ) при приеме	–32,60	–25,24	–24,08

Как видно из приведенных выше таблиц, при наличии источников внешних шумов происходит незначительное ухудшение достоверности приема сигнала. Также стоит отметить, что даже при наличии сильного акустического шума (табл. 3) для аудиосигнала, при обработке которого легче других происходит синхронизация, вероятность ошибки возросла незначительно, в то же время для других аудиосигналов достоверность приема оставалась на удовлетворительном уровне. Наиболее показательными являются результаты, приведенные в таблице 2, так как шумовой фон в этом случае считается наиболее приближенным к реальной ситуации – передаче информации в естественной среде, в людных местах. Как видно из таблицы 2, достоверность сигнала, несмотря на наличие шумов, остается на достаточно хорошем уровне.

Подводя итоги, следует отметить, что выбранная стегосистема, использующая вложение информации при помощи эхо-сигналов, подтвердила

свою состоятельность при удалении источника информации от приемника при отсутствии и наличии различного рода шумов на расстоянии в десять метров. Достоверность информации во всех исследуемых схемах эксперимента оставалась на удовлетворительном уровне. В дальнейшем планируется увеличить расстояние между источником и приемником сигналов до 30–50 метров.

Список используемых источников

1. W. Bender, D. Gruhl, A. Lu. Echo Hiding // Lecture Notes in Computer Science, 1996.

2. Коржик В. И., Алексеев В. Г., Федянин И. А. Выделение цифровых “водяных” знаков из аудиосигналов с использованием методов кепстрального анализа // 63 научно-техническая конференция профессорского-преподавательского состава, научных сотрудников и аспирантов: материалы ГОУВПО СПбГУТ. СПб., 2011. С. 225.

3. Donald G. Childers, David P. Skinner, Robert C. Kemerait. The Cepstrum: A Guide to Processing // Proceedings of IEEE, vol. 65, no 10. October, 1977.

УДК 531.76.081

КАЛИБРОВКА АНАЛИЗАТОРОВ СЕТЕВЫХ ПРОТОКОЛОВ ПУТЕМ ИЗМЕРЕНИЙ СКОРОСТИ ПЕРЕДАЧИ ИНФОРМАЦИИ В ОПТИЧЕСКОМ ТРАКТЕ

И. С. Королёв, К. Б. Савкин, Н. П. Хатырев

Всероссийский научно-исследовательский институт оптико-физических измерений

Рассмотрена возможность калибровки анализаторов сетевых протоколов путем прямых измерений скорости передачи информации в волоконно-оптических системах с синхронными форматами передачи. Проанализированы востребованность данного вида измерений и опыт ведущих производителей средств измерений. Исследованы погрешности, связанные с применением систем восстановления тактовой частоты для решения этой задачи.

волоконная оптика, волоконно-оптические системы передачи информации, SDH, СЦИ, бит в секунду.

Волоконно-оптические системы связи и передачи информации (ВОСПИ) являются наиболее востребованной технологией обмена цифровыми данными как в общегражданской, так и военной области. При разработке, испытаниях и эксплуатации ВОСПИ измерениям подлежит ряд параметров, характеризующих устойчивость их функционирования.

Одним из наиболее важных является скорость передачи информации (СПИ) [бит/с] [1]. Значения этой величины характеризуют коэффициенты ошибок и фазового дрожания при тестировании ВОСПИ [2].

Для измерений параметров ВОСПИ, в т. ч. СПИ, применяются специализированные средства измерений (СИ) – анализаторы протоколов, сетевые тестеры и др. Общее количество таких приборов, эксплуатируемых в настоящее время на территории РФ, оценивается объемом более 10 тыс. штук.

С технической точки зрения СИ данного вида представляют собой совокупность прецизионного генератора оптических сигналов, высокоточного измерительного приемника этих сигналов и ряда других устройств, набор которых меняется для различных типов СИ.

Метрологическое обеспечение рассматриваемого класса СИ параметров ВОСПИ в целом в Российской Федерации фрагментарно и не единообразно. Различные метрологические центры имеют разные взгляды как на набор метрологических характеристик анализаторов сетевых протоколов и других СИ, так и на место этих приборов в Государственной системе обеспечения единства измерений. Во многом причиной такой ситуации послужила многофункциональность анализаторов сетевых протоколов и большое количество чисто логических параметров информационного сигнала, отображаемых этими СИ. В большинстве случаев, в качестве метрологических характеристик в эксплуатационной документации указываются параметры сигналов на электрических интерфейсах плезиохронной цифровой иерархии (ПЦИ, PDH), низкоскоростных интерфейсах SDH и Ethernet. Для оптических интерфейсов нормируются средняя мощность выходного сигнала и чувствительность приемного тракта, в части динамических характеристик сигнала, как правило, задаются номинальные значения для поддерживаемых интерфейсов и пределы допускаемой относительной погрешности установки тактовой частоты передатчика.

Измерения СПИ получили широкое распространение в процессе тестирования высокоскоростных ВОСПИ с синхронной передачей данных, таких как синхронная цифровая иерархия (СЦИ) и Ethernet, которые являются в настоящее время основными для передачи больших массивов оцифрованной информации. Для работы данных ВОСПИ необходимо поддержание стабильного значения СПИ, единого для всех одноуровневых элементов системы. Тестирование проводится при строительстве новых линий, при их модернизации, а также в процессе устранения возникшего снижения пропускной способности.

Для сетей с синхронной передачей данных принят ряд номинальных значений СПИ в диапазоне от 100 Мб/с до 11 Гб/с, отраженный в соответствующих рекомендациях МСЭ-Т [3, 4, 5].

Измерения СПИ, а, следовательно, и метрологическое обеспечение таких измерений с помощью универсальных оптико-физических СИ невозможны. Основная проблема заключается в том, что используемые последовательности импульсов хотя и являются повторяющимися, но не являются периодическими.

Обеспечение единства измерений СПИ в Российской Федерации отсутствовало, несмотря на наличие большого парка СИ, разнообразие их марок и моделей. Де-факто многочисленность операторов, эксплуатирующих ВОСПИ и, зачастую, отсутствие унификации СИ нередко приводит к случайному сопоставлению различных приборов для измерений СПИ при выполнении операций тестирования ВОСПИ.

Учитывая то, что средства измерений СПИ имеют относительную погрешность измерений порядка от $1{,}5 \cdot 10^{-6}$ до $6 \cdot 10^{-6}$, для метрологического обеспечения таких измерений необходимо обеспечить погрешность воспроизведения не хуже $5 \cdot 10^{-7}$ на уровне Государственного первичного специального эталона.

Обеспечение единства измерений СПИ в волоконно-оптических системах возможно двумя основными путями:

1) воспроизведение эталонной последовательности оптических импульсов с высокой стабильностью СПИ;

2) прецизионные измерения СПИ последовательности оптических импульсов, генерируемой СИ.

В первом случае воспроизведение единицы должно осуществляться в виде псевдослучайной последовательности оптических импульсов (ПСП).

При использовании второго метода, передача единицы происходит посредством измерения СПИ сигнала, генерируемого СИ.

Авторами впервые в России предложено использовать для прямых измерений СПИ метод измерений тактовой частоты сигнала (информационного, либо тестового). По результатам проведенного анализа, для проведения исследований был выбран класс вспомогательных устройств – системы восстановления тактовой частоты (СВТЧ). Они производятся мелкими партиями и предназначены для синхронизации измерительного оборудования, например – стробоскопических осциллографов с измеряемым информационным сигналом. Поскольку системы восстановления тактовой частоты не аттестуются как СИ, то необходимо было провести исследования погрешностей преобразования с помощью СВТЧ оптико-физического информационного сигнала в периодический выходной сигнал, частота которого равна тактовой частоте. Численно значение тактовой частоты и СПИ совпадают.

В этой связи был проведен ряд экспериментов. На вход устройства восстановления тактовой частоты Agilent N4877A подавался сигнал с генератора импульсов, привязанного к рубидиевому стандарту частоты. Сигнал

представлял собой периодическую последовательность импульсов, имитирующую информационную последовательность интерфейса STM-1 СЦИ. Одновременно частота повторения импульсов указанной последовательности измерялась прецизионным частотомером. Сигнал восстановленной тактовой частоты с выхода N4877A поступал на второй канал частотомера. Измерялось значение отношения частоты повторения импульсов последовательности, формируемой генератором, и частоты сигнала с выхода СВТЧ. После чего сигнал с генератора импульса использовался для запуска генератора ПСП. Сформированная ПСП поступала на вход СВТЧ. Измерялось также отношение частот сигнала генератора импульсов и СВТЧ. Полученные результаты, приведенные в таблице, показали высокую точность и стабильность восстановления сигнала тактовой частоты СВТЧ. Таким образом, характеристики системы соответствуют требованиям для измерений СПИ в современных ВОСПИ.

ТАБЛИЦА. Результаты экспериментальных исследований

Номинальная скорость передачи информации, бит/с	51840000 (STM-0)	155220000 (STM-1)	622080000 (STM-4)
Отклонение от номинальной скорости, бит/с	0,007 ($1{,}35\cdot10^{-10}$)	0,03 ($1{,}93\cdot10^{-10}$)	0,14 ($2{,}25\cdot10^{-10}$)
Разброс значений скорости, бит/с	2,18 ($4{,}21\cdot10^{-8}$)	1 ($6{,}44\cdot10^{-9}$)	3,4 ($5{,}47\cdot10^{-9}$)
Среднеквадратическое отклонение (СКО), бит/с	0,035 ($6{,}75\cdot10^{-9}$)	0,09 ($5{,}8\cdot10^{-9}$)	0,53 ($8{,}52\cdot10^{-9}$)
Отклонение (девиация) Аллана, бит/с	0,033 ($6{,}37\cdot10^{-10}$)	0,09 ($5{,}8\cdot10^{-10}$)	0,48 ($7{,}72\cdot10^{-10}$)

Результаты экспериментов, проведенных с различными источниками ПСП (рабочими СИ СПИ и генераторами ПСП) демонстрируют высокую стабильность воспроизведения и измерений СПИ. Достигнутые значения погрешности измерений СПИ с помощью системы восстановления тактовой частоты (менее $3{,}5\cdot10^{-8}$) значительно меньше погрешностей, приписываемых наиболее точным рабочим СИ ($3\cdot10^{-6}$ и более [5]). Это позволило создать с использованием СВТЧ эталонную установку для воспроизведения и передачи единицы СПИ в ВОСПИ. Схема созданной установки приведена на рисунке.

Сигнал, формируемый источником импульсной последовательности, разделяется оптоволоконным делителем и поступает одновременно на оптический вход стробоскопического осциллографа и малошумящее фотоприемное устройство. Демодулированный электрический сигнал поступает на вход СВТЧ, сигнал с одного выхода которой используется для синхрони-

зации осциллографа, а с другого – на вход высокоточного частотомера, совмещенного с рубидиевым стандартом частоты. Таким образом, возможно одновременно с измерениями СПИ контролировать параметры глазковой диаграммы в соответствии с [4, 6].

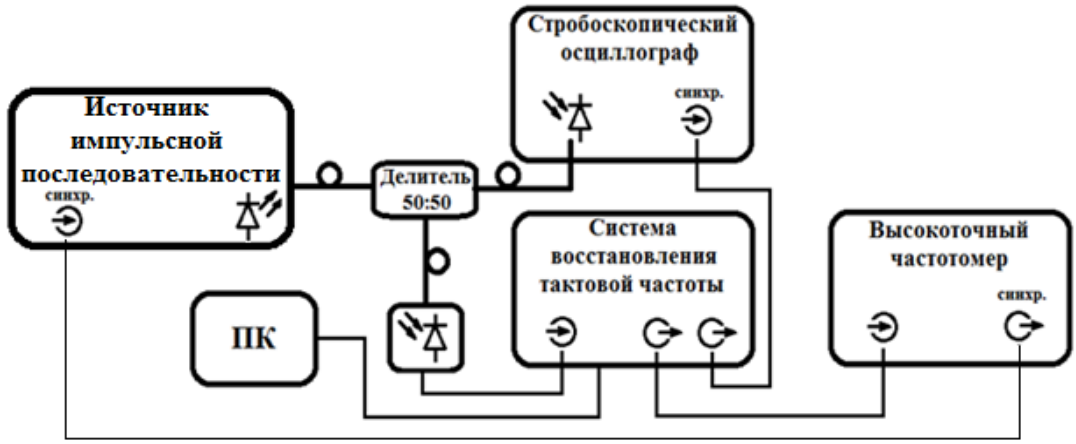


Рисунок. Схема эталонной установки
для измерений скорости передачи информации в ВОСПИ

В процессе проведения работ по усовершенствованию Государственного первичного специального эталона ГЭТ 90, созданная эталонная установка была включена в его состав. Указанные работы были приняты комиссией Росстандарта. Аппаратура воспроизведения и передачи единицы СПИ в оптическом тракте обеспечивает воспроизведение эталонных последовательностей импульсов с нормированными значениями СПИ, соответствующими основным форматам синхронной цифровой иерархии. Точные значения равны 155,520 Мбит/с; 622,080 Мбит/с; 2,488320 Гбит/с; 9,953280 Гбит/с. Аппаратура передачи обеспечивает передачу воспроизведенной единицы вторичным эталонам или высокоточным СИ. Аппаратура передачи представляет собой эталонное СИ СПИ, калибруемое с помощью аппаратуры воспроизведения единицы и обеспечивающее измерения СПИ в лазерных импульсных последовательностях, формируемых рабочим эталоном в диапазоне от 50 Мб/с до 11,5 Гб/с [7].

Учитывая размер территории и протяженность волоконно-оптических сетей Российской Федерации, проект поверочной схемы для СИ СПИ, предусматривает создание рабочих эталонов СПИ. В настоящее время уточняются технические требования на их разработку

Список используемых источников

1. Постановление Правительства РФ от 31.10.2009 № 879 «Об утверждении Положения о единицах величин, допускаемых к применению в Российской Федерации».

2. Dave M. Spirile, Andrew D. Ellis, Peter E. Barnsley. Optical Time Division Multiplexing Systems and Networks. IEEE Communication Magazine, December 1999.
3. IEEE 802.3: Ethernet.
4. ITU-T Recommendation G. 957. Optical interfaces for equipment and systems relating to the synchronous digital hierarchy.
5. Слепов Н. Н. Синхронные цифровые сети SDH. М. : Эко-Трендз, 1997. 148 с.
6. ITU-T Recommendation G. 959.1. Optical transport network physical layer interfaces.
7. Государственный первичный специальный эталон единиц динамических параметров импульсного лазерного излучения и скорости передачи информации в оптическом тракте: Доклад Федеральному агентству по техническому регулированию и метрологии. М. : ФГУП «ВНИИОФИ», 2015.

УДК 004.72

АНАЛИЗ АРХИТЕКТУРЫ И ТЕХНОЛОГИИ ПРОГРАММНО-КОНФИГУРИРУЕМЫХ СЕТЕЙ

Д. Д. Корякин, Д. В. Попков, И. О. Сошников, Е. А. Степанова

Военная академия связи имени Маршала Советского союза С. М. Буденного

Программно-определяемые сети сегодня являются актуальной темой на корпоративном уровне. Причин для этого несколько, и их становится все больше с каждым днем. Самая многообещающая – и, возможно, прибыльная – особенность ПКС, это её потенциальная способность сделать сеть напрямую программируемой.

программно-конфигурируемые сети, виртуализация сетевых устройств, OpenFlow.

Основными направлениями развития сетей центров обработки данных и корпоративных сетей являются:

– рост объемов трафика, из-за увеличения медиа потока поддержка мобильных пользователей;

– высокопроизводительные кластеры для обработки данных;

– виртуализация, для предоставления облачных услуг и сервисов.

Сеть в классическом виде, управление через командную строку и формирования конфигурационных файлов, становится тормозящим фактором развития вычислительной инфраструктуры. Стандартные подходы к решению проблем, например, на основе виртуализации сетей (VLAN, VRF), не соответствует уровню развития виртуализации серверов и систем хранения данных. Традиционные сети как правило статичны и не успевают за динамикой развития современных IT технологий. Низкая масштабируемость

традиционной сети не соответствует требуемым параметрам центров обработки данных и корпоративных сетей, а управление каждым устройством сети слишком сложно и не эффективно. Привязка к выбранному вендору не гарантирует поддержку разрабатываемых приложений и сервисов. В итоге традиционная архитектура сети становится неэффективна в динамических средах.

Для решения этой проблемы необходима новая технология или подход к построению инфотелекоммуникационных сетей позволяющая решить перечисленные выше проблемы. Такой технологией является Software Defined Networking (SDN) или программно-конфигурированные сети (ПКС).

ПКС – сеть передачи данных, в которой уровень управления сетью отделён от устройств передачи данных и реализуется программно, являясь одной из форм виртуализации вычислительных ресурсов.

Каждое сетевое устройство (роутер, коммутатор и т. д.) можно логически разделить на три компонента (рис. 1):

– уровень управления – это уровень обеспечения управляемости устройства (командная строка, встроенный веб-сервер или API и протоколы управления);

– уровень управления трафиком – это алгоритмы и функционал задачей которых является реакция на изменения трафика;

– передача трафика – функционал, обеспечивающий физическую передачу данных.

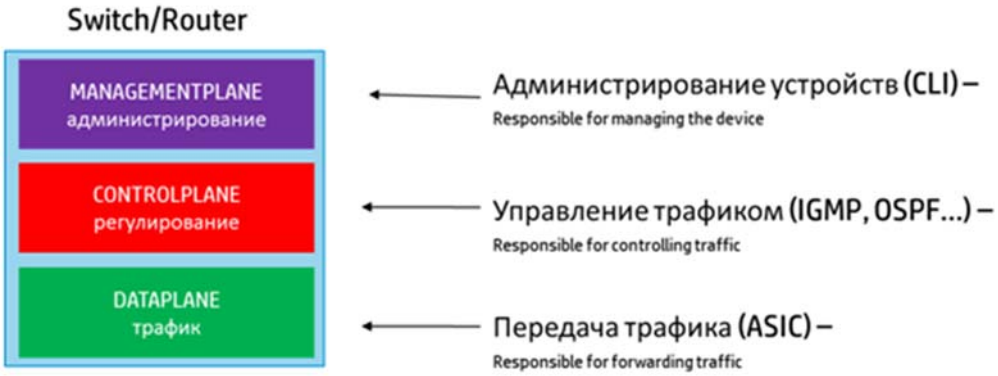


Рис. 1. Традиционное сетевое устройство

Если централизовать управление трафиком, отделив управление от устройств и централизовать управление устройствами, получится «новое» сетевое устройство обслуживающие только поток данных (уровень передачи трафика), становиться более простым и естественно более дешевым. Полностью лишить «интеллекта» сетевое устройство не получиться, но его достаточно заменить простой таблицей переадресации.

Весь «интеллект» реализовывается на отдельном центральном устройстве называемое контроллером ПКС.

В результате внесенных изменений в существующею сеть и оборудование получаем:

– разделение функций передачи трафика от функций управления (включая контроль как самого трафика, так и осуществляющих его передачу устройств);

– стандартный и открытый интерфейс между устройствами управления и передачи (OpenFlow);

– централизованное управление сетью (контроллер ПКС);

– виртуализация физических ресурсов сети;

– возможности программирования как оборудования (OpenFlow), так и приложений (API контроллер ПКС);

– быстрее реагировать на изменения в сети;

– оптимизирование передачи трафика (2 и 3 уровня модели OSI) через большее количество резервных путей;

– быстрая настройка оборудования сети;

– существенное сокращение времени развертывания приложений;

– упрощение управления сетевыми устройствами;

– сокращение затрат на управление сетями;

– увеличение производительности, централизованное применение политик, уменьшение задержек приводит к более эффективному взаимодействию пользователей и приложений как в корпоративных сетях, так и в сетях дата-центров;

– простота управления, управление целыми сетями, а не сетевыми устройствами;

– основанные на стандартах протоколы позволят взаимодействовать различным производителям сетевого оборудования между собой, одновременно увеличивая выбор заказчику и конкуренцию между вендорами при снижении затрат, ускоряя инновации как в области программного обеспечения, так и аппаратных средств;

– контроллер SDN поддерживает открытый интерфейс программирования (API), который позволяет его программировать, создавая среду для автоматизации и контроля, а также масштабировать функционал для будущих приложений (рис. 2);

– приложения могут запрашивать напрямую определенные требования к сети;

– видимость всего трафика сети контроллером.

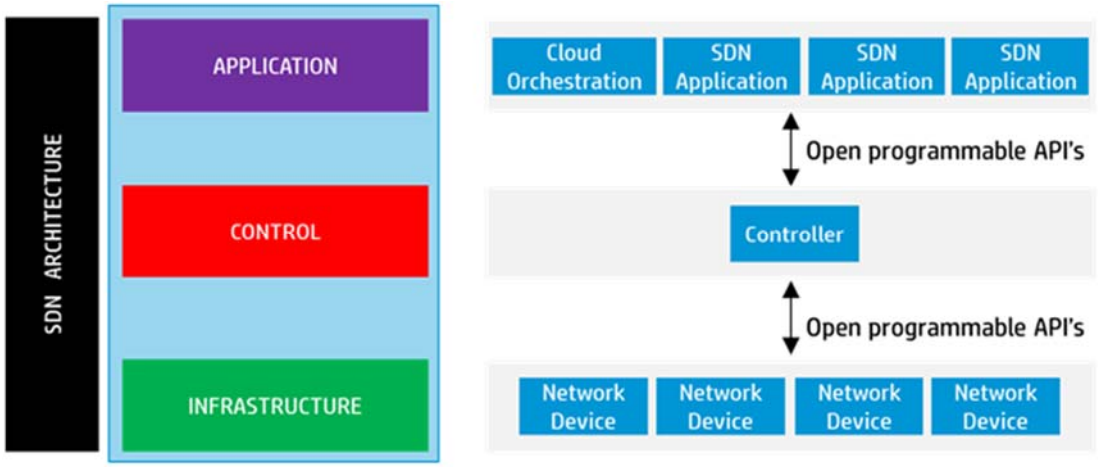


Рис. 2. Структура и компоненты SDN

Исходя из рис. 3, кроме классического управления сетью прямыми командами системного администратора к контроллеру, ПКС контроллер поддерживает запуск на себе приложений управления сетью.

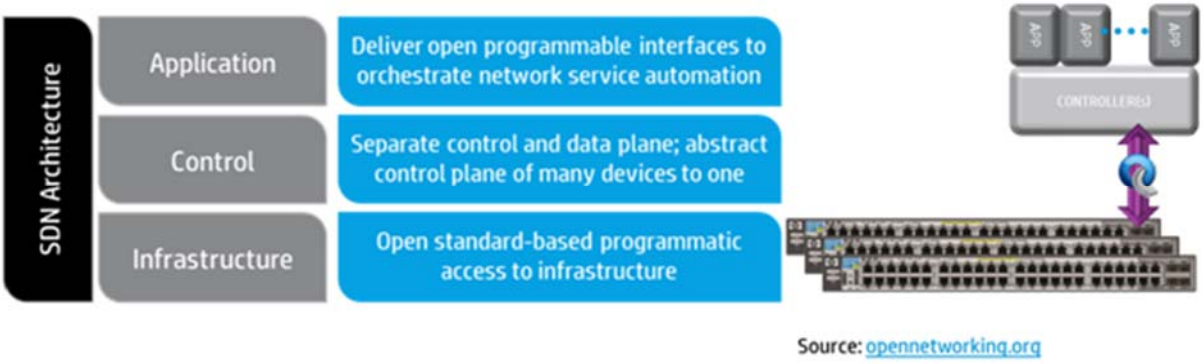


Рис. 3. Общая архитектура ПКС

Каждое ПКС приложение является интерфейсом оптимизации сети под конкретное приложение и его основная роль — изменение сети в реальном времени под текущие нужды обслуживаемой программы. Например, изменение QoS сети между телефонными абонентами для совершения HD видеозвонка без задержек или создание VPN тоннеля между двумя абонентами [2].

Рассматривая информационные потоки в архитектуре ПКС, выделяются два основных направления обмена информацией: первый – между ПКС приложениями и второй для управления сетевыми устройствами.

Первый поток именуется как «северный мост», а второй как «южный мост». В качестве «северного моста» выступает протокол на основе REST API, а в качестве «южного моста» протокол OpenFlow (рис. 4).

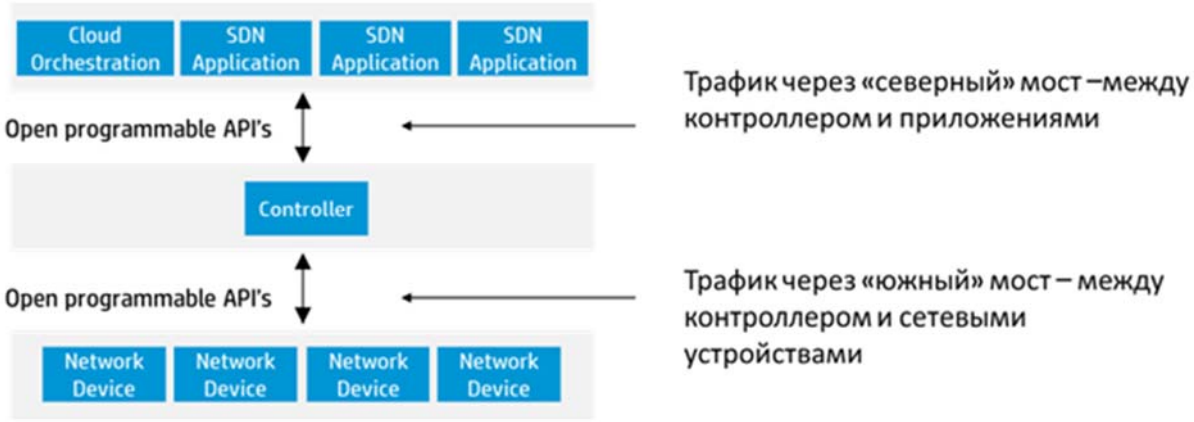


Рис. 4. Управляющие информационные потоки контроллера ПКС

OpenFlow – протокол, являющийся главным элементом технологии ПКС, который необходим для взаимодействия контроллера с сетевыми устройствами. Контроллер используется для управления таблицами потоков коммутаторов, на основании которых принимается решение о передаче принятого пакета на конкретный порт коммутатора. Таким образом, в сети формируются прямые сетевые соединения с минимальными задержками передачи данных и необходимыми параметрами [1].

В ходе анализа технологии ПКС можно выделить достоинства и недостатки, отображенные на рис. 5.

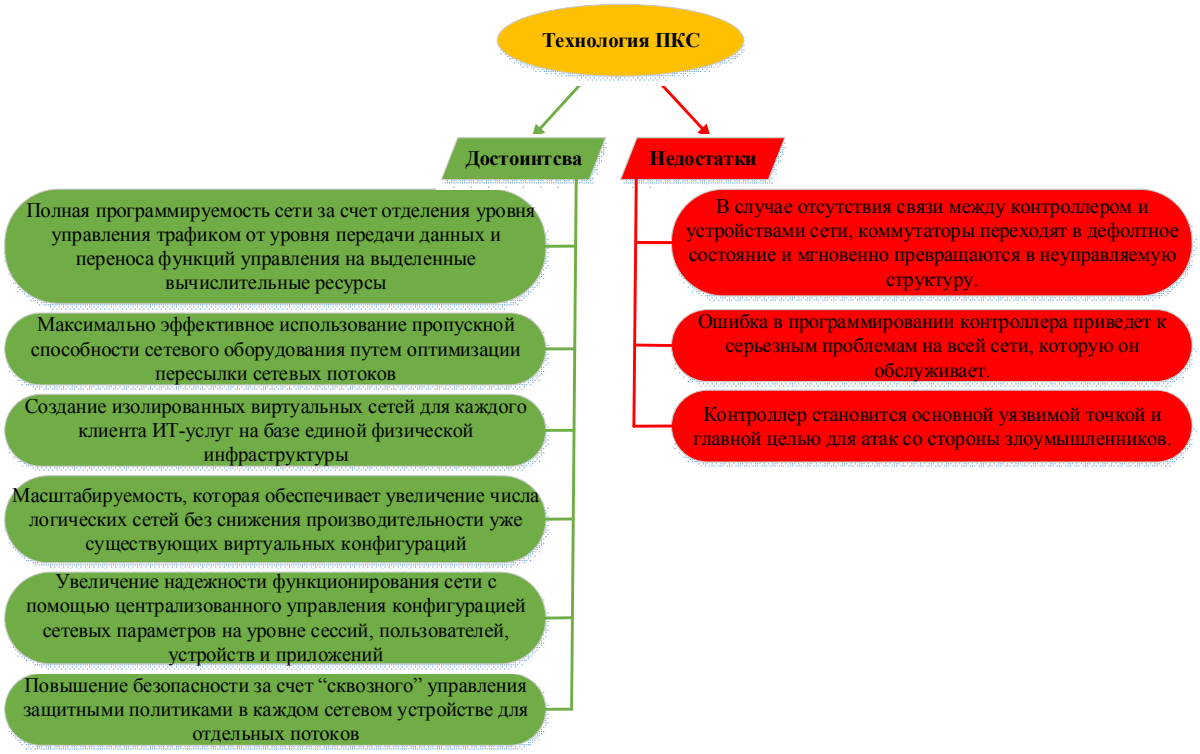


Рис. 5. Достоинства и недостатки технологии ПКС

Список используемых источников

1. Олифер В. Г., Олифер Н. А. Компьютерные сети. Принципы, технологии, протоколы: учебное пособие для вузов. 4-ое изд. СПб. : Питер, 2010. 944 с.
2. Селихов Ю. Р., Шуклин А. В., Юрсков С. В., Хамуш А. Л. Инжиниринг трафика в программно определяемых сетях // Молодой ученый. 2016. № 11. С. 461–467.

Статья представлена начальником отдела научно-исследовательского центра Военной академии связи, доцентом, кандидатом технических наук Д. О. Федосеевым.

УДК 004.72

ОСОБЕННОСТИ ПРИМЕНЕНИЯ ТЕХНОЛОГИИ OPENFLOW В ПРОГРАММНО-КОНФИГУРИРУЕМЫХ СЕТЯХ

Д. Д. Корякин, Д. В. Попков, И. О. Сошников, Е. А. Степанова

Военная академия связи имени Маршала Советского союза С. М. Буденного

Развитие технологий привело к необходимости обработки больших объемов информации. В последнее время изменилась концепция обработки информации и сеть становится главным ограничителем развития вычислительных систем. Причина заключается в том, что сеть является статичной. Существующие методы адресации, логического деления и способы конфигурирование соответствующего оборудования в подобных сетях становится неэффективными. Для решения данных проблем была разработана концепция программно-конфигурируемых сетей.

программно-конфигурируемые сети, OpenFlow, out – of – band, in – band.

Программно-конфигурируемая сеть (ПКС) – это новый подход к построению архитектуры компьютерных сетей, при котором уровень управления (УУ) сетью (состоянием сетевой инфраструктуры и потоками данных в сети) и уровень передачи данных (УПД) разделяются за счет переноса функций управления (выполняемых в традиционной сети маршрутизаторами и коммутаторами) на отдельное центральное устройство, называемое контроллером. За счет такого разделения контроль состояния сети и управление сетью логически централизовано на контроллере. Также данный подход позволяет уровню управления абстрагироваться от физической сетевой инфраструктуры уровня передачи данных, используя некоторое логическое представление сети. Взаимодействие между УУ и УПД осуществляется посредством единого унифицированного открытого интерфейса (рис. 1).

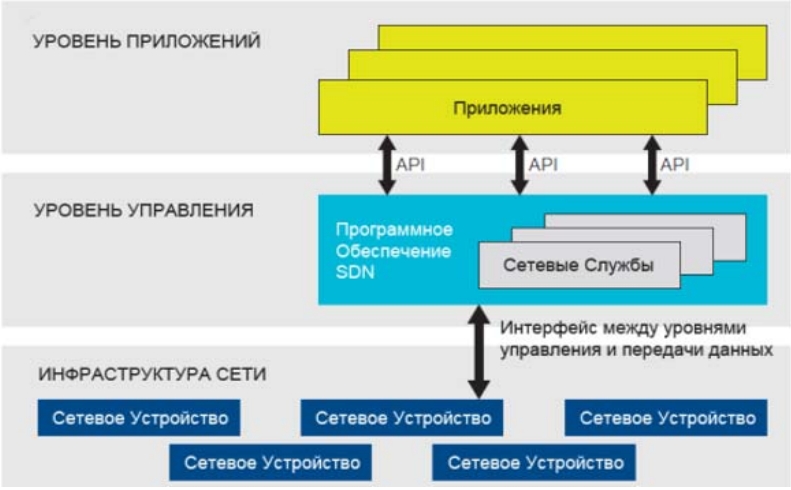


Рис.1. Архитектура программно-конфигурируемых сетей

Интерфейсом между уровнями управления и передачи данных является OpenFlow – протокол взаимодействия между сетевыми устройствами (коммутаторами) программно-управляемой сети SDN и централизованным контроллером. Данная технология является одной из наиболее перспективных и развивающихся в реализации подхода программно-конфигурируемых сетей. Основным её документом является спецификация OpenFlow [1], в которой описываются основные компоненты OpenFlow-сети, принципы работы и взаимодействия компонентов (протокол OpenFlow). Согласно данной спецификации основными компонентами OpenFlow сети являются: контроллер, который включает в себя сетевую операционную систему и сетевые приложения; OpenFlow коммутатор; защищенный канал между контроллером и коммутатором; протокол OpenFlow. На рис. 2 представлены основные компоненты OpenFlow сети.

Общий принцип функционирования OpenFlow-сети заключается в следующем: каждый OpenFlow коммутатор устанавливает защищенный канал с контроллером, посредством которого контроллер управляет им. Взаимодействие между коммутаторами и контроллером осуществляется посредством сообщений протокола OpenFlow. Контроллер получает информацию об изменении состояний элементов в сети, на основе которой он конфигурирует сетевое оборудование, управляет сетевой инфраструктурой и потоками данных в сети [2].

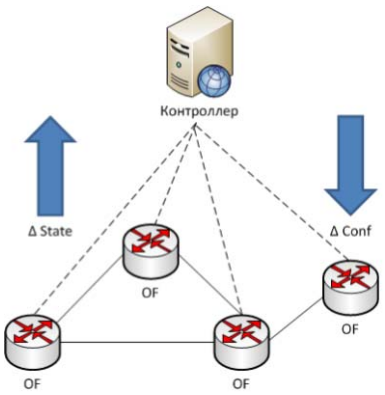


Рис. 2. Основные компоненты OpenFlow сети

Развитие OpenFlow прошло через ряд версий – от версии 1.0 до 1.4. Большинство производителей сетевого оборудования изначально реализовали поддержку версии 1.0, которая имела множество ограничений и проблем с масштабируемостью. Она показала, что ONF предложил рынку неполноценный продукт. Версии 1.1 и 1.2 считаются переходными и практически никто из производителей не реализует их поддержку. Наиболее перспективной считается версия 1.3, в которую включена поддержка MPLS меток, per-flow счетчиков, Provider Backbone Bridging (PBB) и еще некоторых полезных функций [3]. По результатам тестирования большого количества коммутаторов разных производителей (на момент написания статьи), можно сказать, что поддержка версии 1.3 на «железных» коммутаторах пока очень ограничена.

OpenFlow не является полностью «открытым» протоколом, однако его разработка контролируется закрытой группой, состоящий примерно из 150 компаний, формирующих ONF. Работа ведется в скрытом от широкой публики режиме и ее результат виден только после публикации новой версии в качестве стандарта.

Для корректной работы OpenFlow коммутатора необходимо, чтобы он мог устанавливать и поддерживать соединение с соответствующим контроллером. Существует два основных подхода к организации такого соединения:

– передавать сообщения OpenFlow по физически независимому каналу, изолированному от сети передачи данных (*out-of-band*);

– для передачи управляющей информации можно использовать непосредственно сеть передачи данных, которой управляет контроллер (*in-band*).

В случае использования out-of-band подхода в OpenFlow коммутаторе выделяется отдельный порт. Вся управляющая информация между контроллером и коммутатором передается через этот порт, для передачи пакетов в сети передачи данных используются другие порты коммутатора. Таким образом, для управления коммутаторами создается отдельная сеть согласно рис. 3.

Преимуществами out-of-band подхода являются простота (упрощается реализация OpenFlow коммутатора), надежность (трафик в сети передачи данных никак не влияет на передачу управляющей информации), безопасность (машины, не входящие в сеть управления, не имеют физической возможности получить доступ к управлению настройками коммутатора) [1].

В случае in-band подхода (второй подход) для передачи управляющей информации используется та же сеть, что и для передачи пользовательских данных согласно рис. 4.

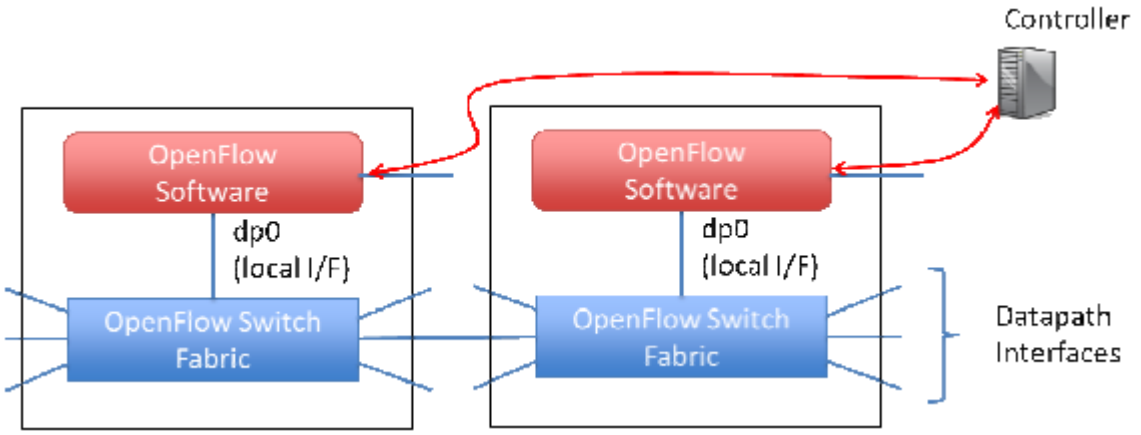


Рис. 3. Out-of-band подход управления коммутаторами в ПКС сети

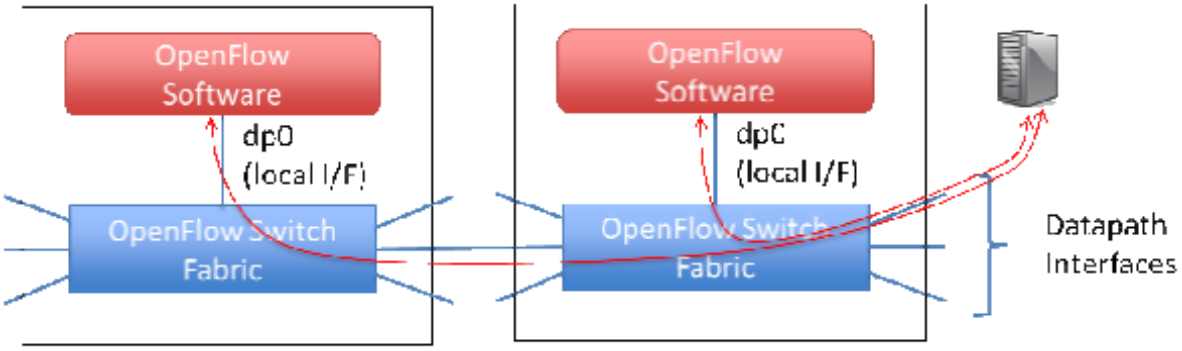


Рис. 4. In-band подход управления коммутаторами в ПКС сети

К преимуществам in-band подхода можно отнести экономичность, так как не требуется выделения отдельных портов и физических каналов под сеть управления, сокращение количества сетевого оборудования, упрощается проектирование и поддержка сети [4]. Однако могут возникать риски, связанные с надежностью (перегрузки в сети передачи данных, отказы каналов) и с безопасностью (возможности DDoS-атак на контроллер).

Во многих случаях перечисленные выше достоинства in-band управления делают его использование более предпочтительным, чем out-of band управление.

Список используемых источников

1. Mininet. Official Website [Электронный ресурс] // Mininet. URL: http://mininet.org/ (дата обращения 02.02.2015).

2. Коломеец А. Е, Сурков Л. В. Программно-конфигурируемые сети на базе протокола OpenFlow // Электронный научно-технический журнал «Инженерный вестник» МГТУ им. Н. Э. Баумана. 2014. № 5. 9 с. URL: http://engbul.bmstu.ru/doc/711486.html (дата обращения 02.02.2015).

3. Смелянский Р. Л. Программно-конфигурируемые сети [Электронный ресурс] // Открытые системы. 2012. № 9. URL: http://www.osp.ru/os/2012/09/13032491/ (дата обращения 02.02.2015).

4. OpenFlow. Official Website [Электронный ресурс] // OpenFlow. URL: http://archive.openflow.org/wk/index.php/OpenFlow_Tutorial/ (дата обращения 02.02.2015).

Статья представлена начальником отдела научно-исследовательского центра Военной академии связи, доцентом, кандидатом технических наук Д. О. Федосеевым.

УДК 004.056.5

ОБЗОР ВОЗМОЖНОСТЕЙ РЕАЛИЗАЦИИ КАНАЛЬНОЙ СТЕГАНОГРАФИИ НА ОСНОВЕ ПРОТОКОЛОВ СЕТЕВОГО И ТРАНСПОРТНОГО УРОВНЕЙ МОДЕЛИ OSI

А. С. Костырин, А. В. Красов

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

В данной работе приведена классификация канальной (сетевой) стеганографии. Рассмотрены возможности реализации методов канальной стеганографии на основе модификации заголовков протоколов IP, TCP, ICMP. Также классифицированы и приведены сведения о целесообразности использования того или иного метода, и сложности детектирования факта сокрытия информации с его применением.

канальная стеганография, сокрытие информации, классификация видов стеганографии, защита информации, сети передачи данных.

Стеганография – способ передачи или хранения информации с учётом сохранения в тайне самого факта такой передачи (хранения). В отличие от криптографии, которая скрывает содержимое тайного сообщения, стеганография скрывает сам факт его существования. Таким образом, стеганография потенциально обеспечивает не только безопасность, но также анонимность и конфиденциальность, которые очень важны в современном обществе.

Канальная стеганография – способ сокрытия факта передачи информации в сетях передачи данных.

Методы сетевой стеганографии можно разделить на группы (рис. 1) [1]:

1) методы стеганографии, суть которых в изменении данных в полях заголовков сетевых протоколах и в полях полезной нагрузки пакетов;

2) методы стеганографии, в которых изменяется структура передачи пакетов, например, изменяются очередности передачи пакетов или преднамеренное введение потерь пакетов при их передаче;

3) смешанные (гибридные) методы стеганографии – при их применении изменяются содержимое пакетов, сроки доставки пакетов и порядок их передачи.

Каждый из этих методов делится ещё на несколько групп; например, методы модификации пакетов включают в себя три разных метода:

– методы изменения данных в полях заголовков протокола: они основаны на модификации полей заголовков IP, TCP, SCTP и так далее;

– методы модификации полезной нагрузки пакета; в этом случае применяются всевозможные алгоритмы водяных знаков, речевых кодеков и прочих стеганографических техник по скрытию данных.

Методы модификации структуры передачи пакетов включают в себя три направления:

– методы, в которых изменяется порядок последовательности пакетов;

– методы, изменяющие задержку между пакетами;

– методы, суть которых заключается во введении преднамеренной потери пакетов путём пропуска порядковых номеров у отправителя.

Смешанные (гибридные) методы стеганографии используют два подхода: методы потери аудио пакетов (LACK) и ретрансляция пакетов (RSTEG) [2].

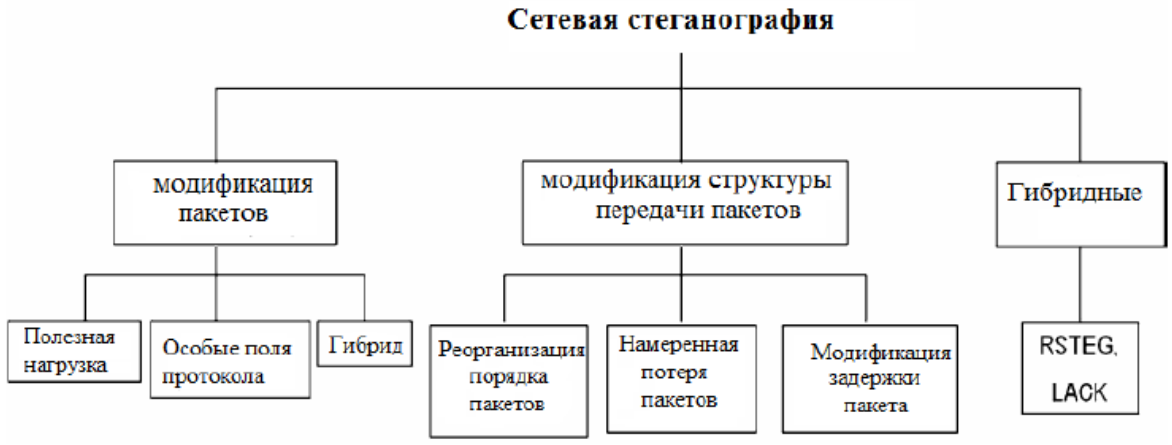


Рис. 1. Классификация методов канальной стеганографии

Далее рассмотрены методы канальной стеганографии на основе использования протоколов стека TCP/IP.

Internet Protocol – это протокол сетевого уровня. Это connection-less протокол, обеспечивающий наилучшие возможности для протоколов более высоких уровней, может отправлять пакеты на удаленный пункт назначения наиболее экономичным способом. Рис. 2 описывает структуру заголовка IP.

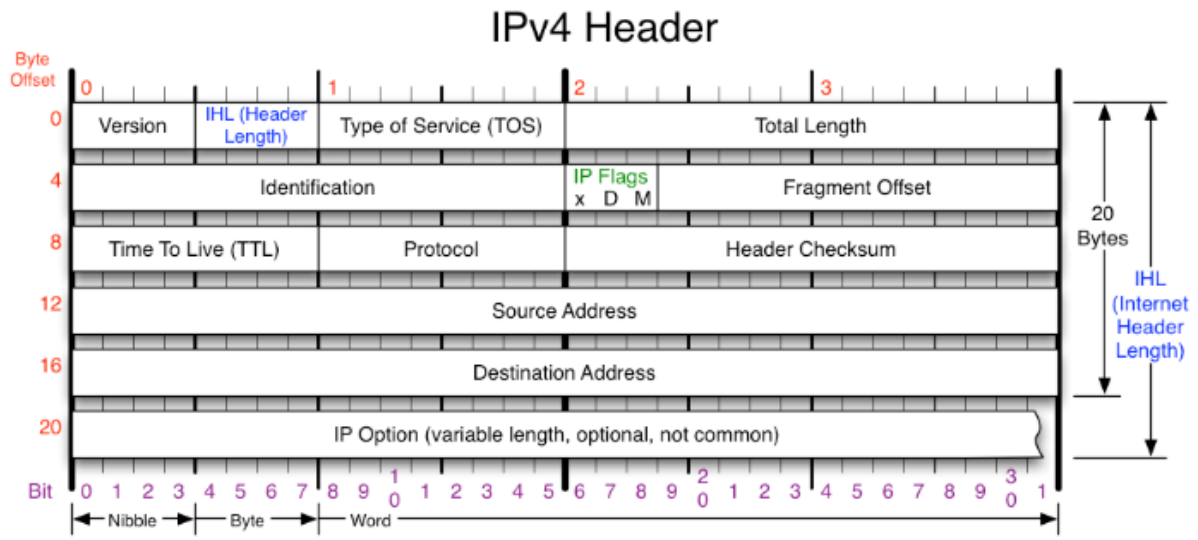


Рис. 2. Заголовок пакета IPv4

Type of Service: восемь Type of Service (ToS) бит в заголовке IP используются для указания параметров качества услуг для маршрутизаторов по пути следования пакета. В настоящее время редко используются для их изначального назначения (как показано в [1]). Могут быть использованы в DiffServ.

Существует потенциал для использования бит в этом поле как носителя стеганографической информации [3], потому что большинство сетей не используют их. Однако, это может быть легко обнаружено так как большинство операционных систем по умолчанию обнуляют это поле.

IP Flags: IP-пакеты включают в себя два флага, Do not Fragment (DF), указывая, что пакет должен быть отброшен, если он не может быть отправлен без фрагментации, и More Fragments (MF), который равен 0, если пакет содержит последний фрагмент, или если пакет не был фрагментирован.

Имеется стеганографический потенциал использования поля DF [4]. Если пакет меньше максимального размера сегмента, поле DF не влияет на поведение данных пакетов. Однако нормальное состояние DF может быть предсказано из контекста пакета, так что обнаружить модификацию данного поля не составляет труда.

IP Fragment Offset: когда IP-пакеты фрагментируются, отдельные фрагменты содержат поле Offset; оно позволяет принимающему узлу восстановить фрагменты в правильной позиции. Информация может передаваться скрытно путем изменения размеров фрагментов отправляемым узлом [5, 6], и таким образом изменяя значение поля Offset. Как и в случае обнаружением изменения поля ToS, это метод стеганографии легко обнаружить. В сетях, где используется MTU path discovery, фрагментация пакетов является ненормальным поведением [7].

IP Options: IP-пакеты очень редко содержат "options", поэтому их стеганографический потенциал ограничен. В [8] описывается использование параметра IP Timestamp, но такие пакеты не только легко обнаруживаются, они также не могут проходить более 20 узлов, что делает этот способ стеганографии мало пригодным в Интернете.

IP Identification: как описано в [9], поле IP Identification (IP ID) предназначено для определения корректной последовательности фрагментов при сборке пакета, и составляет 16 бит в IP-заголовке. Поскольку IP ID используется для отличия фрагментов, составляющих один пакет от фрагментов, составляющих другой, единственные ограничения на значение этого поля – уникальность во время нахождения фрагментов пакетов в сети и непредсказуемость.

Стеганографический потенциал этого поля велик, однако зная, какие алгоритмы используют различные операционные системы для заполнения этого поля уникальными битами, имеется возможность обнаружить факт сокрытия данных в поле IPID

Transport Control Protocol – это ориентированный на соединение протокол, который обеспечивает гарантированную доставку данных. За счет улучшенной коррекции ошибок и надежности, в нем много нагрузки контроля, которая может быть успешно использована для скрытой связи. Поля заголовка пакета TCP представлены на рис. 3.

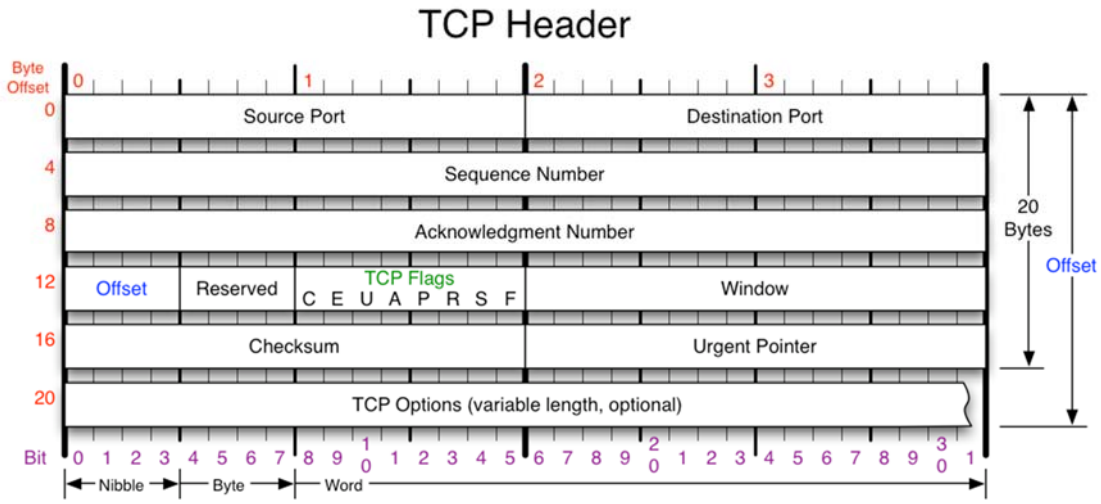


Рис. 3. Заголовок пакета TCP

TCP Sequence Number: номер последовательности TCP поддерживает функции надежности, предоставляемые TCP (и в некоторой степени, функции управления потоком). Каждому октету данных, передаваемых по TCP-потоку, присваивается Sequence Number. В протоколе TCP, соедине-

ние (определяемое парой сокетов) может быть использовано снова, и, следовательно, узел должен быть в состоянии обнаружить, является ли сегмент с текущей или с предыдущей реализации соединения.

Ценность данного поля для сокрытия передаваемых данных высока из-за относительно высокой пропускной способности (размер поля 32 бита) и сложности обнаружения. Метод детектирования стеганографии в этом поле строится на знании алгоритмов генерации его в различных операционных системах и выявления отклонений от этих алгоритмов.

TCP Timestamp: Опция TCP timestamp позволяет узлу точно измерить время прохождения пакета по пути, а также уменьшает проблемы, связанные с порядковым номером пакета в сетях с большой пропускной способностью и задержкой.

Опция timestamp состоит из двух 32 битных полей, TS Value и TS EchoReply. Значение TC Value устанавливается на основе временной метки отправителя, и именно в это поле имеется возможность внести скрытые данные. Единственным ограничением является то, что частота отсчета часов отправителя составляет от 1 Гц до 1 кГц, и является монотонной

Возможность обнаружения скрытого канала в данном поле заключается в том, что не все операционные системы используют это поле. Соответственно, отправка пакетов с машин с ОС без поддержки данного поля будет подозрительным.

Internet Control Message Protocol был разработан, чтобы передавать уведомления об ошибках и сервисные сообщения между узлами сети. ICMP пакеты инкапсулируются внутри IP-дейтаграмм. Рис. 5 показывает заголовок ICMP.

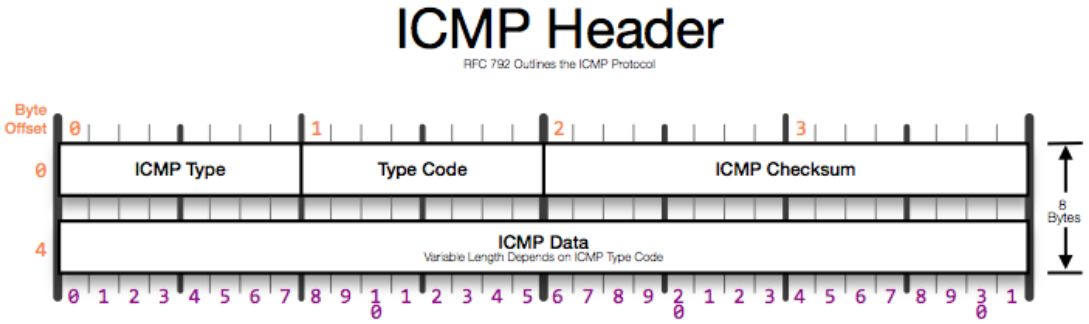


Рис. 5. Заголовок пакета ICMP

ICMP Echo Request и Echo Reply. ICMP EchoRequest используется для проверки доступен ли удаленный хост или нет. Необязательное поле данных позволяет вернуть отправителю данные переменной длины. Параметры IP, такие как router alert, record route и timestamp можно использовать для сокрытия данных внутри ICMPпакета [10]. В настоящее время большин-

ство брандмауэров отфильтровывает входящие эхо-запросы, но они разрешают эхо-ответы, что обеспечивает широкие возможности для стеганографии в ICMP пакетах в обход брандмауэра.

Список используемых источников

1. Postel, J.: STD5: Internet protocol. IETF (1981).
2. 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. ISBN 978-5-89160-125-3.
3. Небаева К. А., Скородумов С. А. Стеганография в IP-телефонии и сложности ее реализации // Актуальные проблемы инфотелекоммуникаций в науке и образовании сборник научных статей. V международная научно-техническая и научно-методическая конференция. СПб. : СПбГУТ, 2016. С. 494–498.
4. Ahsan, K., Kundur, D.: Practical data hiding in TCP/IP [Электронныйресурс] /ACM Workshop on Multimedia and Security. [сайт]. URL: http://ee.tamu.edu/~deepa/pdf/acm02.pdf (дата обращения 29.01.2017).
5. Кириллов Д. И. Методика построения системы обнаружения вторжений для VoIP трафика // T-Comm: Телекоммуникации и транспорт. 2009. Т. 3. № 5. С. 49.
6. Ковцур М. М., Никитин В. Н., Юркин Д. В. Протоколы обеспечения безопасности VoIP-телефонии// Защита информации. Инсайд. 2012. № 3 (45). С. 74–80.
7. Mogul, J., Deering, S.: RFC1191: Path MTU discovery. IETF (1990).
8. Handel, T., Sandford, M.: Hiding data in the OSI network model. In Anderson, R., ed.: Information Hiding. Vol. 1174 of Lecture Notes in Computer Science., Springer-Verlag (1996). PP. 23–38.
9. Postel, J.: STD5: Internet protocol. IETF (1981).
10. Debasish Mandal. Covert Channel over ICMP. [Электронныйресурс] // Debasish Mandal's Blog [сайт]. URL: http://www.debasish.in/ (дата обращения 29.01.2017).

УДК 004.056.5

РЕАЛИЗАЦИЯ МЕТОДА КАНАЛЬНОЙ СТЕГАНОГРАФИИ С ИСПОЛЬЗОВАНИЕМ ПРОТОКОЛА ICMP

А. С. Костырин, А. В. Красов

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

В данной работе рассматривается практическая реализация сокрытия информации в сетевом протоколе ICMP. Приведены сведения о спроектированном и написанном ПО для скрытого удаленного управления ЭВМ, представлены результаты эксперимента по удаленному управлению ЭВМ с сокрытием передачи управляющих данных в протоколе ICMP.

канальная стеганография, сокрытие информации, классификация видов стеганографии, защита информации, сети передачи данных.

Стеганография – способ передачи или хранения информации с учётом сохранения в тайне самого факта такой передачи (хранения). В отличие от криптографии, которая скрывает содержимое тайного сообщения, стеганография скрывает сам факт его существования. Таким образом, стеганография потенциально обеспечивает не только безопасность, но также анонимность и конфиденциальность, которые очень важны в современном обществе [1].

Канальная стеганография – способ сокрытия факта передачи информации в сетях передачи данных.

Протокол ICMP (*Internet Control Message Protocol*) – протокол стека TCP/IP. Служит для передачи сообщений о сетевых ошибках и для обеспечения некоторых сервисных функций [2].

ICMP принадлежит третьему (сетевому) уровню модели OSI.

ICMP сообщения инкапсулируются в пакеты IP (Рис. 1)

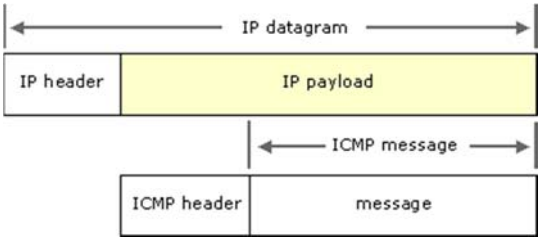


Рис. 1. ICMP сообщение в IP пакете

ICMP пакет состоит из (рис. 2):

– ICMP type–тип сообщения ICMP;

– Typecode–подтип сообщения ICMP;

– ICMP checksum – контрольная сумма пакета;

– ICMP data– полезная нагрузка ICMP пакета (зависит от типа сообщения).

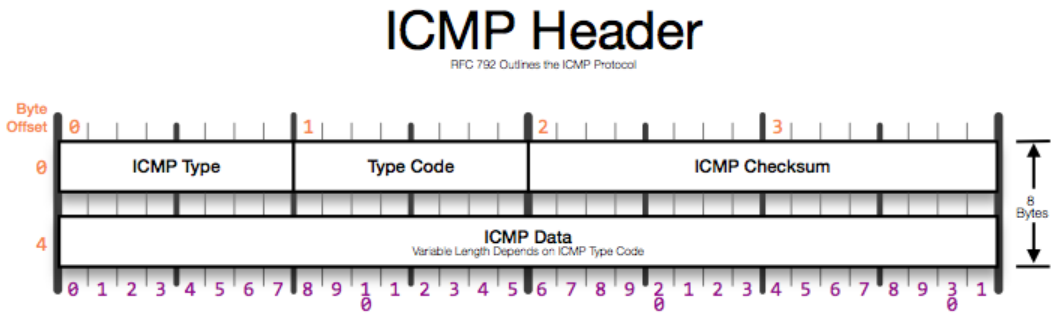


Рис. 2. ICMP пакет

Часто используемые типы сообщений:

– ICMP-сообщения (тип 12) генерируются при нахождении ошибок в заголовке IP-пакета (за исключением самих ICMP-пакетов, дабы не привести к бесконечно растущему потоку ICMP-сообщений об ICMP-сообщениях);

– тип 3 генерируются маршрутизатором при отсутствии маршрута к адресату;

– утилита Ping, служащая для проверки возможности доставки IP-пакетов, использует ICMP-сообщения с типом 8 (эхо-запрос) и 0 (эхо-ответ);

– утилита Traceroute, отображающая путь следования IP-пакетов, использует ICMP-сообщения с типом 11;

– ICMP-сообщения с типом 5 используются маршрутизаторами для обновления записей в таблице маршрутизации отправителя;

– ICMP-сообщения с типом 4 используются получателем (или маршрутизатором) для управления скоростью отправки сообщений отправителем.

ICMP туннель (ICMPTX) – устанавливает скрытое соединение между двумя компьютерами, используя ICMP эхо запросы и ответы (типы 8 и 0 ICMP сообщений) [3].

ICMP туннелирование возможно потому, что стандарт RFC 792 позволяет задавать блок данных произвольной длинны для типов 0 (эхо-ответ) или 8 (эхо-запрос) ICMP-пакетов.

ICMP туннелирование работает путем введения произвольных данных в эхо-пакет, отправленный на удаленный компьютер. Удаленный компьютер отвечает тем же самым способом, подставляя свои данные вэхо-ответ и отправляя его обратно. Клиент выполняет все коммуникации с использованием эхо-запросов, в то время как сервер может использовать как эхо-запросы, так и эхо-ответы [4].

ICMP-туннелирование может применятся для скрытия факта передачи данных и удаленного управления в обход правил брандмауэра. В зависимости от реализации программного обеспечения ICMP туннелирования, этот тип соединения также может быть классифицирован как зашифрованный канал связи между двумя компьютерами. Без применения систем DPI (*Deep Packet Inspection*), сетевые администраторы не имеют возможности обнаружить этот тип трафика в своей сети.

Цель: реализовать скрытое управление удаленным хостом путем передачи данных управления в ICMP–туннеле.

В качестве носителя информации будут применяться только тип 8 ICMP сообщений (эхо-запросы), как со стороны сервера, так и со стороны клиента. В данном случае сервер – управляемый хост, будет слушать ICMP сообщения на одном из своих интерфейсов, расшифровывать их и выполнять инструкции. Затем результат выполнения команды будет отправлен с помощью эхо-запроса клиенту. Клиент же в свою очередь принимает команды от пользователя, отправляет их удаленному серверу, упаковывая в эхо-запросы и принимает результат выполнения команды.

В качестве языка программирования выбран Python 3.6 для возможности наиболее быстрой разработки и портирования на другие платформы (однако целевой платформой является *linux*).

Программа не использует каких-либо дополнительных модулей, кроме стандартной библиотеки. Формирование пакетов ICMP происходит полностью «в ручном» режиме. Структура формируемого программой пакета (рис. 3).

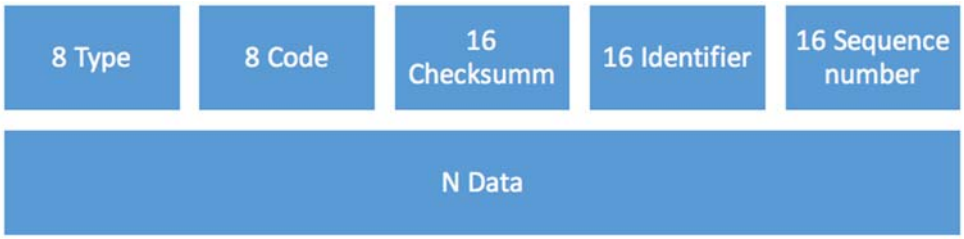


Рис. 3. Структура формируемого программой пакета

Где:

– Type – тип сообщения, 8 для эхо-запроса;

– Code – подтип сообщения, 0 для эхо-запроса;

– Checksum – Контрольная сумма пакета, алгоритм формирования контрольной суммы описан в стандарте RFC 1071;

– Identifier – идентификатор, используется для определения пар пакетов эхо-запрос/эхо-ответ. В программе в качестве идентификатора используется текущий идентификатор процесса (PID);

– Sequence number–номер последовательности, используется для определения пар пакетов эхо-запрос/эхо-ответ. В программе в качестве номера последовательности используется 1;

– Data – данные, с помощью которых производится удаленное управление. Данные имеют формат “@@data” для удобства разборки полученных пакетов с использованием регулярных выражений. Данные передаются в открытом виде, шифрование данных не применяется.

Конфигурация хостов: для проведения эксперимента использовались два хоста – клиент и сервер. Клиент находился на виртуальной машине под управлением операционной системой Linux (*Ubuntu* 16.4). Сервером выступал хост с гипервизором, операционная система – Linux (*Ubuntu* 16.10). В качестве гипервизора был выбран Oracle Virtual Box.

Конфигурация сети: сеть была сконфигурирована таким образом, что клиент и сервер находились в одной подсети. IPадрес сервера – 192.168.0.100, IPадрес клиента – 192.168.0.105. Для контроля эксперимента на сервере запущенно ПО анализатор трафика – Wireshark.

Сценарий проведения эксперимента:

– запуск сервера и клиента с определенными согласно конфигурации сети;

– выполнение операций по управлению сервером с клиента через remote shell;

– проверка результатов сеанса управления на сервере анализ захваченных с помощью Wireshark пакетов;

– в качестве операций по управлению сервером были выбраны:

– ls – операция листинга содержания текущего каталога;

– pwd– вывод названия текущего каталога;

– echo text > file.txt – вывод в файл file.txt текста text.

В результате проведения эксперимента, можем убедиться, что:

– на клиенте было отображено название и содержание текущего каталога на сервере;

– файл, созданный с помощью команды на клиенте, присутствует на сервере;

– трафик управления инкапсулировался только в пакеты ICMP и данные управления передавались в открытом виде в пакетах ICMP, причем на каждый echo-request следовал echo-reply (рис. 4, 5).

No.	Time	Source	Destination	Protocol	Length	Info
110	171.454260724	192.168.0.105	192.168.0.100	ICMP	60	Echo (ping) request id=0x4904, seq=256/1, ttl=64 (reply in 111)
111	171.454306653	192.168.0.100	192.168.0.105	ICMP	52	Echo (ping) reply id=0x4904, seq=256/1, ttl=64 (request in 110)
152	274.066757608	192.168.0.105	192.168.0.100	ICMP	60	Echo (ping) request id=0x4d04, seq=256/1, ttl=64 (reply in 153)
153	274.066816145	192.168.0.100	192.168.0.105	ICMP	46	Echo (ping) reply id=0x4d04, seq=256/1, ttl=64 (request in 152)
154	274.097588144	192.168.0.100	192.168.0.105	ICMP	52	Echo (ping) request id=0x2d53, seq=256/1, ttl=64 (reply in 155)
155	274.098448523	192.168.0.105	192.168.0.100	ICMP	60	Echo (ping) reply id=0x2d53, seq=256/1, ttl=64 (request in 154)
157	275.099060163	192.168.0.100	192.168.0.105	ICMP	54	Echo (ping) request id=0x2d53, seq=256/1, ttl=64 (reply in 158)
158	275.103044289	192.168.0.105	192.168.0.100	ICMP	60	Echo (ping) reply id=0x2d53, seq=256/1, ttl=64 (request in 157)

Рис. 4. Перехват трафика управления в Wireshark

```
Sequence number (LE): 1 (0x0001)
[Response frame: 228]
Data (13 bytes)
    Data: 40402f686f6d652f616c65780a
    [Length: 13]

0000  08 00 27 a3 f5 47 2c d0  5a ec 97 96 08 00 45 00   ..'..G,. Z.....E.
0010  00 29 37 6d 40 00 40 01  81 49 c0 a8 00 64 c0 a8   .)7m@.@. .I...d..
0020  00 69 08 00 b4 82 2d 53  01 00 40 40 2f 68 6f 6d   .i....-S ..@@/hom
0030  65 2f 61 6c 65 78 0a                              e/alex.
```

Рис. 5. Детальный разбор прихваченных ICMP пакетов

Как результат данного эксперимента, можно сделать вывод, что возможность канальной стеганографии с применением протокола ICMP создает реальную угрозу передачи конфиденциальных данных без ведома пользователя. Возможный сценарий применения данной техники – это

скрытая передача данных и управление сервером частной компании после успешной эксплуатации уязвимости в ПО и эскалации привилегий. Имеется возможность даже построить скрытую сеть поверх туннелей ICMP с использованием стека протоколов TCP/IP. Как уже было сказано, большинство современных межсетевых экранов не имеют защиты от использования ICMP-туннелирования, и обнаружение скрытой передачи информации возможно только с применением технологии DPI и тщательного контроля трафика администратором сети. Таким образом, разработка быстрых алгоритмов обнаружения ICMP-туннелирования в сети является перспективным направлением исследования.

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. ISBN 978-5-89160-125-3.
2. Postel, J.: RFC 792 (1981).
3. Daniel Stodle. Ping Tunnel: For those times when everything else is blocked [сайт]. URL: http://www.cs.uit.no/~daniels/PingTunnel/
4. Debasish Mandal. Covert Channel over ICMP [Электронный ресурс] // Debasish Mandal's Blog [сайт]. URL: http://www.debasish.in/ (дата обращения 12.02.2017).

УДК 004.728.8

ЗАЩИТА СЕТИ ПЕРЕДАЧИ ДАННЫХ С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИИ OPENDNS

А. В. Красов, Н. О. Лоханько, Р. С. Подоляк

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

Данная статься посвящена технологии OpenDNS. В статье описывается алгоритм работы этой технологии и методика её использовании для защиты сети от различных атак. OpenDNS является решением, которое может использоваться в сети на «первой линии обороны». Защита от DNS это универсальный способ подхода к защите соединений благодаря тому, что служба DNS является одной из основополагающих служб Интернета. Особенность защиты DNS состоит в том, что она не зависит от порта и протокола (http, torrent, ftp и т. д.), т. к. в момент, когда пользователь или инфицированный компьютер инициирует обращение к какому-либо домену, при установлении сессии, он обращается к DNS.

безопасность сети, OpenDNS, DNS.

Традиционно компьютерная сеть организации представляет из себя закрытый периметр, однако, с появлением облачных технологий этот периметр стал размываться. Эта тенденция развивается уже несколько лет и становиться всё более актуальной. Облачные технологии позволяют предоставить такие услуги как приложение как сервис, инфраструктура как сервис и платформа как сервис. Также следует учитывать тот факт, что часть сотрудников компаний стала мобильна. При этом актуальность защиты данных видов доступа и вообще информации с каждым годом всё больше растёт. Особенно на фоне последних событий и новостей в области банковской сферы.

Согласно прогнозу компании Garther, к 2018 г. 25 % корпоративного трафика будет обходить периметральную защиту. Проблема в данном случае усугубляется тем, что многие сотрудники не используют технологии VPN для защиты передаваемого трафика, чем открывают широкие возможности для теневого IT и подвергают опасности компрометации свои данные и данные компании. Таким образом значительная часть трафика будет обходить межсетевые экраны на границах сети.

OpenDNS является решением которое может стоять на так называемой первой линии обороны. Эта система состоит из нескольких классов решений. Защита с использованием DNS это универсальный способ подхода к защите соединений благодаря тому, что служба DNS является одной из основополагающих служб Интернета. Так или иначе практически все устройства в сети пользуются DNS сервисом. Особенность защиты с использование DNS состоит в том, что он не зависит от порта и протокола, который использует пользователь (http, torrent, ftp и т. д.), т. к. в момент, когда пользователь инициирует обращение к какому-либо домену, при установлении сессии, он обращается к DNS. Таким образом обращение к DNS происходит раньше, чем установление соединения с большинством вредоносных сайтов и ботнетов.

По статистике 15 % вредоносного программного обеспечения использует не стандартные (80 и 443), а произвольные порты для установления соединений с C&C сервером. То есть порядка 15 % вредоносов используют другие каналы для соединения с C&C сервером, это может быть ICMP payload, DNS payload и т. д. При этом 91 % C&C соединений может быть блокировано уже на уровне DNS запросов.

Технология OpenDNS состоит из двух логических частей, первой и которых является компонент Umbrella, являющимся первичным механизмом защиты сети подробнее о котором будет написано ниже. Второй частью является компонент Investigate. Это интеллектуальный сервис для расследования инцидентов, который помогает операторам информационной безопасности как вручную за очень короткое время с единой консоли получать всю

аналитику по вредоносным доменам и всей ассоциированной с ними информации, так и с использованием API интегрироваться в СМ системы для автоматизации расследования инцидентов.

Компонент Umbrella состоит из нескольких составляющих, каждая и которых обеспечивает защиту на своём уровне. Он обеспечивает предотвращение угроз, защиту внутри и снаружи сети, динамическое обновление, блокировку по домену на всех портах, также имеет встроенные настраиваемые API интеграции. Сервис представляет механизм защиты и фильтрации DNS запросов. При этом механизм является облачным и не требует установки туннеля с сетью компании, благодаря чему пользователь является защищенным вне зависимости от своего географического положения [1].

Сервис Investigate обеспечивает аналитику благодаря которой обеспечивается фильтрация доступа. С помощью нее можно обнаруживать и даже предугадывать всю инфраструктуру атакующего. Для анализа используется информация, полученная от следующих инструментов:

– база пассивной информации DNS это информация об истории регистрации DNS имён, инфраструктуры, которая была привязана к ним. Также при анализе учитывается атрубуты BGP и автономные системы, привязанные к ним;

– WHOIS представляет из себя базу данных с информацией о владельцах доменов и их изменениях. Благодаря этой базе можно проанализировать зарегистрированные на пользователя домены и если они являются вредоносными, то сделать вывод о новых доменах этого пользователя;

– репутация поведенческого анализа, обнаруженная различными движками моделирования поведения.

– атрибуция автономных систем BGP – база автономных систем, замеченных за вредоносной активностью;

– IP геолокация – функция, которая позволяет выяснить и проанализировать расположение инфраструктуры атакующего, в том числе географически;

– индексы репутации для IP адресов – механизм, позволяющий отследить регистрацию вредоносных доменов на одном IP адресе.

Рассмотрим некий экскурс в том, каким образом вредоносная программа получает доступ к своим C&C серверам. Очень старая методика – это статически заданный адрес C&C сервера к которому вредоносная программа подсоединялась, но защититься от такого достаточно легко. Нужно просто закрыть на межсетевом экране IP адрес или серию IP адресов к которым подсоединяется ботнет [2].

Следующая технология называется Fast Flux. В этом случае существует одно доменное имя, которое с высокой частотой меняет разрешение на IP адрес. Таким образом обращение идёт к доменному имени, но IP адреса очень часто меняются. Для борьбы с этим необходимо закрыть обращение

к домену, что тоже не сложно, однако требует более глубокого анализа трафика.

Следующий этап развития – это механизм генерации доменов (DGA). Он появился в 2007 г. во вредоносной программе Conficker. Данный метод не имеет статически заданных IP адресов или доменных имен. В нём используется инфраструктура C&C серверов, которые посылают обновления вредоносной программе, которые подписаны сертификатом. Каждый день такая инфраструктура может сгенерировать порядка 50000 абсолютно случайных доменных имён и загружать их на вредоносную программу. При этом для противодействия этому способу нужно регистрировать все эти 50000 DNS имён, что фактически невозможно. При этом сама C&C инфраструктура регистрируется примерно на 1 % имен (500), но этого вполне достаточно чтобы 1 раз в день соединиться с C&C сервером и получить очередное обновление.

Компонент Investigate имеет следующие механизмы анализа доменных имён и запросов к ним:

Статистическое моделирование. Система работает по модели статистического моделирования, и использует три главных шаблона (модели поведения), которые в свою очередь разбиваются на аналитические модели.

1) Виновность по поведению:
    a. Модель совместных запросов.
    b. Геолокационная модель.
    c. Модель индекса безопасности.
2) Виновность по связям:
    a. Модель предсказуемого IP сегмента.
    b. Корреляция DNS и WHOIS данных.
3) Шаблон виновности:
    a. Модель всплесков активности.
    b. Модель оценки языкового шаблона (NLP).
    c. Обнаружение DGA.

Модель совместных запросов. В данном случае анализируется за короткий промежуток времени доменов, рядом стоящих с известным вредоносным доменом. Набирается статистически значимое количество запросов на разных хостах в мире и если оно превышает определённый порог можно сделать вывод о том, что данный домен является частью инфраструктуры атакующего.

Модель всплесков активности. Распознаются поведенческие шаблоны известных вредоносных активностей. По поведению возможно узнать не только используемую в данный момент инфраструктуру, но и ту, которая подготавливается

Мониторинг предсказуемого IP сегмента. Система отслеживает домены со схожими отпечатками активности, зарегистрированными на этих IP

адресах, а также определяет какие атаки могли быть с ними ассоциированы, после чего проводится блокировка доменов и ассоциированных с ними ресурсов.

Корреляция DNS. При анализе цепочки DNS запросов, можно обнаруживать не только инфраструктуру атакующего, но и сайты, которые являются легитимными, но были скомпрометированы.

Пассивная DNS информация даёт возможность отследить то, как проходила атака с течением времени, как изменялась инфраструктура, какие сервера и в каких регионах использовались для проведения атаки, какие IP адреса подключались к инфраструктуре. Анализ этих данных позволяет строить графы развертывания инфраструктуры атакующего и предугадывать его действия.

Геолокационный анализ. Оценивается географическая привязка IP адресов, ассоциированных с доменом.

Модель языкового моделирования. В именах вредоносных доменов часто содержатся имена известных производителей или похожие на них. Система определяет, кому принадлежит домен и на основе этого выносит решение о блокировке.

Обнаружение алгоритмов DGA. DNS имя ассоциируется с неким языковым шаблоном (есть ли какие-нибудь взаимосвязи между символами), после чего проверяется, не было ли имя сгенерировано случайно.

Внедрение системы можно произвести несколькими способами.

Самое простое решение – это указать на компьютере или на DHCP сервере выдавать IP адрес OpenDNS инфраструктуры. Однако этот метод неудобен если требуется обращаться к внутренним доменам.

Если существуют какие-нибудь внутренние ресурсы, имена к которым нужно разрешать, то можно настроить переадресацию на DNS сервере чтобы разрешение внешних доменов проходил на OpenDNS инфраструктуре.

Если требуется интеграция с AD, написание политик доступа и фильтрации исходя из членства пользователей в группах – развертывается виртуальная машина с виртуальным аплаенсом Umbrella, она указывается как основной DNS сервер для сети, при это из инфраструктуры Umbrella на эту виртуальную машину спускается список внутренних доменов, для которых будет выполняться переадресация DNS запросов на корпоративный DNS сервер

Помимо этого, есть роуминг клиент, который загружается из OpenDNS облака и может раздаваться через групповые политики и устанавливаться на компьютеры конечных пользователей. Также из облака будет синхронизироваться список корпоративных доменов Благодаря этому происходит защита пользователей находящихся вне корпоративного периметра.

Список используемых источников

1. Казаков Д. OpenDNS [Электронный ресурс] // Cisco Club [сайт]. 23.11.2016. URL: http://ciscoclub.ru/opendns (дата обращения 14.02.2017).
2. UDP Flood (англ.) // DDoS Attack Glossary (Incapsula, Inc.).

УДК 004.72

ИСПОЛЬЗОВАНИЕ ИНФРАСТРУКТУРЫ, ОРИЕНТИРОВАННОЙ НА ПРИЛОЖЕНИЯ КОМПАНИИ CISCO SYSTEMS INC. В СОВРЕМЕННЫХ СЕТЯХ ЦОД

А. В. Красов, Н. В. Савинов, И. А. Ушаков

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

В настоящей статье приведен обзор технологии компании Cisco Systems – ACI, применяемой для построения сетей центров обработки данных. Освещаются предпосылки модернизации сетей дата центров. Рассмотрены принципы построения подобных сетей: топология Leaf-and-Spine, аппаратная и программная части ACI-фабрики, использование контроллера APIC, применение политик и профилирование приложений. Описаны преимущества внедрения ACI-фабрики с точки зрения информационной безопасности. Приведено сравнение концепции ACI с концепцией SDN.

центр обработки данных, информационная безопасность, инфраструктура, ориентированная на приложения ACI, Cisco Systems, ACI-фабрика, контроллер APIC, политики, профиль приложения.

В настоящее время для сетей связи имеет огромное значение организация центров обработки данных (*datacenters*). Дата центры представляют собой сложную систему, включающую как телекоммуникационное оборудование, так и, главным образом, систему хранения данных. При организации сетей ЦОД важную роль играют создание надежной системы электропитания, резервные линии связи, способные передавать огромные потоки данных, система охлаждения, а также системы информационной безопасности, главными задачами которых является ограничение неправомерного доступа к данным, их защита от изменения и удаления [1]. От производительности, отказоустойчивой и постоянной работы центров обработки данных напрямую зависят интересы компаний, например, быстрое подключение к сети Интернет и безостановочное функционирование в этой сети. Таким образом, при остановке работы ЦОД в корпоративных сетях неизбежно появятся проблемы с производительностью, а, возможно, и полный отказ работы,

что несомненно приведет к большим материальным затратам. С появлением и развитием облачных вычислений (*cloud computing*) и необходимостью обработки колоссальных объемов информации – введение термина «большие данные» (*big data*) [2], в сфере информационных технологий появляются тенденции к модернизации и усовершенствованию ЦОД, поиск новых подходов к улучшению их инфраструктуры и повышения их производительности [3]. Одним из подобных подходов является проприетарное решение компании Cisco Systems Inc. – использование инфраструктуры сетей ЦОД, ориентированной на приложения. Под приложениями в данной инфраструктуре принимаются «облачные» сервисы, с большим числом пользователей и огромным потоком проходящего трафика.

ACI (Application Centric Infrastructure) – инновационный метод организации архитектуры сети дата центров, использующий целостный системный подход с тесной связью физической и виртуальной составляющей ЦОД. ACI существенно оптимизирует и упрощает весь процесс развертывания приложений, использует общую политику функционирования и упрощает управление с точки зрения сети, приложений, безопасности и информации [1]. Предпосылки создания новой архитектуры возникли с увеличением объемов обрабатываемой информации, а также с развитием систем виртуализации: стало понятно, что широко используемая трехуровневая модель организации сети (доступ, распределение, ядро) не подходит для сети центров обработки данных, так как данные сети очень специфичны – высокая нагруженность MAC-адресов, так как одному физическому порту сервера может соответствовать множество виртуальных MAC-адресов, необходимость легко увеличивать количество сетевых элементов, при этом сохраняя простоту дизайна сети, а также обеспечение избыточных связей для простого обмена потоками трафика внутри ЦОД (так называемый «*east-west traffic*» [4]).

В основе ACI лежит архитектура Leaf-and-Spine, представленная на рис. 1.

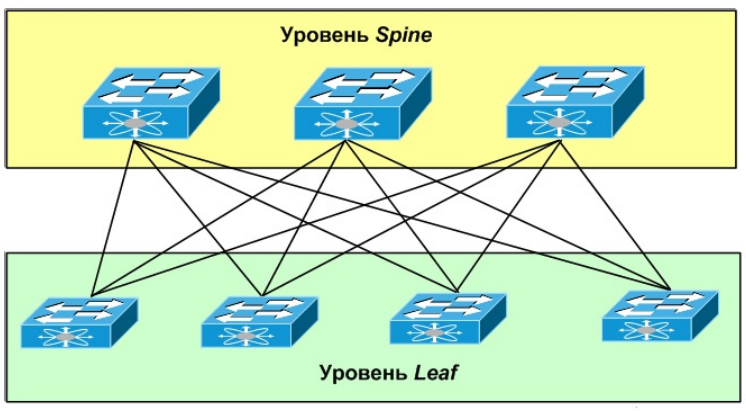


Рис. 1. Архитектура Leaf-and-Spine

В качестве коммутаторов ACI Spine используются коммутаторы компании Cisco Systems Inc. серии Nexus 9508 или 9336PQ [4]. Данные мощные коммутаторы специально разработаны для эксплуатации в сетях ЦОД как традиционного типа, так и сетей ACI, а также обеспечивают высокую плотность агрегирования трафика и поддерживают интерфейсы с пропускной способностью 1, 10, 25, 40, 50 и 100 Gigabit Ethernet.

Коммутаторы уровня Spine называют коммутаторами уровня ядра или магистральными коммутаторами, а в свою очередь сеть ЦОД на основе архитектуры ACI называют ACI-фабрикой (ACI-fabric), так как значениями английского слова «fabric» могут быть «ткань» или «структура». В качестве коммутаторов уровня Leaf, или же периферийных коммутаторов, используются коммутаторы компании Cisco Systems Inc. серии Nexus 9396PX, 9396TX или 93128TX, поддерживающие интерфейсы с пропускными способностями 1, 10 и 40 Gigabit Ethernet. Отличительной особенностью таких фабрик, как ACI, является то, что устройства уровня Leaf соединяются только с устройствами уровня Spine, и никаких соединений между устройствами одного и того же уровня [5].

Коммутаторы уровней Leaf and Spine почти полностью представляют собой аппаратную основу ACI-фабрики, но она также включает в себя контроллер Cisco APIC (*Application Policy Infrastructure Controller*), а программной основой становятся виртуальный коммутатор приложений AVS (*Application Virtual Switch*) и различные типы гипервизоров, например, VMWare [4]. Для всей фабрики именно контроллер APIC становится единым средством управления и контроля всей сетевой инфраструктуры. В его задачи входит предоставление доступа к конфигурациям устройств, управление, мониторинг инфраструктуры, отслеживание жизненного цикла приложений и устранение неполадок. Использование данного централизованного контроллера с программируемым интерфейсом API (*Application Programming Interface*) обеспечивает доступ на уровне приложений к физическим и виртуальным элементам ACI-фабрики посредством графического пользовательского интерфейса GUI (*Graphical User Interface*), интерфейса командной строки CLI (*Command Line Interface*) или API (*Application Programming Interface*) [6]. В фабрике каждый отдельный узел – магистральный или периферийный коммутатор, получают уникальный идентификатор, который позволяет устройству загрузить соответствующие конфигурационные атрибуты с контроллера.

Всю ACI-фабрику можно условно разделить на три составляющих: аппаратная часть сети, политики фабрики (*fabric policies*) и политики доступа (*access policies*). Назначением данных политик является регулирование внутреннего взаимодействия между узлами фабрики, регулирование внешнего взаимодействия между Leaf-узлами фабрики и серверами, сетевым оборудованием и хранилищами. В свою очередь политики можно

разделить на политики, настраиваемые на интерфейсах (в дальнейшем объединяются в группы политик интерфейсов) и политики коммутаторов (аналогично объединяются в политику группы коммутаторов). В идеале политика, подобно шаблону, прописывается только один раз, а в дальнейшем лишь настраивается на новых устройствах, и они добавляются в соответствующую политику группы. На рис. 2 приведена основная структура направлений использования APIC.

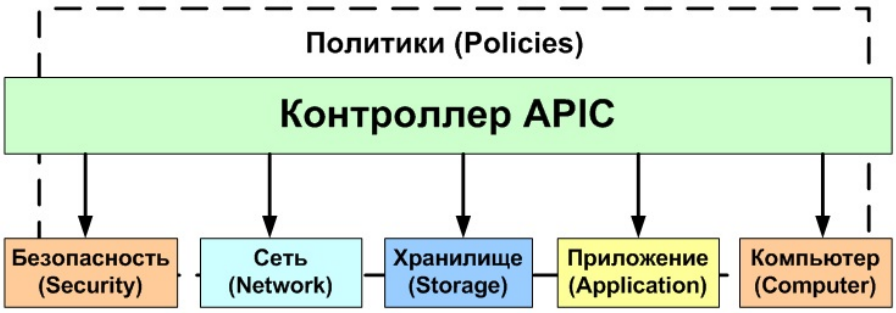


Рис. 2. Общая структура функций APIC

Одним из главных преимуществ ACI-фабрики является ее легкая расширяемость, в виду использования простой модели Leaf and Spine и мощных коммутаторов, поддерживающих скорости 40 и 50 Gigabit Ethernet (в дальнейшем при росте объемов обрабатываемого трафика и расширяемости сети, данные коммутаторы могут поддерживать сетевые интерфейсы со скоростями 100 Gigabit Ethernet, однако, на данный момент развития сети ЦОД не нуждаются в такой огромной пропускной способности). Также предпосылкой для расширяемости ACI-фабрики становится использование подхода к централизованному управлению. Данное решение не просто дает возможность расширять сеть, но и «растягивать» ее — две территориально отдаленных фабрики (например, в двух разных зданиях дата центров) становятся одной большой фабрикой, называемой «растянутой фабрикой» (*stretched fabric*) [6].

К достоинствам ACI относится высокий уровень автоматизации функционирования и управления всей ACI-фабрикой, связанный с применением политик: администратор сети отдает контроллеру APIC почти полную «власть», и тот следит за состоянием фабрики, получает информацию о трафике и его балансировке в сети и обеспечивает должный уровень безопасности сети. Другими словами, задача администратора ACI-фабрики создать профиль приложения на основе политик, в котором ему необходимо указать все необходимые настройки и передать его контроллеру APIC, который запрограммирует соответствующие коммутаторы согласно с этим профилем приложений. Использование программной настройки сетевых элементов

означает перенос большой доли администрирования в программную плоскость, то есть в плоскость управления. В концепции сетей SDN лежит отделение управления сетевых устройств от самих этих устройств и наделение функцией управления сетевыми устройствами лишь сетевой контроллер, который и является главнейшим элементов плоскости управления сети. Решение инфраструктуры, ориентированной на приложения от компании Cisco Systems Inc. имеет много общего с программно-конфигурируемыми сетями SDN, но главным отличием является то, что решение ACI является проприетарным. Вся ACI-фабрика строится исключительно на основе оборудования, выпускаемого компанией Cisco Systems Inc. – линейке коммутаторов Nexus, которые являются довольно сложными и дорогими устройствами, имеющими возможность работать как в режиме ACI-фабрики с централизованным управлением, так и в другом режиме со своей собственной плоскостью управления, в то время как концепция сетей SDN независима от вендоров и стремится к упрощению и удешевлению сетевых устройств.

В итоге, подход компании Cisco Systems Inc. к организации сетей ЦОД взял самое лучшее из концепций программно-конфигурируемых сетей SDN и традиционных сетей. ACI обладает рядом важных преимуществ, таких как легкая расширяемость, централизованное аппаратное управление, высокая производительность и информационная безопасность.

Список используемых источников

1. Андрианов В. И., Красов А. В., Липатников В. А. Инновационное управление рисками информационной безопасности. СПб. : СПбГУТ, 2012. 396 с.

2. Дубровин Н. Д., Ушаков И. А., Чечулин А. А. Применение технологии больших данных в системах управления информацией и событиями безопасности // Актуальные проблемы инфотелекоммуникаций в науке и образовании. V международная научно-техническая и научно-методическая конференция: сб. науч. ст. СПб. : СПбГУТ, 2016. С. 348–353.

3. Красов А. В., Левин М. В., Цветков А. Ю. Метод управления трафиком в гибридной программно-определяемой сети // Информационные технологии и телекоммуникации. 2016. Т. 4. № 2. С. 53–63.

4. Sanchez A., Vega A., Chari A. Operating Cisco Application Centric Infrastructure, Cisco Press, 2015, 456 p.

5. Eriksson J., Hedlund R. Cisco ACI and VMware NSX, a comparison between Software Defined Networks. 2016.

6. Официальный сайт Cisco Systems Inc. URL: http://www.cisco.com/c/ru_ru/solutions/data-center-virtualization/application-centric-infrastructure/ (дата обращения: 19.01.2017).

УДК 004.7

ВАРИАНТ ПОВЫШЕНИЯ УСТОЙЧИВОСТИ ФУНКЦИОНИРОВАНИЯ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ В УСЛОВИЯХ ВНЕШНИХ УГРОЗ

С. И. Кузнецов, О. А. Остроумов, Е. В. Сухорукова, С. П. Тесля

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

Статья посвящена устойчивости функционирования телекоммуникационных сетей. Проведен краткий анализ угроз таким сетям и представлен способ защиты логической структуры информационно-телекоммуникационных сетей. Предложен вариант защиты логической структуры, позволяющий повысить безопасность и скрытность работы каналов связи за счет усложнения процедуры определения адресов.

информационно-телекоммуникационная сеть, линейные системы, устойчивость, внешние угрозы.

Построение информационно-телекоммуникационных сетей (ИТКС) на перспективных технологиях, использование сетевых ресурсов Единой сети электросвязи Российской Федерации (ЕСЭ РФ), приводит к возникновению угроз информационной безопасности, которые свойственны ИТКС гражданского назначения.

В настоящее время на территории разных зарубежных стран действуют специальные подразделения и информационно-аналитические центры, в задачи которых входит организация доступа в компьютерные системы и сети, перехват, обработка и анализ данных, циркулирующих в ИТКС РФ. Добывание сведений об ИТКС включает в себя сбор информации о структуре ИТКС, алгоритмах ее функционирования, применяемом телекоммуникационном оборудовании, топологической привязке логической структуры ИТКС и ее узлов и т. п., и достигается выполнением различного рода мероприятий.

Применение комплекса различных средств позволяет специальные подразделения и информационно-аналитическим центрам осуществлять [1]:

несанкционированный доступ к узлу или логической структуре (ЛС) ИТКС с целью удаленного контроля, обеспечения дальнейших действий, а также использования скомпрометированных узлов или ЛС ИТКС в качестве плацдарма для атаки;

анализ таблиц маршрутизации оборудования ИТКС;

анализ трафика, проходящего через узлы (в том числе и технологического) или входящего/исходящего трафика ЛС ИТКС;

сканирование узлов и ЛС ИТКС на предмет определения типа оборудования, версий программного обеспечения;

анализ конфигураций сетевого оборудования (после НСД);

анализ топологии ИТКС.

Обеспечение безопасности ИТКС предполагает в первую очередь защиту ее со стороны внешних угроз, направленных на нарушение ее нормального функционирования.

Наиболее опасными и самыми распространенными угрозами несанкционированного воздействия являются сканирование сети и отказ в обслуживание, в частности DDos атака. Полностью защититься от DDoS-атак на сегодняшний день невозможно. Однако, на настоящий момент существует масса как аппаратно-программных средств защиты, так и организационных методов противостояния [1].

Основными целями противодействия злоумышленнику (противнику) являются: нейтрализация (ослабление) несанкционированных деструктивных воздействий противоборствующей стороны на информационные объекты ИТКС; поддержание противоборствующей стороны в полном или частичном неведении путем лишения его необходимой информации; введение противоборствующей стороны в заблуждение путем создания условий для сбора ложной информации от ИТКС [1].

Основными направлениями достижения указанных целей являются: защита ИТКС путем повышения устойчивости ее функционирования в условиях применения противоборствующей стороны «информационного оружия»; противодействие подразделениям и информационно-аналитическим центрам путем дезорганизации ее действий.

Наряду с требованиями по защите информации от НСД и вредоносного программного обеспечения очень актуально решение задач противодействия с целью реализации процессов предотвращения воздействий на элементы ИТКС.

Существующие методы и способы защиты ЛС адресного пространства ИТКС от несанкционированного воздействия [2] позволяют выделить следующие характерных недостатки: вероятность выделения каналов связи, за счет прослушивания и реконструкции трафика в некоторой точке ИТКС путем идентификации адресов корреспондентов; низкую скрытность связи вследствие увеличения вероятности распознавания структуры сети ИТКС за счет обнаружения идентификаторов ее элементов при информационном обмене; выделение диапазона IP-адресов, используемых для формирования канала передачи данных, за счет маршрутизации пакетов по общему маршруту сети, прослушиванию трафика в нескольких точках сети, приближенных к отправителю и получателю пункту, и реконструкции его.

Целью предлагаемого варианта является повышение безопасности и скрытности работы канала связи за счет усложнения процедуры определения адресов и выявления взаимосвязей удаленных сегментов распределенных сегментов ИТКС при анализе трафика в некоторой точке сети.

Вариант изменения ЛС адресного пространства реализуется следующим образом.

Для передачи информации между удаленными сегментами сети ИТКС (например, ЛВС1 и ЛВС2 ИТКС) посредством протоколов взаимодействия устанавливают канал связи, под которым, в данном случае, понимают информационный поток от отправителя к получателю.

Информационный поток от ЛВС1 к ЛВС2 передают через соответствующие маршрутизаторы и сеть связи общего пользования. В процессе установления соединения отправителю и получателю необходимо произвести согласование сетевых адресов. Для этого у всех корреспондентов предварительно задают базу, включающую IP-адреса первого сетевого адаптера $A1_{ск}$ и индивидуальные ключи Хэш-функции ПК взаимодействия, за них принимают все элементы, не своей ЛВС.

На начальном этапе подключают два сетевых адаптера к сети связи общего пользования с динамической адресацией в выделенном диапазоне IP-адресов для организации связи, через различные точки доступа (под которыми подразумеваются точки доступа различных провайдеров услуг связи сети общего пользования). Формируют в постоянно запоминающих устройства базу данных, включающую адреса всех элементов взаимодействия и их индивидуальные ключи (инициализирующие векторы) Хэш-функции. Затем записывают данные в постоянно-запоминающем устройстве. Аналогичные действия производятся на всех элементах взаимодействия.

Первоначально производится согласование адресов всех рабочих станций между собой, для этого у отправителя формируют пакет согласования. Затем формируют промежуточный пакет, для чего в зарезервированное поле пакета согласования включают обратный адрес отправителя $A_{обр.отпр.}$ В информационной части пакета указывается принадлежность этого пакета к пакетам согласования.

После чего кодируют любым из известных способов кодирования, например, как представлено в [3], полученный промежуточный пакет и рассчитывают значение Хэш-функции от исходного пакета, затем включают рассчитанное значение Хэш-функции от пакета согласования и преобразуют его в формат TCP/IP. Далее делают запрос на прокси-сервер. В результате чего получают цепочку свободных IP-адресов, состоящую из определенного количества взаимодействующих прокси серверов. Для полученных адресов происходит тройное инкапсулированние, то есть сначала инкапсулируется пакет для третьего сервера, затем для второго и только потом для первого и т. д. В поля адрес отправителя включают адрес отправителя

$А_{отпр}$, в поля адрес получателя включают адрес первого сервера. Кодируют пакет, путем добавления ключа и служебной информации. Закодированный пакет передают первому серверу и т. д.

Во время создания пакета сервер устанавливает свой IP-адрес. Передают сформированные информационные пакеты сообщений всем ПК взаимодействия, записывают время отправления каждого пакета в базе данных оперативно-запоминающего устройства.

После приема у получателя пакета согласования из его заголовка выделяют адреса отправителя $А_{отпр}$, выделяют из постоянно-запоминающего устройства ключ Хэш-функции, соответствующую данному адресу и находят ее значение от информационной части пакета и сравнивают их (например, побитно) со значением Хэш-функции, рассчитанной от пакета согласования. При несовпадении значений Хэш-функции принятый пакет не анализируют, т. к. его отправитель не является санкционированным участником информационного обмена. При совпадении значений из принятого пакета сообщений выделяют кодированные данные путем отделения IP-заголовка.

Для подтверждения факта получения от отправителя пакета у получателя формируют уведомляющий пакет сообщений, представляющий собой уведомление о получении пакета согласования. Затем к пакету добавляют обратный адрес ПК взаимодействия $А2_{ск}$ ($А_{обр.тр}N$ или $А_{получ.обр}$), составляющий 32 бита информации, предварительно зафиксированный в таблице получают промежуточный пакет данных и т. д.

Для смены IP-адреса рабочей станции отключают сетевой адаптер от точки доступа. Изменяют MAC-адрес (адрес физического уровня) сетевого адаптера (или иного физического устройства, осуществляющего подключение к сети). Вновь подключают его к точке доступа. За счет того, что время жизни прежней связки адресов MAC-IP на сервере провайдера (поставщика услуг) не истекло и считается активным, получаем новый IP-адрес рабочей станции, отличный от предыдущего. Записывают в базу данных постоянно-запоминающего устройства значение нового IP-адреса, с пометкой $А_{обр.тр}$, а значение второго IP-адреса с пометкой $А_{тр}$ и т. д.

Затем осуществляется обмен информацией по существующим виртуальным каналам. Для контроля и распределения пакетов по виртуальным каналам на стороне отправителя применяется набор условий, определяющий порядок передачи пакетов, а именно выбор адреса транзита и количество пакетов сессии, через каждый адрес транзита, с этой целью считается количество отправленных пакетов, проверяется соответствие количества пакетов данной сессии выбранному адресу транзита, при превышение ими предельного, рассчитанного числа ΔSN, изменяют условный номер выбранного виртуального канала N следующее значение, в соответствие с которым и выбирают значение текущего адреса получателя $А_{обр.тр}\,N$.

После приема у отправителя уведомляющего пакета из его постоянно-запоминающего устройства выделяют адреса ПК взаимодействия $А_{тр}N$, выделяют ключ Хэш-функции, соответствующий данным адресам и находят ее значение и т. д., включающих данное значение Хэш-функции, рассчитанной на ПК взаимодействия и сравнивают их (например, побитно) со значением Хэш-функции с ключом, выделенным из постоянно-запоминающего устройства, от информационного пакета. При несовпадении значений Хэш-функции принятый пакет не анализируют, т. к. отправитель не принадлежит к числу санкционированных участников информационного обмена. При совпадении пакет принимают к обработке из принятого пакета сообщений выделяют кодированные данные путем отделения IP-заголовка и декодируют их. Из первых 64ех бит информации уведомляющего пакета выделяют значение обратного IP-адреса транзита $А_{обр.тр}N$ и отправителя $А_{обр.получ}$ и записывают их в постоянно-запоминающее устройство. Увеличивают количество принятых отчетов о доставке пакета ΔD на $\Delta D = \Delta D + 1$. Изменяют IP-адрес рабочей станции элемента отправителя, для чего отключают сетевой адаптер от точки доступа. Изменяют MAC-адрес (адрес физического уровня) сетевого адаптера (или иного физического устройства, осуществляющего подключение к сети). Вновь подключают его к точке доступа. Записывают в базу данных постоянно-запоминающего устройства значение нового IP-адреса, с пометкой $А_{обр.тр}$, а значение второго IP-адреса обозначают пометкой $А_{тр}$. Затем формируют новый информационный пакет.

Предложенный вариант изменения ЛС адресного пространства заключается в расширении адресного пространства элементов ИТКС, тройной инкапсуляции пакетов, организации маскирующего обмена между ложными и реальными сетевыми устройствами элементов ИТКС, а также введении действий по восстановлению связи в маскированной структуре ИТКС, обеспечивает повышение скрытности за счет маскирования ЛС адресного пространства, маршрутов передачи сообщений, адресов отправителя и получателя и снижения сложности обеспечения доступности сетевых устройств, в условиях воздействия, путем ведения действий по восстановлению связи в случае нарушения синхронизации выбора адресов при приеме и передаче пакетов сообщений.

Список используемых источников

1. Максимов Р. В. Контроль безопасности информации в информационно-вычислительных сетях. В кн. Контроль безопасности связи и информации: учеб. пособие / В. С. Киреев, О. К. Савицкий, Ю. И. Стародубцев, М. М. Тараскин; Под ред. Е. А. Карпова. СПб. : ВУС, 2002.

2. Олифер В. Г. и Олифер Н. А. Компьютерные сети. Принципы, технологии, протоколы. уч. для вузов, 2-изд. СПб. : Питер, 2003. 863 с.

3. Синюк А. Д., Остроумов О. А. Протокол открытого формирования трехстороннего ключа // Наукоемкие технологии в космических исследованиях Земли. 2013. Т. 5. № 1. С. 20–24.

УДК 621.396.2

ВЗАИМОУВЯЗАННАЯ СЕТЬ РАДИО, РАДИОРЕЛЕЙНОЙ, ТРОПОСФЕРНОЙ И СПУТНИКОВОЙ СВЯЗИ В АРКТИКЕ

И. А. Кулешов, В. В. Шевченко

ПАО «Информационные телекоммуникационные технологии»

В статье сделан анализ факторов, влияющих на организацию связи в Арктике, разработана взаимоувязанная сеть радио, радиорелейной, тропосферной и спутниковой связи для Арктической зоны, которая может лечь в основу (как образец) организации связи на островных и материковых базах, сделано предложение о применении перспективной технологии Wi-Fi.

Арктика, радио, радиорелейная, тропосферная связь, спутниковая связь, радиосвязь на средних и коротких волнах, взаимоувязанная сеть радиосвязи, технологии Wi-Fi.

Арктическая зона России в целом представляет собой колоссальный сырьевой резерв и относится к числу немногих регионов мира, где имеются практически нетронутые запасы нефти, газа и минерального сырья.

Прилегающие к России Арктические территории требуют защиты. Надежное управление объектами и структурами требует современной постоянно действующей связи.

На создание системы связи и организацию связи в Арктике влияют следующие факторы [1]:

1. Значительные водные просторы, ледовые территории и тундра. В акватории Арктики не много островов, которые находятся на больших расстояниях между собой и материковой частью.

2. Суровые климатические условия. Температура воздуха опускается до минус 55°÷60°. Близки к 0° средние температуры летних месяцев. Для Арктики характерны полярные дни и ночи.

3. Отсутствие сети транспортных дорог в тундре. Сообщения между населенными пунктами возможны водным транспортом во время короткой навигации с мая по сентябрь или авиацией.

4. В Арктической зоне часто возникают полярные сияния, так называемые «полярные шапки». Магнитные и ионосферные бури отрицательно влияют на распространение коротких радиоволн.

Эти факторы необходимо учитывать при строительстве систем связи.

В настоящее время в Арктике создаются новые материковые и островные базы. Учитывая климатические и физико-географические условия для организации управления на объектах, предлагается строить взаимоувязанную сеть радиосвязи, представленную на рисунке.

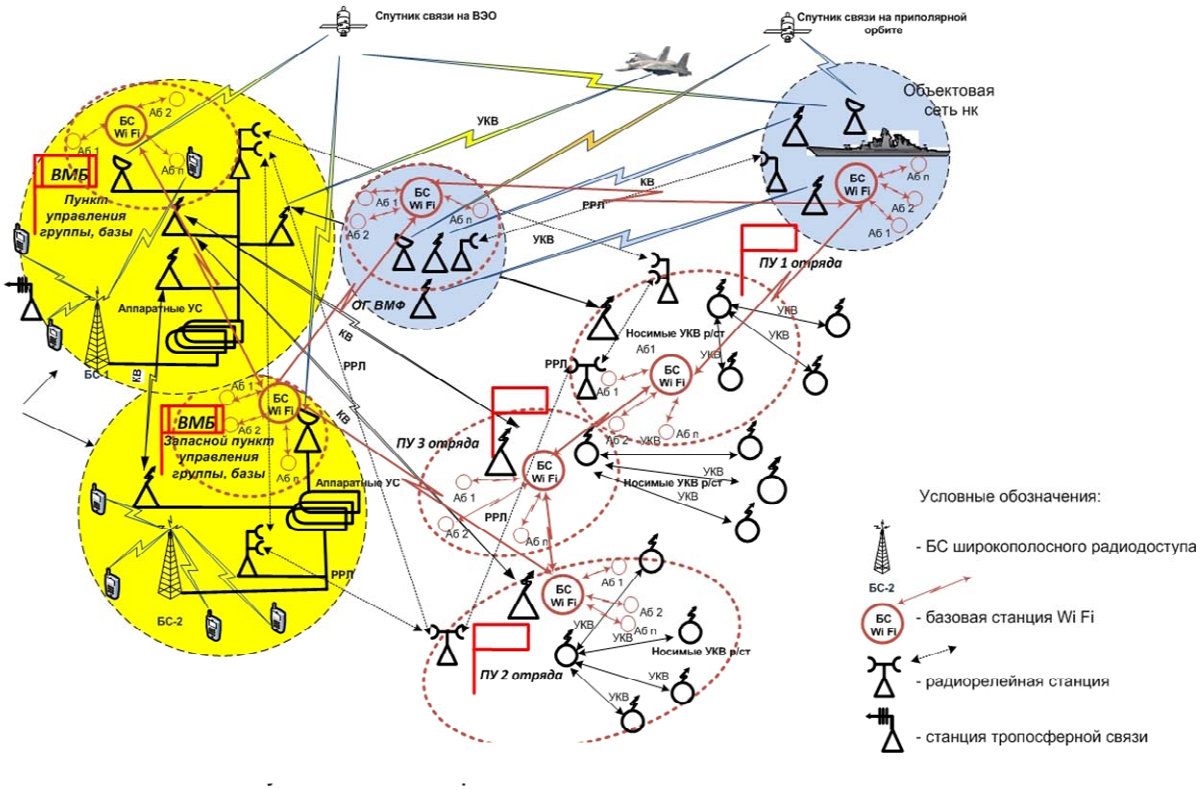


Рисунок. Взаимоувязанная сеть радио, радиорелейной, тропосферной и спутниковой связи в Арктике

От высших звеньев управления с пунктами управления баз необходимо организовать спутниковую связь. В зависимости от расположения баз использовать спутники связи на геостационарной орбите – до 75° с. ш. (Ямал, Экспресс, Гонец) и севернее 75° – спутники на ВЭО Меридиан и на приполярной орбите Гонец. В перспективе можно будет использовать ресурсы разрабатываемых сетей спутниковой связи Арктика, Элипс и RGS-B [2].

В качестве оконечных станций спутниковой связи предлагается использовать Р-441, Р-444-ПТН и Р-444-ПТД.

От пунктов управления баз с объектами рекомендуется организовать следующие виды связи:

– радиорелейную связь с помощью специальных мобильных комплексов (СМК-О, СМК-В, производства радиозавода им. А. С. Попова), с пропускной способностью 8–34 Мбит/с и дальностью связи до 30 км или Р-419Л1, обеспечивающих и радиорелейную связь и организацию локальной соты мобильной связи стандарта GSM/DCS с возможностью выхода абонентов в легитимные сети сотовой связи, сети радиорелейной, проводной, спутниковой связи и УКВ радиосвязи;

– радиодоступ с помощью базовых (БС) станций «Мир» на дальность до 40 км, номерной емкостью более 1300 абонентов;

– КВ радиосвязь земной волной до 40 км.

На объектах организуется радиодоступ и УКВ радиосвязь с помощью абонентских носимых станций.

Между объектами организуется радиорелейная связь, КВ и УКВ радиосвязь.

На расстояниях до 200 км возможна тропосферная связь с помощью контейнерных цифровых станций тропосферной связи Р-423-АМК, работающих в частотном диапазоне 4,4–5 ГГц, с пропускной способностью до 2048 кбит/с.

Возможна организация тропосферной связи с помощью малогабаритной перевозимой цифровой станции диапазона 4,4–5 ГГц «Сосник-4ПМ» с антенной диаметром 1,5 м, обеспечивающей с пропускную способность до 512 кбит/с.

Применение перспективной технологии Wi-Fi

В перспективе возможно применение широкополосных радиосредств, обеспечивающих высокие скорости передачи, по технологии Wi-Fi (стандарт IEEE 802.11).

Технология Wi-Fi позволяет обеспечивать передачу сигнала с полосой до 60 МГц, адаптивно в зависимости от помеховой обстановки изменять скорость работы. Применяемые виды модуляции – DBPSK, DQPSK, CCK, PBCC, BPSK, QPSK, 16QAM, 64QAM. Канальная скорость передачи – 1; 2; 5,5; 6; 9; 11; 12; 18; 22; 24; 33; 36; 48; 54 Мбит/сек.

Дальность связи на ненаправленные антенны может быть до 10 км. Радиостанции УКВ-ДЦВ диапазона в режиме широкополосного радиодоступа вполне смогут заменить радиорелейные станции. Применяя ненаправленную антенну, можно строить объектовые сети связи на пунктах управления, узлах связи, объектах различного назначения, судах и кораблях. Варианты применения сетей радиодоступа Wi-Fi представлены на рисунке (см. выше).

ООО «СТЦ» представлен модельный ряд оборудования на базе технологии Wi-Fi (стандарты IEEE 802.11a/b/g/n) с возможностями технологий LTE и GPRS/EDGE в виде двух платформ – для военной и гражданской

связи, с применением протоколов со скоростью передачи фактических данных до 300 Мбит/с на один радиоинтерфейс. Диапазоны рабочих частот от 200 МГц до 6425 МГц. Полосы рабочих частот – 2.5, 5, 10, 20, 40, 60 МГц. Шаг сетки рабочих частот от 1 до 5 МГц. Мощность передатчика от 50 мВт до 1 Вт.

При создании современной телекоммуникационной инфраструктуры в Арктике целесообразно применять SDR-технологии. Некоторые аспекты SDR-технологий в системе связи ВМФ изложены авторами в сборнике трудов «Радиотехника, электроника и связь» [3].

Заключение

Организацию связи в Арктике усложняют суровые климатические условия, отсутствие дорог, краткосрочная навигация, а также высокоширотные северные сияния, магнитные и ионосферные бури.

Тропосферная и радиорелейная связь возможна как на островах, так и между ними. Тропосферные и радиорелейные средства возможно применить для строительства осей и рокад связи на материковой и островной частях. Дальность связи определяется техническими возможностями оборудования: до 180 км тропосферный интервал и до 20–40 км – радиорелейный.

Радиосвязь возможна на средних и длинных волнах. Коротковолновая радиосвязь подвержена сильным замираниям и многолучёвости, поэтому возможна земной волной на небольшие расстояния. Для связи на дальние расстояния более 40 км необходимо использовать меридиональные КВ радиолинии с ретрансляторами.

УКВ радиосвязь возможна на короткие расстояния. На объектах возможно организовывать сотовую связь.

Спутниковая связь в Арктической зоне является приоритетной. С геостационарной орбиты возможна связь до 74°с. ш. На более высоких широтах возможна спутниковая связь только с высокоэллиптической орбиты.

Список используемых источников

1. Николашин Ю. Л., Кулешов И. А., Солозобов С. А., Шевченко В. В. Проблемы создания современной телекоммуникационной инфраструктуры в Арктической зоне // Интегрированные системы управления: сб. науч. тр., часть 2 / под ред. Э. Д. Павлыгина. Ульяновск : ФНПЦ АО «НПО «Марс», 2016. С. 125–136.

2. Шинкарев В. И., Липатов И. А., Николаенко В. М. и др. Особенности обеспечения спутниковой связи по высокоскоростным трактам в X диапазоне в районе Северного Полюса // Системы связи и радионавигации. Сборник тезисов II Всероссийской НТК / Под редакцией В. Ф. Шабанова. Красноярск : АО «НПП «Радиосвязь», 2015. С. 6–10.

3. Солозобов С. А., Шевченко В. В., Махортов Ю. Ф. Некоторые аспекты SDR-технологий в системе связи ВМФ // Сборник докладов III Международной научно-технической конференции «Радиотехника, электроника и связь». Омск : Издательский дом наука, 2015. С. 212–217.

УДК 004.056.53

МЕТОД ОБЕСПЕЧЕНИЯ ПОДЛИННОСТИ КУПЮР НА ОСНОВЕ КВАНТОВОЙ КРИПТОГРАФИИ

Д. В. Кушнир, М. В. Павлюкович

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

В настоящее время важной проблемой остаётся использование надёжных способов подтверждения подлинности банкнот. Существующие методы обладают рядом недостатков. В работе исследуется способ обеспечения подлинности банкнот на основе известных принципов квантовой криптографии, проводится анализ данного способа защиты и рассматриваются различные аспекты потенциального использования.

квантовая криптография, купюра, квантовая банкнота, обеспечение подлинности.

После 2014 г. наблюдается тенденция на резкое увеличение объема оборота наличности в РФ [1], несмотря на то, что к началу 2017 г. этот объем незначительно уменьшается, остается актуальным вопрос подтверждения подлинности банкнот.

В настоящий момент, в зависимости от номинала купюры, существует от девяти до двадцати признаков подлинности [2]. Даже с учетом того, что в обороте используются купюры образца 1997 г., самая последняя модификация, упоминаемая в открытых источниках, датируется 2010 г. Стоит отметить, что подобные модификации вносят минимальные косметические изменения на купюры. Это обусловлено как минимум тем, что каждая модификация требует обновления оборудования (в том числе путем утилизации предыдущего), что является весьма дорогостоящим процессом. Для проверки машиночитаемых признаков [3] подлинности банкнот также требуются разноплановые устройства [4] – ультрафиолет, лупа и т. д. Для проверки человекочитаемых признаков необходимо присутствие человека.

В качестве недостатков такого механизма подтверждения подлинности можно выделить высокую стоимость оборудования и модернизации, невозможность существенных косметических изменений, невозможность отказа от большего числа признаков подлинности, направленных на узнавание человеческим глазом, в том числе направленных на распознавание техническими средствами.

Качественно новым подходом к обеспечению подлинности наличности может служить квантовая банкнота [5], подтверждение подлинности кото-

рой основано на принципах квантовой криптографии. Стивен Визнер предлагал закреплять кванты на банкноте (такой способ крепления именовал ловушками) таким образом, чтобы их правильная поляризация была известна только банку, как и базис для их верного прочтения. Эта информация сопряжена с серийным номером купюры для удобства поиска. Теорема о запрете клонирования подразумевает, что злоумышленник не сможет скопировать такую банкноту, ничего о ней не зная, а неправильное считывание приводит к разрушению ловушек и невозможности восстановления.

На данный момент идея квантовой банкноты выглядит следующим образом: с использованием квантовых криптографических протоколов формируется уникальная последовательность фотонов, которые закрепляются на купюре [6] (не менее 100, на случай декогерентности).

Декогерентность может быть вызвана различными воздействиями со стороны окружающей среды, приводящими к нестабильности квантового состояния фотонов в ловушках.

Базис для считывания фотонов связан с серийным номером купюры. Описание банкноты (базис, состояния фотонов, номер купюры) хранятся в банке. Сначала считыватель обращается к банку для уточнения базиса, запрашивая его по номеру купюры. Если подобный номер купюры имеется, то банк высылает в ответ базис. В следующий раз считыватель и банк сравнивают положения фотонов. Если все верно – купюра легитимна. Схема взаимодействия считывателя и банка представлена на рисунке.

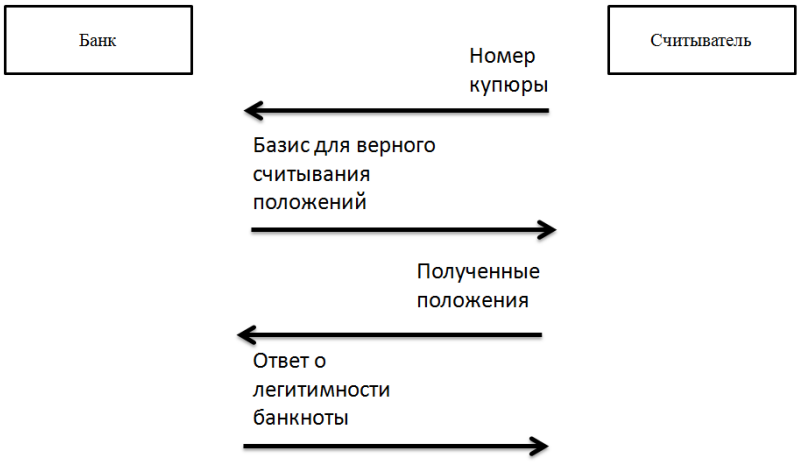


Рисунок. Схема взаимодействия банка и считывателя

При обороте банкноты, необходимо наличие не только считывателя, но и лазера, который будет как воспроизводить существующие метки, так и наносить новые (например, при выдаче сдачи или для повторного использования банкноты). Фотон разрушается после считывания, поэтому оба

устройства необходимы. В качестве эмитента может выступать не только Центральный банк Российской федерации (ЦБ РФ), но и партнеры [7].

При использовании квантовой банкноты в повседневном обороте, подразумевается нанесение метки лицензированным считывателем на пустую купюру, используя уже имеющуюся базу серийных номеров купюр и заранее проработанную последовательность.

Квантовые банкноты обладают рядом достоинств:

1. Невозможность подделки.

Теорема о запрете клонирования гласит, что создание идеальной копии произвольного неизвестного квантового состояния невозможно, что исключает возможность подделки купюры, ведь неизвестно, какую информацию несут в себе квантовые ловушки, которые разрушатся при любой попытке считывании, а злоумышленник также не сможет восстановить разрушенную ловушку.

2. Менее трудоемкий процесс производства и модификации признаков подлинности, в том числе сокращение числа признаков подлинности.

Подразумевается, что квантовая банкнота позволит отказаться от некоторых машиночитаемых и человекочитемых признаков, что позволит сосредоточиться не только на качестве и надежности используемых методов, но и удобной визуализации для граждан.

3. Упрощенный процесс ликвидации нелегитимной банкноты.

Считыватель позволяет определить наличие ловушек на банкноте, даже пустых. Существование на купюре большого числа разрушенных квантовых меток позволяет машине подать сигнал на более детальное рассмотрение подобной купюры, в том числе человеком, что позволит более детально рассматривать возможные инциденты, вызванные мошенническими действиями.

4. Не требуется полный отказ от существующих методов подтверждения подлинности.

Выдача купюр с квантовыми метками может осуществляться на базе имеющихся терминалов, что позволяет оставить некоторые существующие признаки подлинности, за счет которых происходит взаимодействие с существующими банкоматами и в повседневном обороте, где не имеется необходимых квантовых считывателей.

В процессе исследования метода обеспечения подлинности купюр на основе квантовой криптографии обнаружен ряд недостатков:

1. Сложность реализации ловушек для фотонов [8].

Кванты склонны к декогерентности. Фотоны считаются наиболее устойчивыми, но ловушка не защищает элемент от воздействий окружающей среды и служит лишь средством крепления к купюре.

2. Неправильная попытка считывания информации из ловушек приводит к их уничтожению и бесполезности в итоге самой купюры.

Невозможно использование купюры, если подразумевается наличие на ней квантовой банкноты, которую не сможет обнаружить считыватель. При возникновении подобной ситуации принимается решение в пользу нелигитимности подобной купюры и потребуется проверка подобного инцидента.

3. Невозможность использования банкнот без специализированных технических устройств.

Например, в домашней обстановке проверка подлинности купюр, при неимении считывателя, будет осуществляться за счет проверки человекочитаемых признаков, без проверки машиночитаемых признаков.

В качестве итогов следует сформулировать, что удалось проанализировать возможность функционирования такой системы оборота банкнот и исследовать необходимые элементы инфраструктуры.

В результате анализа метода обеспечения подлинности купюр на основе квантовой криптографии сделан вывод, что квантовые банкноты могут служить как альтернативным признаком подлинности, так и дополнением существующим.

Для реализации идеи требуется более серьезное техническое оснащение не только на уровне предприятий.

Список используемых источников

1. Центральный банк Российской Федерации [Электронный ресурс] // Центральный банк Российской Федерации: Банкноты и монеты: Показатели наличного денежного обращения. Режим доступа: https://www.cbr.ru/Bank-notes_coins/?PrtId=nal (дата обращения 25.03.2017).

2. Центральный банк Российской Федерации [Электронный ресурс] // Центральный банк Российской Федерации: Банкноты и монеты: Банкноты. Режим доступа: https://www.cbr.ru/Bank-notes_coins/?PrtId=banknotes_itm (дата обращения 25.03.2017).

3. Центральный банк Российской Федерации [Электронный ресурс] // Центральный банк Российской Федерации: Банкноты и монеты: Перечень машиночитаемых защитных признаков банкнот Банка России, подлежащих проверке кредитными организациями. – Режим доступа: https://www.cbr.ru/Bank-notes_coins/?PrtId=machine_readable (дата обращения 25.03.2017).

4. Центральный банк Российской Федерации [Электронный ресурс] // Центральный банк Российской Федерации: Банкноты и монеты: Оборудование для обработки денежной наличности. Режим доступа: https://www.cbr.ru/Bank-notes_coins/?PrtId=banknotes_itm (дата обращения 25.03.2017).

5. The ACM Digital Library is published by the Association for Computing Machinery [Электронный ресурс] // СПС Stephen Wiesner: A special issue on cryptography. Режим доступа: http://archive.li/J4a0q#selection-275.19-275.50 (дата обращения 25.03.2017).

6. Bartkiewicz, K., Černoch, A., Chimczak, G., Lemr, K., Miranowicz, A., Franco, F., Experimental quantum forgery of quantum optical money [Электронный ресурс] // arXiv is an e-print service in the fields of physics, mathematics, computer science, quantitative biology, quantitative finance and statistics: Quantitative Finance: Computational Finance. 2016. Режим доступа: https://arxiv.org/pdf/1604.04453.pdf (дата обращения 25.03.2017).

7. Центральный банк Российской Федерации [Электронный ресурс] // Центральный банк Российской Федерации: Национальная платежная система: Реестр кредитных организаций, признанных Банком России значимыми на рынке платежных услуг. Режим доступа: https://www.cbr.ru/Bank-notes_coins/?PrtId=nal (дата обращения: 25.03.2017).

8. DailyTechInfo [Электронный ресурс] // Новости науки и техники: Ученым удалось заморозить свет, поймав его в ловушку из охлажденных атомов. Режим доступа: http://www.dailytechinfo.org/news/8535-uchenym-udalos-zamorozit-svet-poymav-ego-v-lovushku-iz-ohlazhdennyh-atomov.html (дата обращения: 25.03.2017).

УДК 004.056(075.8)

ОБРАЩЕНИЕ ЧИСЛА В ПРОСТОМ ПОЛЕ

Д. В. Кушнир, С. Н. Шемякин

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

В несимметричных криптографических системах возникает необходимость определения обратных чисел k a в простом поле. Модуль, определяющий простое поле в системах защиты информации, достаточно велик. Это приводит к необходимости рассмотрения алгоритмов, которые позволяют уменьшить вычислительные затраты.

В работе предлагается модификация алгоритма Евклида, не требующая выполнения циклических операций. Алгоритм основан на поведении остатков последовательных чисел кратных k a и превышающих значение модуля до приведения по модулю.

асимметричные криптографические системы, теория чисел, алгоритм Евклида, нахождение обратного числа.

В асимметричных криптографических системах (криптосистемы Эль Гамаля, криптосистемы на эллиптических кривых) при шифровании и расшифровании возникает необходимость определения числа, обратного некоторому заданному числу a в простом поле GF(p) [1, 2].

В существующих асимметричных криптосистемах модуль p может быть больше 2^{1000}. Поэтому представляют интерес алгоритмы обращения чисел, которые позволят уменьшить вычислительные затраты при шифровании-расшифровании.

В настоящее время общепринятым методом решения этой задачи можно считать расширенный алгоритм Евклида [1, 2, 3, 4, 5, 6, 7]. Эквивалентным ему по сущности и вычислительным затратам, но несколько иным по форме является метод, использующий непрерывные (цепные) дроби [3, 4, 5].

Следующая схема обращения [7, 8] работает для любого модуля, возвращая либо правильную обратную величину, либо 0, если её не существует.

Алгоритм Thomas.

1. Начальная установка.
   $z = a \bmod p$;
   $x = 1$;
2. Цикл
   while ($z \neq 1$)
   $q = -\text{flor } (p/z)$;
   $z = p + qz$;
   $x = q*x \bmod p$;
   return x.

Здесь flor (p/z) означает ближайшее целое снизу от результата деления p на z. Алгоритм возвращает $x = a^{-1} \bmod p$. В исходном тексте в тело цикла следует добавить дополнительную команду выхода:

if $z = o$ then $(x = 0)\&(\text{break})$;

Данная схема обращения является модификацией базового алгоритма Евклида. Обратное восхождение в ней отсутствует, поэтому она работает несколько быстрее.

В настоящей статье предлагается ещё одна модификация расширенного алгоритма Евклида, уменьшающую длину циклических операций.

Пусть задано некоторое простое поле GF(p) и некоторое число a, для которого необходимо найти обратное $a^{-1} \bmod p$, $a \leq (p - 1)/2$. Если $a > (p - 1)/2$, то ищем решение для $(p - a)^{-1}$.

Зададим множество $\mathfrak{I}$: $\{y = x*a \bmod p, x = 1, 2, \ldots p - 1\}$. Пример графика множества показан на рис. 1.

Найдём уравнение прямой, проходящей через точки M_1, M_2. Можно показать, что эта прямая пройдёт и через следующую из нижнего ряда множества $\mathfrak{I}$, более того, они будут на равных расстояниях между собой.

$M_1(x_1, y_1)$: $x_1 = 1 + \text{flor } (p/a)$;

$y_1 = a*x_1 \bmod p$.

$M_2(x_2, y_2)$: $x_2 = x_1 + \text{flor } ((p - y_1)/a) + 1$;

$y_2 = a*x_1 \bmod p = y_1 + a(\text{flor } ((p - y_1)/a) + 1) \bmod p$.

Уравнение прямой L_1:

$$L_1: y = (\Delta y/\Delta x)* x + x_1 \Delta y/\Delta x + y_1 \equiv k^* x + b.$$

Здесь $\Delta x = x_2 - x_1$; $\Delta y = y_1 - y_2$.

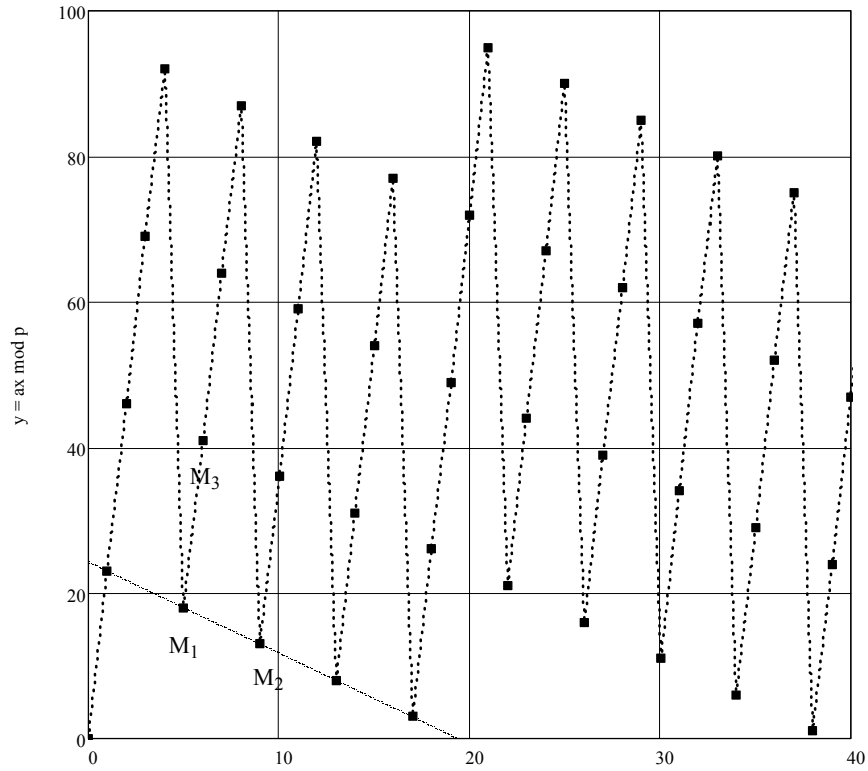


Рис. 1. Множество чисел, кратных числу a. $a = 23$, $p = 97$

Тогда значение целочисленной обратной величины $x = a^{-1} \bmod p$ определяется из уравнения:

$$1 = k*x + b, \;\; a^{-1} \bmod p = x. \tag{1}$$

или

$$-1 = k*x + b, \;\; a^{-1} \bmod p = p - x. \tag{2}$$

Данное уравнение разрешимо в целых числах при

$$y_1 = \pm 1 \bmod \Delta y. \tag{3}$$

Обратный элемент $a^{-1} \bmod p$ отсутствует при

$$y_1 = 0 \bmod \Delta y.$$

При $y_1 = +1 \bmod \Delta y$ используем уравнение (1), а при -1 уравнение (2).

При невыполнении условия (3) следует перейти от точки $M_1(x_1, y_1)$ к одной из точек $M_i(x_i, y_i)$, где условие (3) выполняется:

$$x_i = x_1 + i,$$

$$y_i = y_1 + a*i$$

и найти уравнение прямой L_2 с тем же коэффициентом наклона.

При больших значениях модуля p может возникнуть задача поиска обратного к числу y_1:

$$i* y_1 = \pm 1 \bmod \Delta y. \quad (4)$$

Для малых величин Δy значение числа i легко определяется подбором, в остальных случаях можно воспользоваться любым алгоритмом поиска обратного, в том числе и предлагаемым.

Процедуры поиска точки $M_i(x_i, y_i)$ различны при $\Delta y > 0$ при $\Delta y < 0$.

Пример 1. $\Delta y > 0$

Найти a^{-1} в поле GF(97), $a = 23$.

Точка M_1: $x_1 = 1 + \text{flor}\,(p/a) = 1 + 4 = 5$,

$y_1 = a*x_1 - p = 18$.

Точка M_2: $x_2 = x_1 + \text{flor}\,((p - y_1)/a) + 1 = 9$;

$y_2 = y_1 + a*(\text{flor}\,((p - y_1)/a) + 1) - p = 13$.

$\Delta x = x_2 - x_1 = 4$;

$\Delta y = y_1 - y_2 = 5$.

Проверка разрешимости уравнения:

$y_1 \bmod \Delta y = 18 \bmod 5 = 3$.

Значение $\Delta y > 0$, а также достаточно мало. Условие (3) не выполняется. Переходим к точке x_3, y_3:

$x_3 = x_1 + 1 = 6$;

$y_3 = y_1 + a = 41 = 1 \bmod \Delta y$.

Уравнение прямой L_2 будет:

$L_2 : \Delta y*(x - x_3) + \Delta x*(y - y_3) = 0$.

При y = 1 получаем $x = 38 = a^{-1} \bmod p = 23^{-1} \bmod p$.

Пример 2. $\Delta y < 0$ (рис. 2).

$a = 35$.

Точка M_1: $x_1 = 1 + \text{flor}\,(p/a) = 1 + 2 = 3$,

$y_1 = a*x_1 - p = 8$.

Точка M_2: $x_2 = x_1 + \text{flor}\,((p - y_1)/a) + 1 = 6$;

$y_2 = y_1 + a*(\text{flor}\,((p - y_1)/a) + 1) - p = 16$.

$\Delta x = x_2 - x_1 = 3$;

$\Delta y = y_1 - y_2 = -8 < 0$.

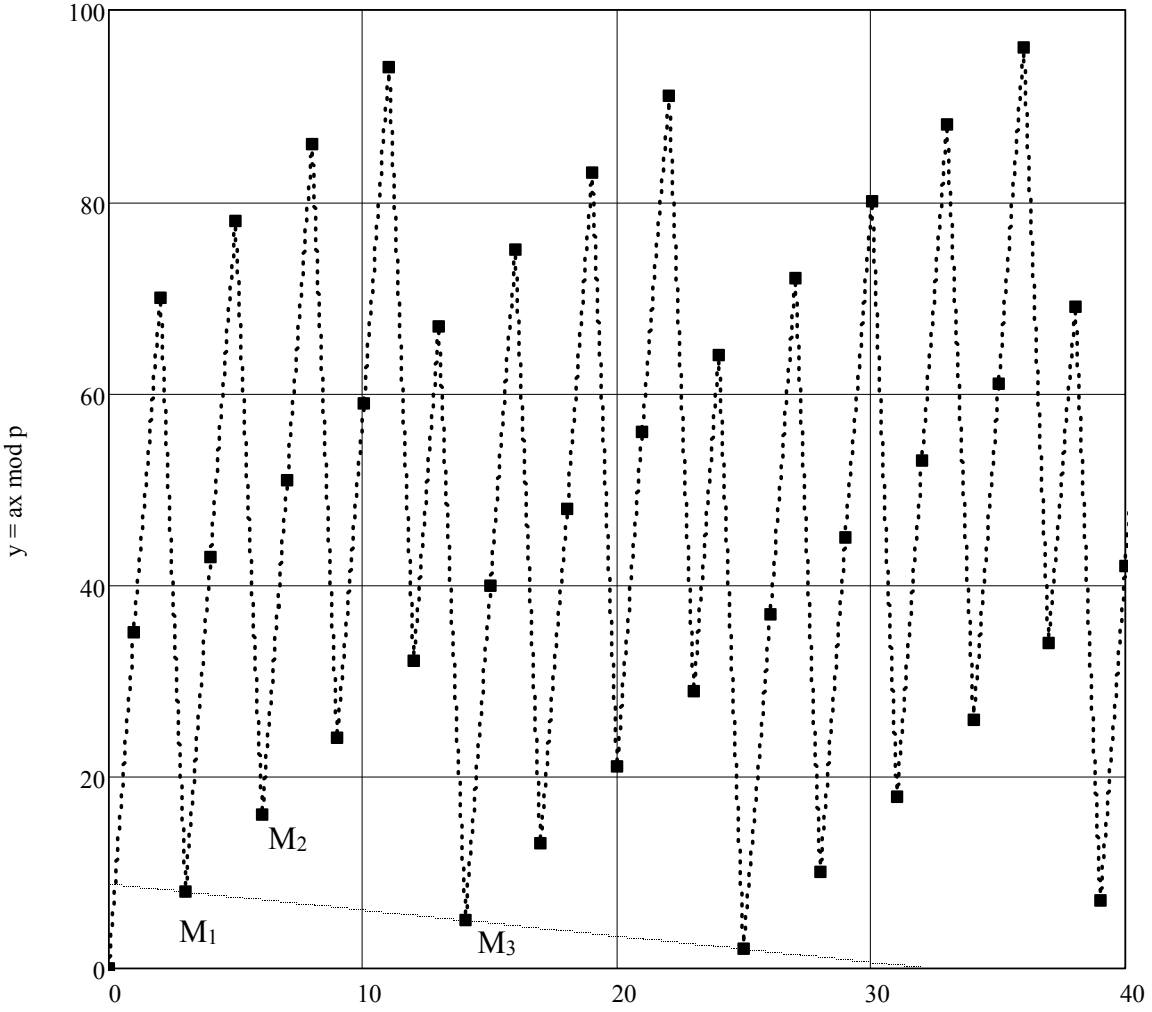


Рис. 2. Множество чисел, кратных числу a. $a = 35$, $p = 97$

Необходимо найти точку M_3, ближайшую снизу к точке M_1 и заново определить Δx, Δy.

Находим i:

$$i = \min \{-\Delta y * i > p - a * \text{flor}\,(p/a)\} = 4.$$

Находим координаты точки M_3

$$x_3 = i * x_1 + \text{flor}\,(p/a) - 1 = 14;$$

$$y_3 = -i * \Delta y + a * \text{flor}\,(p/a) - p = 5.$$

$$\Delta x = x_3 - x_1 = 11;$$

$$\Delta y = y_1 - y_3 = 3.$$

Проверка разрешимости уравнения (4):

$y_1 \bmod \Delta y = 8 \bmod 3 = -1.$

Уравнение прямой будет

$$\Delta x^*(y - y_1) + \Delta y^* (x - x_1) = 0,$$

$$11 (-1 - 8) + 3 (x - 3) = 0.$$

$$x = 36.$$

Ответ будет

$$a^{-1} \bmod p = p - x = 97 - 36 = 61.$$

Список используемых источников

1. Коржик В. И., Просихин В. П., Яковлев В. А. Основы криптографии: учебное пособие, СПб ГУТ. СПб., 2014. 275 с.

2. Рябко Б. Я., Фионов А. Н. Криптографические методы защиты информации. М. : Горячая линия – Телеком, 2005. 226 с.

3. Бухштаб А. А. Теория чисел. М. : Просвещение, 1966. 383 с.

4. Виноградов И. М. Основы теории чисел. М. : Наука, 1965. 172 с.

5. Дирихле П. Г. Л. Лекции по теории чисел. В обработке и с добавлениями Р. Дедекинда; пер. с нем. / Под ред. Б. И. Сегала. Изд. 5-е. М. : Книжный дом «ЛИБРОКОМ», URSS, 2016. 368 с.

6. Айерленд К. А., Роузен М. Классическое введение в современную теорию чисел. М. : Мир, 1987. 415 с.

7. Крэндалл Р., Померанс К. Простые числа. Криптографические и вычислительные аспекты. М. : Книжный дом «ЛИБРОКОМ», URSS, 2011. 663 с.

8. Thomas J., Keller J., Larsen G. The calculation of multiplicative inverses over GF(p) efficiently where P is f Mersenne prime // IEEE Trans. Comp., C-35: 478–482, 1986.

УДК 004.056

АНАЛИЗ МЕХАНИЗМОВ ОБЕСПЕЧЕНИЯ ЗАЩИЩЕННОГО ДОСТУПА К ДАННЫМ, РАЗМЕЩЕННЫМ В ОБЛАКЕ

М. В. Левин, Е. С. Фостач

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

С развитием облачных технологий возрастает роль распределенной инфраструктуры, функциональная совместимость и портативность которой являются неотъемлемой составляющей. Однако, обеспечение доступности услуг и масштабируемости виртуальных ресурсов, безопасности и конфиденциальности пользовательских данных

имеет первостепенное значение. Данная работа содержит актуальные для поставщиков облачных услуг решения, которые позволят поддержать доступность, конфиденциальность и целостность личных данных в облачной среде.

защита персональных данных, облачная архитектура, безопасность облачных вычислений, конфиденциальность информации, механизмы аутентификации, угрозы информационной безопасности.

Облачные вычисления представляют собой технологию распределенной обработки данных, где ресурсы и мощности предоставляются пользователю в качестве услуг. Технология облачных вычислений является результатом конвергенции более ранних технологий, таких как параллельные вычисления и распределенные вычисления.

Провайдеры облачных вычислений предлагают свои услуги на базе трех основных моделей сервисов:

- инфраструктура как услуга (IaaS);
- платформа как сервис (PaaS);
- программное обеспечение как услуга (SaaS) [1].

Несмотря на то, что виртуализация сетевых функций и облачные вычисления дают возможность дистанционно разграничить ИТ-инфраструктуру и пользователей, необходимо решить возросшие вместе с этим риски эксплуатации уязвимостей информационной безопасности для того, чтобы в полной мере воспользоваться новыми возможностями вычислительной парадигмы.

Особое значение приобретает данная проблема для поставщиков SaaS услуг [1]. Пользователь, который доверил свои данные для хранения в облаке, теряет контроль над их целостностью, конфиденциальностью и доступностью. Одной из важных задач поставщика услуг является обеспечение трех базовых свойств информационной безопасности, включая задачи организации места хранения и способа представления пользовательских данных.

Таким образом, для поддержания трех базовых свойств информационной безопасности – конфиденциальности, целостности и доступности данных пользователей, обозначим 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.

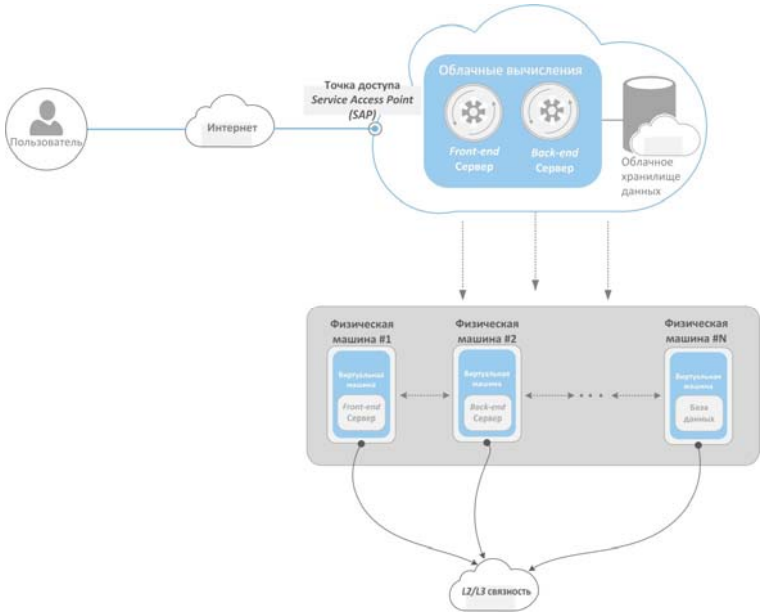


Рис. 1. Функциональная архитектура облачных сред

За основу была взята схема функциональной архитектуры облачной среды, приведенная на рис. 1, на базе которой построено данное исследование. На схеме показан способ развертывания баз данных и приложений на ресурсах облачной инфраструктуры вместе с сетевой схемой взаимодействия. Наглядно показаны уровни коммутации (L2) и маршрутизации (L3) данных между объектами облачной инфраструктуры.

В соответствии с решаемой проблемой, обозначим ключевые аспекты информационной безопасности, которые должны лежать в основе каждого надежного облачного сервиса:

1. Определение способов **конфиденциальной** передачи данных.
2. Организация доступа **авторизованных** пользователей к данным.

Определение способов конфиденциальной передачи данных

Для решения первой задачи необходимо использовать криптографические механизмы, позволяющие обеспечить надежное шифрование данных. Важно отметить, что 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).

Рассмотрим протокол защищенной передачи данных TLS v1.2, в котором реализованы алгоритмы шифрования информации, аутентификации пользователей и контроля целостности получаемых данных [2].

Работа TLS протокола начинается с согласования версии используемого протокола, способа шифрования данных между узлами соединения,

а также проверки достоверности полученных сертификатов, после чего будет установлен криптографически безопасный канал. Отметим, что шифрование с открытым ключом должно использоваться только в процедуре во время первоначальной настройки соединения (TLS *Handshake*), которая позволяет установить общий секретный ключ шифрования без предварительных знаний узлов соединения друг о друге. После настройки TLS-туннеля должна использоваться симметричная криптография, общение в пределах текущей сессии будет зашифровано именно установленными симметричными ключами. Это необходимо для увеличения быстродействия, так как криптография с открытым ключом требует значительно больше вычислительной мощности.

После того, как мы определили протокол, который обеспечит соединение на участке между клиентом и облаком, необходимо перейти к вопросу аутентификации.

Отметим одну из ключевых особенностей протокола TLS v1.2, которая заключается в возможности установления подлинности личности, клиента и сервера (*Chain of Trust*) за счет использования сертификатов подлинности, предоставляемыми центрами сертификации (CA – *certificate authorities*). Центры сертификации выдают подписанные сертификаты, доверие к которому неоспоримо. Таким образом, целый ряд выданных сертификатов образует цепочку доверия. Благодаря этому можно проверить подлинность каждого доверительного узла.

Передача каждого сообщения осуществляется с добавлением MAC-значения (*Message Authentication Code*), который представляет собой одностороннюю криптографическую функцию хэширования, ключи которой известны обоим участникам соединения. При отправке сообщения каждый раз генерируется его MAC-значение, по которому принимающая сторона может проверить полученную информацию на предмет подмены.

Таким образом, показано, что использование протокола TLS v1.2 позволяет создать канал конфиденциальной передачи данных. Однако, отметим, что механизмы работы данного протокола не обеспечивают контроль времени жизни каждой пользовательской сессии и повторную аутентификацию клиента для возобновления сессии в случае разрыва установленного соединения. Так же отметим, что 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 полу-

чать мгновенный доступ к электронным услугам, 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].

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. 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 [4].

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. 2), 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.

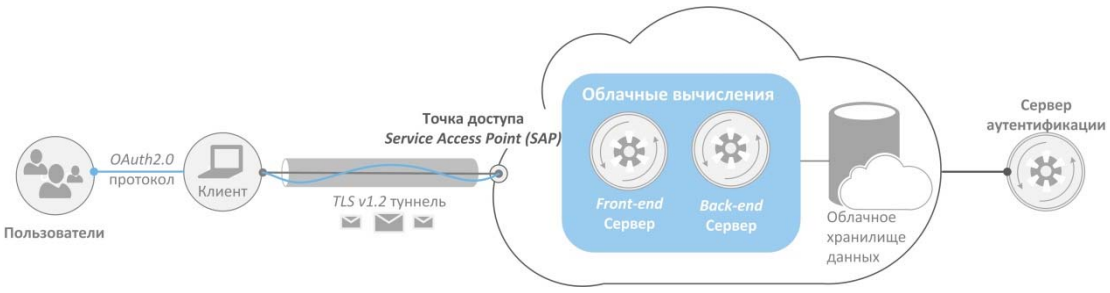


Рис. 2. Концептуальная схема построения защищенной облачной среды

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. URL: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf (дата обращения 30.12.2016).

2. T. Dierks, E. Rescorla. The Transport Layer Security (TLS) Protocol, Version 1.2 (RFC5246). URL: https://tools.ietf.org/html/rfc5246 (дата обращения 05.01.2017).

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. 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, pp. 529–541.

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

УДК 004.057.4, 004.056.5

ВВЕДЕНИЕ В ПРОТОКОЛ 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. Данную статью можно рассматривать, как краткое введение в протокол с целью ознакомления о новых командах необходимых для интегрирования криптографических функций непосредственно в базовый протокол SCTP.

SCTP, S-SCTP, Secure SCTP, информационная безопасность

Для защиты данных, передаваемых с использованием протокола SCTP [1], можно использовать несколько решений, в зависимости от требуемого уровня реализации в модели OSI, а именно: «SCTP поверх IPSec» [2], «TLS поверх SCTP» [3] и находящееся в стадии разработки решение Secure SCTP (далее S-SCTP) [4]. Проведенное сравнение этих решений [5] показало, что предлагаемая разработчиками интеграция криптографических функций непосредственно в протокол SCTP позволяет полностью избежать недостатков не интегрированных решений при этом обеспечивая совместимость с базовым протоколом SCTP для некоторых уровней безопасности.

В связи с тем, что протокол SCTP обладает поддержкой многопоточности (англ. *multistreaming*) и множественной адресации (англ. *multihoming*) [6] основные проблемы при использовании SCTP в сочетании с TLS и IPSec только масштабируются с увеличением числа потоков или добавления новых IP-адресов в ассоциацию. Это вызвано тем, что для N безопасных потоков необходимо создать N TLS соединений и, следовательно, выполнить N процедур их установки: так называемых «рукопожатий». Если число N мало, то проблема не является критичной, но при его увеличении (напомним, что протокол SCTP поддерживает до 65535 входящих и исходящих потоков в рамках одной ассоциации) ситуация усугубляется, так как установка соединения – это медленный процесс, увеличивающий затраты на передачу данных. Таким образом, когда приложение выполняет N соединений нагрузка (с точки зрения использования памяти, ЦПУ и т. п.) линейно увеличивается с течением времени. Проблему можно преодолеть, используя IPSec, но это лишает нас возможности добавить в ассоциацию новый IP-адрес в случае динамической реконфигурации ассоциации [7]. Для новых IP адресов, добавляемых в ассоциацию, необходимо будет устанавливать новые безопасные ассоциации (англ. *Security Associations*) [2].

На текущий момент протокол находится в стадии разработки, которая началась в 2005 г. Базовый документ [4], содержащий техническое описание протокола, имеет статус Интернет-черновика (англ. *Internet Draft*) и пережил уже 23 редакции. Сделать вывод, что разработка протокола находится в завершающей стадии, позволяет тот факт, что на сегодняшний день существует уже несколько его практических реализаций.

Принцип работы заключается в следующем: безопасный сеанс[1] инициализируется уже после того как была создана обычная SCTP-ассоциация [1, 5]. Если это невозможно, например, в связи с тем, что приложение одной из конечных точек не поддерживает S-SCTP или установка безопасного сеанса не удается – приложение может решить, использовать незащищенную ассоциацию для передачи данных или же прервать ее. Одна S-SCTP

[1] Безопасный сеанс (англ. Secure session) – это сеанс, который обеспечивает функции безопасности для установленной SCTP ассоциации.

ассоциация может иметь только один безопасный сеанс для всех потоков данных в случае с многопоточностью и для всех адресов в сценарии с множественной адресацией. Для того чтобы это обеспечить, механизм безопасности встраивается в структурную схему SCTP и взаимодействует с функциональным блоком SCTP, который выполняет группировку/разгруппировку команд[2]/пакетов SCTP и функциональным блоком, который осуществляет управление SCTP пакетами (рис.).

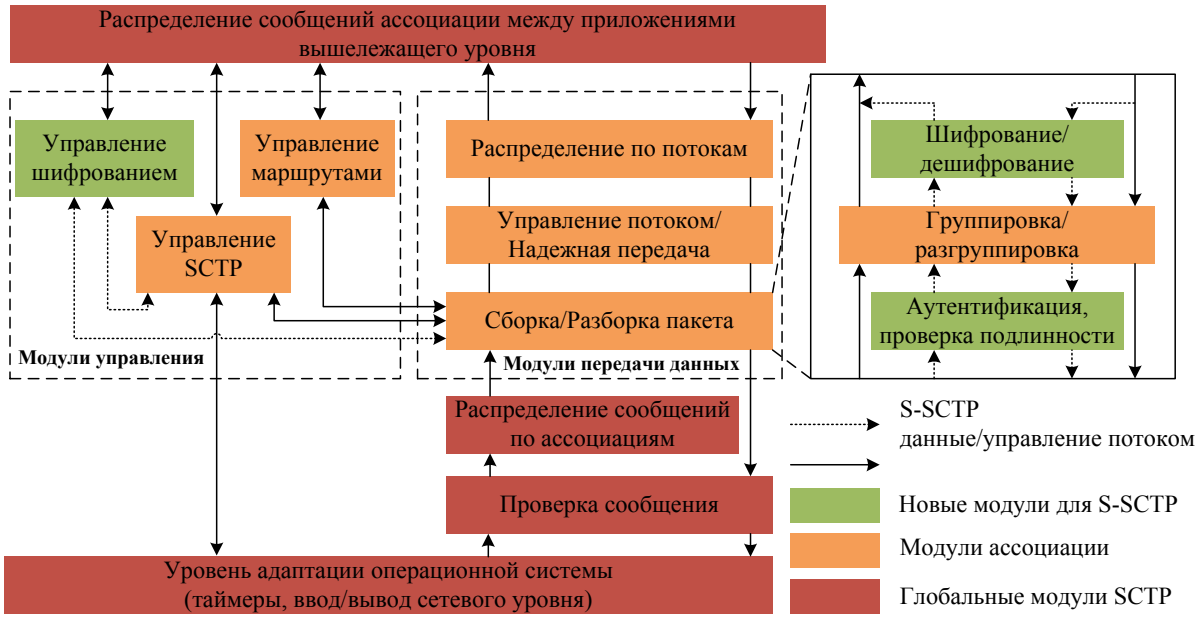


Рисунок. Структурная схема модулей SCTP

S-SCTP позволяет передавать как зашифрованные, так и не зашифрованные данные в рамках одного безопасного сеанса, при этом, в отличие от решения «TLS поверх SCTP», такие данные могут передаваться и в одном потоке. Для уменьшения служебной информации команды, отмеченные для шифрования, группируются и зашифровываются в один блок шифрованных данных «EncData», которые, в свою очередь, могут группироваться вместе с незашифрованными командами «DATA» в один SCTP-пакет. По той же причине криптографическая хеш-функция HMAC вычисляется на весь пакет целиком, а не на каждую зашифрованную команду.

Поддерживаемые уровни безопасности

S-SCTP предлагает несколько уровней безопасности. Приложения, использующие S-SCTP, могут его изменить в течение срока службы сеанса связи в любой момент. Всего поддерживается четыре уровня безопасности (англ. security level):

[2] Отечественная нормативно-правовая база устанавливает использование термина «команда», однако, в технической литературе часто вместо этого термина можно встретить термин «фрагмент».

уровень «*0*». S-SCTP не использует ни зашифрованные данные, ни аутентификацию. Пакет S-SCTP имеет такой же формат, что и пакет SCTP, поэтому этот уровень полностью совместим с базовым протоколом SCTP;

уровень «*1*». требуется аутентификация пакетов, но не используется шифрование. Каждый исходящий пакет (включая общий заголовок пакета SCTP) проходит проверку подлинности – это означает, что в формат пакета включается команда (англ. *chunk*) «Authentication, AUTH» [8];

уровень «*2*». команды «DATA», передающие данные пользователя, могут быть зашифрованы. Пакет S-SCTP, если он содержит такие данные, должен обязательно проходить проверку подлинности. Если же пакет включает в себя только незашифрованные данные пользователя и/или управляющие команды, то проверка подлинности не требуется.

уровень «*3*». Это самый высокий уровень безопасности. Каждый исходящий пакет S-SCTP зашифровывается и проходит проверку подлинности.

Еще одной особенностью S-SCTP является одновременная поддержка конечными точками разных уровней безопасности в рамках одной ассоциации. Например, для повышения производительности работы ассоциации функции безопасности могут использоваться только для одного направления: от сервера к клиенту (уровни безопасности 3 и 0 соответственно).

Изменения протокола SCTP

Для поддержки криптографических функций в базовый протокол вводятся новые команды[3], которые могут быть объединены с другими командами в единый пакет. Так как протокол S-SCTP является протоколом, ориентированным на соединение, то его работу можно условно разбить на несколько фаз: «установления безопасного сеанса связи», «передача данных» и «разрушение безопасного сеанса связи». Также для каждой команды вводится набор обязательных и необязательных параметров, но, к сожалению, объем статьи не позволяет их привести, поэтому читатель может ознакомиться с ними самостоятельно [4].

Secure Session Open request. Передается конечной точкой с целью установления безопасного сеанса связи, также может быть использована для обновления секретного мастер-ключа[4] или набора шифров после установления безопасного сеанса. Для подтверждения приема используется «Secure Session Open Acknowledge».

Secure Session Certificate. Является необязательной командой и может быть отправлена обоими конечными точками. Содержит сертификат, который позволяет аутентифицировать конечную точку, устанавливающую безопасный сеанс.

[3] Формат перечисленных в статье команд приведен в п. 5.1 [4].

[4] Секретный мастер-ключ (англ. Master secret key) – S-SCTP использует два вида секретных ключей: для аутентификации пакетов S-SCTP и для шифрования/дешифрования данных.

ТАБЛИЦА. Новые команды для поддержки Secure SCTP

Код команды		Фаза работы	Название команды	
0xD0	208	Установление безопасного сеанса связи	SSOpReq	Secure Session Open Request Chunk
0xD1	209		SSCert	Secure Session Certificate Chunk
0xD2	210		SSOpReq_Ack	Secure Session Acknowledge Chunk
0xD3	211		SSSerKey	Secure Session Server Key Chunk
0xD4	212		SSCliKey	Secure Session Client Key Chunk
0xD5	213		SSOpCom	Secure Session Open Complete Chunk
0xD6	214	Разрушение безопасного сеанса связи	SSClose	Secure Session Close Chunk
0xD7	215		SSClose_Ack	Secure Session Close Acknowledge Chunk
0xD8	216	Передача данных	SecLevCHD	Security Level Change Chunk
0xD9	217		SecLevCHD_Ack	Security Level Change Acknowledge Chunk
0x10	16		EncData	Encrypted Data Chunk
0x11	17		AUTH	Authentication Chunk
0x12	18		PADDING	Padding Chunk

Secure Session Server Key и *Secure Session Client Key.* Команды включают параметр, который используется во время алгоритма обмена ключами.

Secure Session Open Complete. Указывает на завершение установления безопасного сеанса. После приема этой команды конечная точка верифицирует данные проверки, которые содержатся в команде. В случае неуспешной проверки в установлении безопасного сеанса будет отказано.

Secure Session Close. Запрос на разрушение текущего безопасного сеанса. При приеме конечной точкой данной команды отправка зашифрованных данных немедленно останавливается. Для подтверждения приема используется команда «*Secure Session Close Acknowledge*».

Security Level Changed. С помощью данной команды встречная конечная точка извещается об установлении нового уровня безопасности. Для подтверждения её приема используется команда *Security Level Changed Acknowledged.*

Encrypted Data. Команда передает зашифрованные данные и может содержать одну или нескольких команд «DATA». Каждый S-SCTP пакет может включать в свой формат несколько команд «EncData», которые, в свою очередь, могут группироваться вместе с незашифрованными командами «DATA».

Padding. Используется вместе с «EncData», если в этом есть необходимость. 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 к нему добавляется «Padding».

Authentication. Предназначается для аутентификации пакета S-SCTP, если этого требует выбранный уровень безопасности.

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], в которой передается параметр «Причина ошибки, Error Causes» с соответствующим кодом ошибки (см. п. 6. [4]).

Список используемых источников

1. Stewart R. RFC4960 Stream Control Transmission Protocol. September 2007. URL: https://tools.ietf.org/html/rfc4960 (дата обращения 04.03.2017).

2. 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 04.03.2017).

3. 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).

4. Hohendorf C., Unurkhaan E., Dreibholz T. Secure SCTP draft-hohendorf-secure-sctp-23.txt. 2017. URL: https://tools.ietf.org/html/draft-hohendorf-secure-sctp-23 (дата обращения 04.03.2017).

5. 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.; Т. 1 / под. ред. С. В. Бачевского. СПб. : СПбГУТ, 2016. 451–456 с.

6. Лейкин А. Протоколы транспортного уровня UDP, TCP, SCTP: достоинства и недостатки // Проводные сети, Первая миля. 2013. №5. С. 62–69.

7. R. Stewart, Q. Xie, M. Tuexen, S. Maruyama, M. Kozuka. RFC 5061 Stream Control Transmission Protocol (SCTP) Dynamic Address Reconfiguration. September 2007. URL: https://tools.ietf.org/html/rfc5061 (дата обращения 04.03.2017).

8. M. Tuexen, R. Stewart, P. Lei, E. Rescorla. RFC 4895 Authenticated Chunks for the Stream Control Transmission Protocol (SCTP). August 2007. URL: https://tools.ietf.org/html/rfc4895 (дата обращения 10.03.2017).

Статья представлена заведующим кафедрой, доктором технических наук, профессором Б. С. Гольдштейном.

УДК 004.4:004.7

ОСНОВНЫЕ ВИДЫ УГРОЗ ПРИ КОМПРОМЕТАЦИИ КОММУТАТОРА В SDN

Н. О. Лоханько, Р. С. Подоляк, И. А. Ушаков

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

Software-defined Networking – новый подход к построению архитектуры компьютерных сетей. Уровень управления сетью и уровень передачи данных разделяются, а функции управления сетью переносятся с маршрутизаторов и коммутаторов на программные приложения, запущенные на отдельном сервере – контроллере. В статье приведен обзор наиболее распространенных атак на канал управления сети SDN, цели, которых хотят достигнуть злоумышленники и способы предотвращения этих угроз.

SDN, dataplane, controlplane, контроллер, ПКС.

Общего понятия у программно-конфигурируемых сетей пока что нет, и рабочие группы, состоящие из крупных IT-корпораций, предлагают свои варианты, вот, например, одно из них.

ONF: 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, 2.

В традиционной сети интернет идет разделение на уровень управления (*controlplane*) и уровень передачи данных (*dataplane*). Каждый уровень выполняет свои задачи, например, уровень управления, отвечает за процесс маршрутизации, TrafficEngineering. Уровень передачи данных отвечает за пересылку пакетов с одного интерфейса на другой (рис. 1) [3].

Концепция программно-конфигурируемых сетей предлагает избавить оборудование от уровня управления и переложить его задачи на контроллер. При этом будет разделена модель традиционно-распределенной маршрутизации на централизованную.

В итоге получается программируемая сеть. Если раньше каждое сетевое устройство принимало решение основываясь на своей информации, то теперь есть контроллер, который видит сеть в целом, и исходя из топологии принимает решение и отправляет задачи коммутаторам. В самом контроллере работают управляющие программы (API), которые реализуют сетевые услуги, например, балансировку нагрузки, маршрутизацию, сетевые экраны (*Firewall*), шифрование, технологию NAT и прочее (рис. 2) [3, 4].

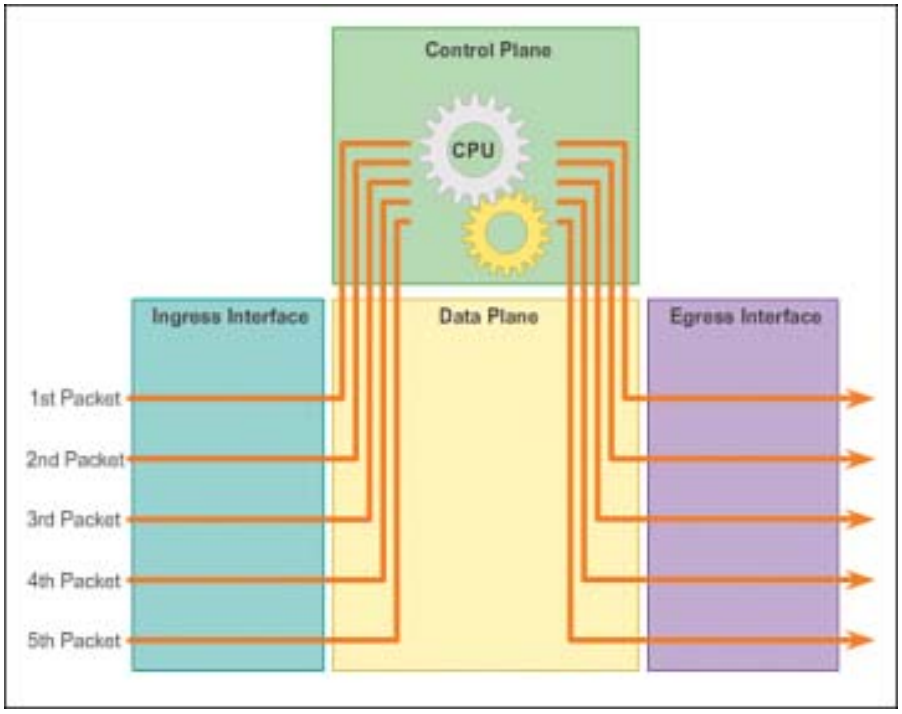


Рис. 1. Процессорная обработка трафика

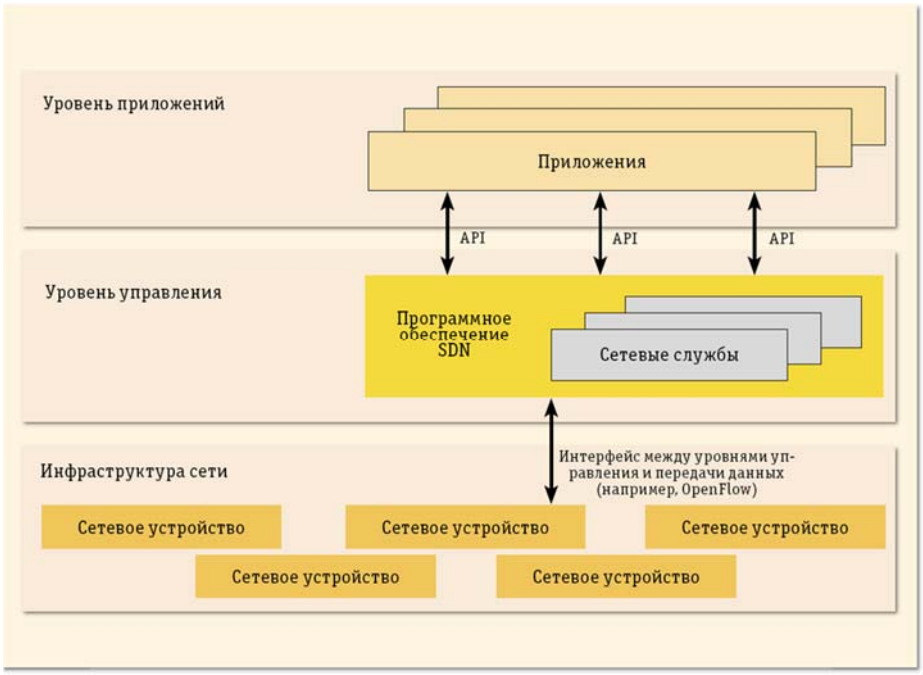


Рис. 2. Структура работы ПКС

С возрастанием потребности в технологии, возрастает и внимание злоумышленников к ней. Централизованный контроллер сети требует повышенного внимания со стороны администратора для обеспечения безопасности и корректного функционирования всей сети, ниже представлен список основных атак, которым подвержены SDN:

– Искажение данных.
– Раскрытие информации ос состоянии и статусе сети.
– Отказ в обслуживании.
– Компрометация коммутатора.
– Атака на канал управления [5, 6, 7].

Рассмотрим основные атаки на канал управления, которые возможны при компрометации коммутатора.

Перехват управляющего трафика

Атакующий может использовать скомпрометированный коммутатор для перехвата управляющего трафика, идущего через данный коммутатор в том случае, если не используется TLS [5]. Более того, атакующий может перехватить управляющий трафик, посылаемый скомпрометированному коммутатору, если перед этим был произведен перехват управляющего канала. TLS защита не сможет противостоять данной атаке в случае, если атакующий способен извлекать криптографические ключи из скомпрометированного коммутатора. Основным методом защиты от подобных атак является использование out-of-band передачи управляющего трафика. Скомпрометированный коммутатор может быть использован для атак на целостность сети. Атакующий может производить подделку видимого для контроллера состояния коммутатора. Такая атака называется – подделка состояния коммутатора. Если в сети не используется протокол TLS или он используется только для аутентификации контроллера, атакующий может создавать поддельные виртуальные коммутаторы в данной сети. Подобная атака называется – подделка состояния сети.

Подделка состояния коммутатора и сети

Скомпрометированный коммутатор используется атакующим для того, чтобы передавать контроллеру ложные сведения о текущем состоянии данного коммутатора или других коммутаторов, которые подключены к контроллеру через скомпрометированный коммутатор. Например, атакующий может передать контроллеру ложную информацию о содержимом таблиц потоков, о статистике по трафику или даже о том, какие интерфейсы имеет коммутатор. Атакующий может использовать подобные атаки для сокрытия своих действий от контроллера. Кроме того, атакующий может подделывать состояние других коммутаторов в случае, если в сети не используется TLS. Данная угроза показывает важность использования аутентификации в SDN сети. Стоит отметить, что даже если TLS используется только для аутентификации контроллеров, атакующий будет не способен произвести MitM атаку на управляющий трафик [5], проходящий через скомпрометированный коммутатор. Однако, если TLS не используется для аутентификации

коммутаторов, то атакующий сможет создавать поддельные коммутаторы в сети. Данная атака может быть использована для изменения сетевой топологии, которая хранится у контроллера. Создавая поддельные коммутаторы, атакующий может влиять на процесс выбора маршрута для потоков в сети.

Компрометации контроллера

Приложения, работающие на контроллере, могут содержать в себе уязвимости, эксплуатация которых приведет к компрометации контроллера атакующим. Также приложения могут уже содержать в себе вредоносный код, если они были загружены от непроверенных производителей. Большинство современных контроллеров не предоставляют разграничение доступа для приложений на контроллере, что приводит к тому, что каждое приложение может иметь доступ не только к внутренним данным других приложений, но и к внутренним структурам контроллера (например, к внутреннему представлению сети). Также многие контроллеры не производят контроль ресурсов, запрашиваемых приложениями. Это происходит из-за того, что в контроллерах, для повышения производительности, приложения реализуются в виде библиотек, которые загружаются в адресное пространство контроллера. Типичной атакой, базирующейся на данных свойствах контроллеров, может быть то, что вредоносное приложение может изменить структуру, содержащую внутреннее представление сети, что приведет к неправильной работе всех приложений на контроллере.

Безопасность играет ключевую роль в дальнейшей миграции сетевых сервисов в «облака» и для дальнейшего развития SDN. Список областей, где пока не стоит использовать SDN, достаточно велик, однако со временем технология будет усовершенствована и для нее будут разработаны надежные системы управления. Преимуществом технологии SDN и ее слабым местом является централизованное управление сетью и маршрутизацией в ней. Обманув контроллер или получив над ним контроль можно в той или иной мере нарушить работу всей сети.

Список используемых источников

1. 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, 2008, vol. 38, no. 2. PP. 69–74.

2. Моделирование и реализация средств виртуализации сетевых функций NFV: отчет о НИР / А. А. Швидкий. СПб. : СПбГУТ, 2015. 50 с.

3. Diane Teare, Bob Vachon, Rick Graziani. Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide, 2015.

4. Левин М. В., Ушаков И. А., Цветков А. Ю., Исаченков П. А. Основы построения компьютерных сетей. СПб. : СПбГУТ, 2016. 56 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. 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.

7. 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.

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

УДК 519.633.2

О ПРИМЕНЕНИИ НЕЛОКАЛЬНЫХ ГРАНИЧНЫХ УСЛОВИЙ В ЗАДАЧЕ РАСПРОСТРАНЕНИЯ РАДИОВОЛН ВБЛИЗИ ПОВЕРХНОСТИ ЗЕМЛИ

М. С. Лытаев

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

В настоящей работе исследуется метод прозрачных нелокальных граничных условий для решения задачи численного моделирования распространения ультракоротких радиоволн вблизи поверхности Земли в параксиальном приближении. Представлена модификация указанного подхода для широкоугольного параболического уравнения. Предложенный метод позволяет обходиться без искусственного вводимого понятия поглощающего слоя при построении численного решения. Выполнено сравнение с методом расщепления Фурье.

распространение радиоволн, неоднородная тропосфера, параболическое уравнение, нелокальное граничное условие.

Эффективность систем телекоммуникаций и обнаружения, основанных на передаче радиосигналов, существенно зависит от текущей метеорологической обстановки и рельефа местности [1]. Хорошо известно, что пространственные изменения индекса преломления и ландшафт земной поверхности способны оказывать существенное влияние на распространение электромагнитных волн. Все бóльшую популярность набирают системы оперативного прогнозирования характеристик распространения радиоволн

в неоднородной тропосфере, например, AREPS и TEMPER [2]. Такие системы способны собирать и обрабатывать метеорологическую информацию из различных источников в реальном времени и обеспечивают наглядное представление полученных результатов.

Важным компонентом такой системы является модуль расчета электромагнитного поля в неоднородной среде. Наибольшую популярность для решения данного класса задач приобрел метод параболического уравнения и основанный на нем алгоритм расщепления Фурье.

Анализ вышеупомянутых систем и лежащих в их основе численных алгоритмов показывает, что они обладают серьезными недостатками. Особенности построения численного решения указанной задачи в полубесконечном интервале высот исследованы недостаточно, что приводит к появлению ложных отражений от верхней границы расчетной области. Введение искусственного поглощающего слоя позволяет уменьшить влияние ложных отражений, однако параметры такого слоя определяются исходя из некоторых эмпирических соображений, что делает затруднительным оценку эффективности алгоритма в зависимости от конкретных условий. Альтернативным подходом является введение нелокальных граничных условий, которые позволяют свести исходную задачу к эквивалентной с ограниченной по высоте областью интегрирования. Следует отметить, что метод нелокальных граничных условий широко используется в аналогических задачах в гидроакустике и квантовой механике [3]. Дополнительную сложность в задаче тропосферного распространения создаёт тот факт, что эффективный индекс преломления выше области интегрирования представляет собой линейно растущую функцию.

Задача распространения электромагнитных волн заключается в нахождении комплексного поля в переменных Пекериса [4]. Функция $V(x,z)$ удовлетворяет уравнению Гельмгольца:

$$\frac{\partial^2 V}{\partial x^2}+\frac{\partial^2 V}{\partial z^2}+k^2(1+m(x,z))V=0, \qquad (1)$$

где $k=2\pi/\mu$ – волновое число в вакууме, μ – длина волны, $m(x,z)=N(x,z)+2z/R$, $N(x,z)$ – индекс преломления среды, R – радиус Земли. Далее предполагается, что $N(x,z)=0$ при $z>z_b$. Функция $V(x,z)$ также удовлетворяет импедансному условию на нижней границе и начальному условию Коши, отвечающему заданной диаграмме направленности антенны [4].

После совершения замены $U(x,z)=e^{-ikx}V(x,z)$, отвечающей параксиальному приближению, формальное решение уравнения (1) для волн, уходящих на бесконечность в положительном направлении по оси x, запишется в операторной форме следующим образом [4]:

$$U(x+\Delta x,z)=e^{ik\Delta x\left(\sqrt{1+L}-1\right)}U(x,z),$$

$$L = \frac{1}{k^2}\frac{\partial^2}{\partial z^2} + m(x,z).$$

Раскладывая операторную экспоненту при помощи аппроксимации Паде-(1,1) [4]:

$$e^{ik\Delta x(\sqrt{L+1}-1)} \approx \frac{4i + (i - k\Delta x)L}{4i + (i + k\Delta x)L}$$

и заменяя оператор L конечно-разностным аналогом $L_h u_j^n = (h^2k^2)^{-1}\Delta^2 u_j^n + m(n\Delta x, jh)$ с учетом граничного условия, получаем численную схему Кранка-Николсон:

$$\left(4i + (i + k\Delta x)L_h\right)u_j^{n+1} = \left(4i + (i - k\Delta x)L_h\right)u_j^n, \qquad (2)$$

где $u_j^m = U(m\Delta x, jh)$, h – шаг сетки по переменной z.

Применяя z-преобразование по переменной n, уравнение (2) при $j \ge B = \lceil z_b / h \rceil$ запишется следующим образом:

$$\left(4i + (i + k\Delta x)(\frac{1}{h^2k^2}\Delta^2 + \frac{2j}{R})\right)\xi\hat{u}_j(\xi) = \left(4i + (i - k\Delta x)(\frac{1}{h^2k^2}\Delta^2 + \frac{2j}{R})\right)\hat{u}_j(\xi), \qquad (3)$$

где

$$\hat{u}_j(\xi) = \sum_{n=0}^{\infty} u_j^n \xi^{-n}.$$

Следуя работе [5], решение уравнения (3) может быть записано в явном виде:

$$\hat{u}_j(\xi) = J_{j+(2+d(\xi))/c}(2/c),$$

$$c = -\frac{2k^2h^3}{R},$$

$$d(\xi) = \frac{2k^2((Bh^3 + 2R\Delta x^2)(1-\xi) + ikB\Delta x h^3(1+\xi))}{R(1 - \xi + ik\Delta x(1+\xi))},$$

J – функция Бесселя первого рода.

Совершая обратное z-преобразование можно получить дискретное нелокальное граничное условие:

$$u_{B-1}^n - s_B^0 u_B^n = \sum_{m=1}^{n-1} u_B^{n-m} s_B^m,$$

где коэффициенты свертки s_B^n определяются следующим образом

$$s_B^n = \frac{\tau^n}{2\pi}\int_0^{2\pi} \frac{\hat{u}_{B+1}(\xi)}{\hat{u}_B(\xi)}\exp(iny)dy.$$

Описанные в [5] способы вычисления коэффициентов свертки в некоторых случаях приводят к неустойчивым результатам. Для эффективного вычисления обратного z-преобразования был разработан адаптивный численный алгоритм, основанный на аппроксимации подынтегральной функции полиномами Чебышева произвольного порядка [6]. Для вычисления отношения функций Бесселя под интегралом используется алгоритм Ленца [5]. Следует отметить, что коэффициенты свертки не зависят от постоянно изменяющихся параметров среды и могут быть вычислены заранее для использования в системах прогнозирования реального времени, где требуется высокая скорость расчетов.

Сравнение описанного метода будет проводиться с программой PETOOL [2], осуществляющей решение задачи методом расщепления Фурье. Будем использовать следующие расчетные параметры: Δx=10 м, Δ z = 0,03 м, высота расчетной области z_b=300 м, высота поглощающего слоя метода расщепления Фурье составляла 300 м. Сначала рассмотрим случай однородной тропосферы при $N(x,z)=0$. Как можно видеть из рис. 1, оба метода демонстрируют почти идеальное совпадение на расстояниях до 60 км, однако далее метод расщепления Фурье приводит к результатам, не соответствующим общепринятым представлениям о дифракции вокруг поверхности Земли. Следует отметить, что путем увеличения высоты расчетной области или выбором подходящей весовой функции для поглощающего слоя всегда удается добиться совпадения с предложенным методом, однако это приводит к увеличению вычислительных затрат.

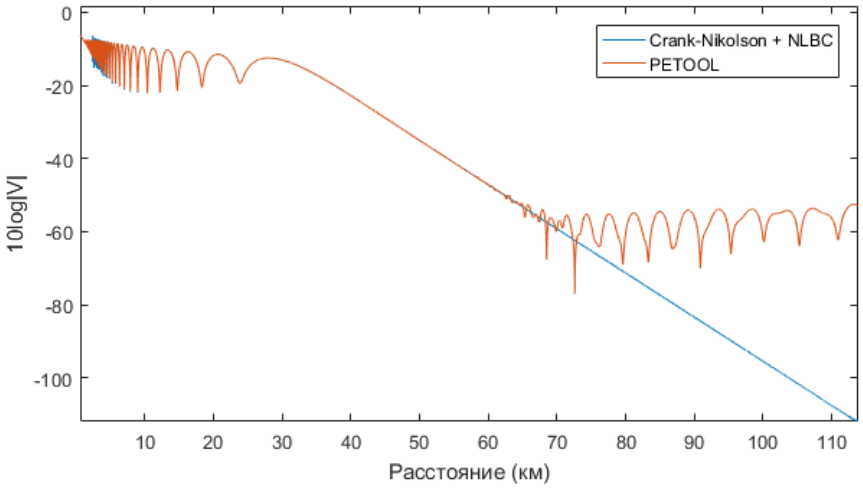


Рис. 1. Ложные отражения метода расщепления Фурье

Далее продемонстрируем работу алгоритма для приподнятого волновода [2], при наличии горизонтального препятствия. Распределение электромагнитного поля изображено на рис. 2.

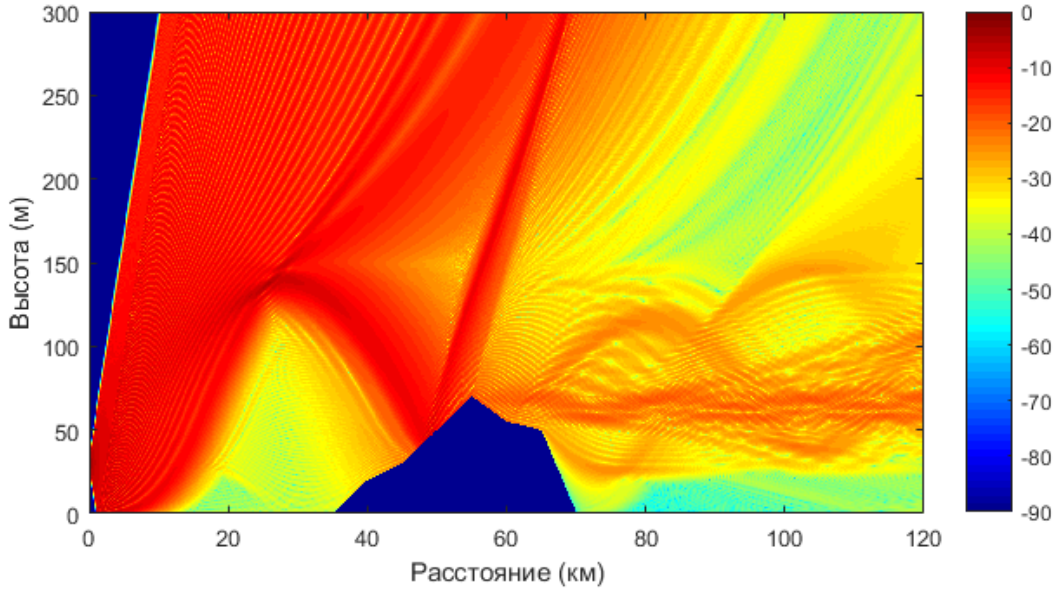


Рис. 2. Распределение электромагнитного поля 10log|V|

Таким образом, предлагаемый подход позволяет строить численное решение задачи на любых расстояниях без введения искусственного поглощающего слоя и прочих эмпирических приемов. Предложенные алгоритмы не требуют ручного подбора расчетных параметров в зависимости от входных данных, а максимальная точность в 110 дБ при решении задачи в стандартной арифметике двойной точности достигается автоматически. В дальнейшем планируется обобщить предложенный подход для произвольной аппроксимации Паде и подробнее исследовать особенности решения задачи в горизонтально неоднородной среде.

Список используемых источников

1. Zhang P., Bai L., Wu Z., Guo L. Applying the Parabolic Equation to Tropospheric Groundwave Propagation: A review of recent achievements and significant milestones // IEEE Antennas and Propagation Magazine. 2016. T. 58. №. 3. PP. 31–44.

2. Ozgun O., Apaydin G., Kuzuoglu M., Sevgi L. PETOOL: MATLAB-based one-way and two-way split-step parabolic equation tool for radiowave propagation over variable terrain // Computer Physics Communications. 2011. T. 182. №. 12. PP. 2638–2654.

3. Feshchenko R. M., Popov A. V. Exact transparent boundary conditions for the parabolic wave equations with linear and quadratic potentials // Wave Motion. 2017. T. 68. PP. 202–209.

4. Levy M. Parabolic equation methods for electromagnetic wave propagation. London. IET, 2000.

5. Ehrhardt M., Mickens R. E. Solutions to the discrete Airy equation: Application to parabolic equation calculations //Journal of computational and applied mathematics. 2004. T. 172. №. 1. PP. 183–206.

6. Dominguez V., Graham I. G., Smyshlyaev V. P. Stability and error estimates for Filon–Clenshaw–Curtis rules for highly oscillatory integrals // IMA Journal of Numerical Analysis. 2011. Т. 31. №. 4. С. 1253–1280.

Статья представлена научным руководителем, кандидатом технических наук А. Г. Владыко.

УДК 004.056 (075.8)

ВЕРОЯТНОСТНО-ВРЕМЕННЫЕ МЕТОДЫ ОЦЕНКИ СООТВЕТСТВИЯ АВТОМАТИЗИРОВАННЫХ СИСТЕМ ТРЕБОВАНИЯМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

А. В. Малых, Д. В. Юркин

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

Теория вероятностных графов является инструментом для анализа и моделирования процедуры определения временных характеристик вероятностных процессов с конечным числом дискретных состояний. В данной работе приведен вероятностно-временной подход к оценке математического ожидания времени выполнения и его дисперсии для процесса оценки соответствия автоматизированных систем требованиям по информационной безопасности. Вероятностно временной подход также позволяет оценить вероятность успешного выполнения оценки в заданное время.

автоматизированные системы, информационная безопасность, вероятностный граф, производящая функция, весовая функция, путь, контур, преобразование графа.

Вероятностно-временная методика оценки автоматизированных систем (АС) основана на теории вероятностных графов. Вероятностный граф применяется для анализа и моделирования дискретной системы событий, что показано в ряде работ по оценке механизмов защиты различных компонент АС [1, 2, 3]. Вероятностным графом дискретной системы называют графическое изображение последовательности операций по выполнению дискретных шагов в системе, отражающее вероятностно-временные соотношения, свойственные ее алгоритму [4]. Каждый из узлов вероятностного графа соответствует одному из характерных временных моментов состояния системы в процессе ее функционирования. Каждая из направленных ветвей отображает переход системы из одного состояния в другое.

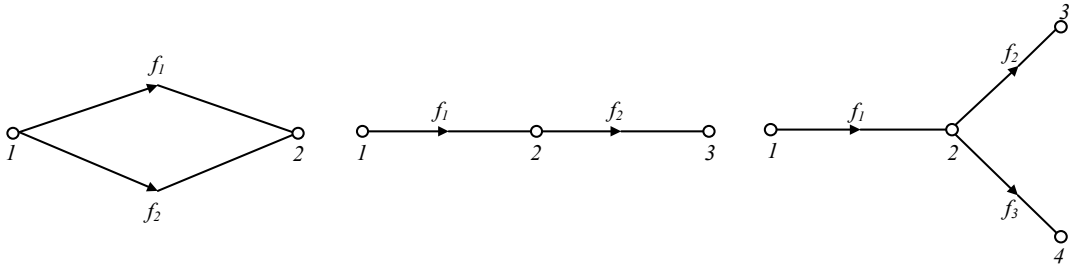
Согласно [5] функция *f(z)* является производящей функцией вероятностей p_i. Использование производящих функций при анализе вероятностных процессов с помощью графов упрощает решение задач.

Для анализа дискретных систем удобно предположить, что величины t_i кратны некоторой величине t, т. е. $t_i = a_i t$, где a_i – целые числа. При этом в качестве единицы масштаба времени примем t. Обозначив $z^t = x$, переходы можно описывать производящей функцией:

$$f(x) = \sum_{i=1}^{\nu} p_i x^{a_i} .$$

Для графа, состоящего из двух узлов и двух параллельных ветвей (рис. 1*а*) с производящими функциями $f_1 = \sum_{i=1}^{\nu} p_i x^{a_i}$ и $f_2 = \sum_{i=1}^{\mu} q_i x^{b_i}$, результирующая производящая функция, характеризующая переход из узла 1 в узел 2, равна:

$$f_{12p} = \sum_{i=1}^{\nu} p_i x^{a_i} + \sum_{i=1}^{\mu} q_1 x^{b_i} = f_1 + f_2 .$$



а) б) в)

Рис. 1. Граф: а) из двух параллельно соединенных ветвей;
б) из двух последовательно соединенных ветвей; в) с разветвлением

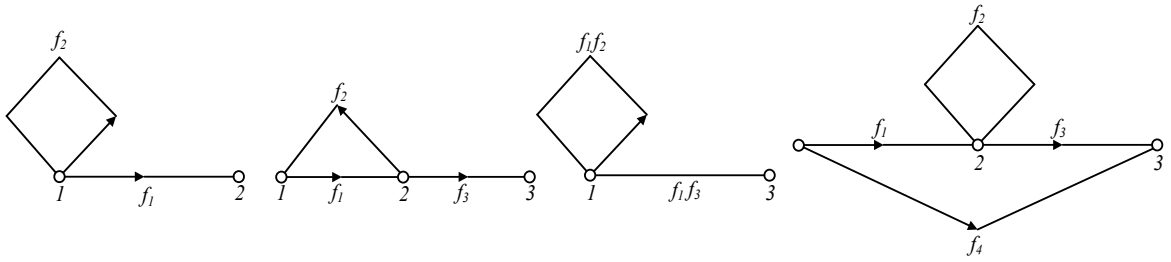
Для графа, состоящего из двух последовательно соединенных ветвей (рис. 1*б*) с теми же производящими функциями, при условии, что переходы из узла 2 в узел 3 и из узла 1 в узел 2 – события независимые, результирующие вероятности переходов находят путем перемножения исходных. Результирующее время перехода равно сумме времен переходов из узла 1 в узел 2 и из узла 2 в узел 3, следовательно:

$$f_{13p} = p_i x^{a_i} \sum_{i=1}^{\mu} q_i x^{b_i} + p_2 x^{a2} \sum_{i=1}^{\mu} q_i x^{b_i} + ... + p_\nu x^{a} v \sum_{l=1}^{\mu} q_i x^{b_i} =$$

$$= \left(\sum_{i=1}^{\nu} p_i x^{a_i} \right) \left(\sum_{i=1}^{\mu} q_i x^{b_i} \right) = f_1 f_2 .$$

Для графа с разветвлением (рис. 1в) $f_{13} = f_1 f_2, f_{14} = f_1 f_3$. Для графа с петлей (рис. 2*а*), т. е. переходом, начинающимся и заканчивающимся в одном и том же узле, рассмотрим сначала случаи $f_1 = p_1^{xa_1}, f_2 = p_2^{xa_2}$. При этом переходы из узла 1 в узел 2 возможны за время a_1 с вероятностью p_1, за время $a_1 + a_2$ – с вероятностью $p_1 \cdot p_2$, за время $a_1 + 2a_2$ – с вероятностью $p_1 \cdot p^2_2$ и т. д., за время $a_1 + ia_2$ – с вероятностью $p_1 \cdot p^i_2$. Следовательно,

$$f_{12p} = p_1 x^{a_1} + \ldots + p_1 x^{a_1} (p_2 x^{a_2})^i = f_1 + f_1 f_2 + \ldots + f_1 f_2^i = f_1/(1 - f_2).$$



а) б) в) г)

Рис. 2. Граф: а) с петлей; б) эквивалентный графу с петлей; в) граф, эквивалентный б); г) с замкнутым контуром и петлей

Аналогично можно показать, что граф рис. 2*б* имеет производящую функцию $f_{13p} = f_1 f_3/(1 - f_1 f_2)$, одинаковую с графом рис. 2*в*, а граф рис. 2*г* – производящую функцию $f_{13p} = f_4 + \frac{f_1 f_3}{1 - f_2} = \frac{f_1 f_3 + f_4 (1 - f_2)}{1 - f_2}$.

Для нахождения производящей функции в общем случае введем понятия пути и контура. Путем из узла *i* в узел *j* называется последовательность одинаково направленных ветвей графа, соединяющих узлы *i* и *j*. Контуром называется путь, начинающийся и заканчивающийся в одном и том же узле. Так, например, переход из узла 1 в узел 4 на графе рис. 3 состоит из трех путей с производящими функциями: $f^{\text{П}}_1 = f_2 f_3, f^{\text{П}}_2 = f_4 f_5, f^{\text{П}}_3 = f_7$ и двух контуров с производящими контурами: $f^{\text{К}}_1 = f_1 f_2, f^{\text{К}}_2 = f_6$.

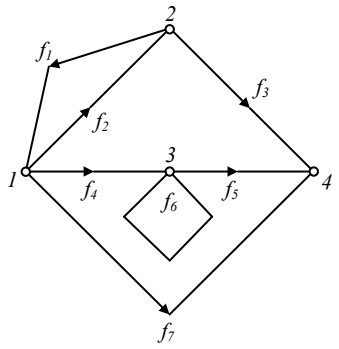


Рис. 3. К пояснению понятий пути и контура графа

В [6] показано, что если в общем случае переход из узла *i* в узел *j* состоит из *n* путей и *m* контуров, то результирующая производящая функция перехода определяется из выражения:

$$f_{ijp} = \frac{\{(f^{\text{П}}_1 + f^{\text{П}}_2 + \ldots + f^{\text{П}}_n)(1 - f^{\text{К}}_1)(1 - f^{\text{К}}_2)\ldots(1 - f^{\text{К}}_m)\}}{\{(1 - f^{\text{К}}_1)(1 - f^{\text{К}}_2)\ldots(1 - f^{\text{К}}_m)\}}.$$

Для определения общей весовой функции по значениям весовых функций отдельных элементов можно воспользоваться правилами эквивалентного преобразования. При последовательном соединении функции перемножаются. При параллельном соединении – суммируются. При наличии обратной связи общая весовая функция вычисляется по формуле $\frac{1}{1-f}$.

С учетом весовых функций ветвей и значений предыдущих узлов можно вычислить значение любого узла.

По правилу Мейсена весовая функция F между входом в точке A и выходом в точке B равна:

$$F_{AB(p)} = \sum_{K=1}^{m} \frac{f_K(p) * \Delta_K(p)}{\Delta(p)},$$

где m – число прямых путей между A и B; $f_k(p)$ – весовая функция k-го прямого пути от вершины A к вершине B (произведение функций всех ребер водящих в последовательность прямого пути); $\Delta(p)$ – главный определитель графа; $\Delta_k(p)$ – k-й минор определителя графа, равный определителю более простого графа, который получается из данного графа путем удаления из него всех ребер и вершин, лежащих на k-м прямом пути, а также всех ребер, входящих в эти вершины и исходящих из этих вершин. Частный случай, когда все контуры касаются k-го пути, $\Delta_k(p) = 1$.

Процедуру проведения проверки АС на выполнение требований можно представить в виде графа в котором узловые точки — это требования, а дуги тестовые испытания.

Данная методика в качестве оценки использует следующие параметры: среднее время (скорость) выполнения проверки $\overline{T}(p_{oo})$ и вероятность успешного выполнения $P(T_{exec} \le T)$ в заданное время.

Среднее время выполнения проверки $\overline{T}$ зависит от среднего количества проверок по каждому требованию на успешное выполнение итерации (обозначим эту величину через n). Тогда может быть представлено как произведение успешного выполнения итерации и времени T_i, затрачиваемого на одну итерацию: $\overline{T} = n \cdot T_i$.

Используя правила преобразования графов, можно найти производящую функцию $f(x)$ перехода из начальной вершины графа в конечную.

Из производящей функции графа получим среднее количество попыток n выполнения проверки на одну успешно завершенную.

Эффективность проверки может быть охарактеризована вероятностью его успешного выполнения в заданное время $P(T_{exec} \le T)$, так как время выполнения проверки является величиной переменной.

В результате, основываясь на теории вероятностных графов можно получить вероятностно-временные характеристики обобщенной процедуры

проверки АС по установленным требованиям в сфере информационной безопасности. С помощью описанной выше методики можно оценить влияние различных условий и порядок организации проведения испытаний на среднее время выполнения, вероятность успешного завершения в заданное время и трудоемкость тестовых испытаний.

Список используемых источников

1. Юркин Д. В., Винель А. В., Таранин В. В. Анализ временных и сложностных характеристик парольной аутентификации в защищенных операционных системах семейства UNIX // Информационно-управляющие системы. 2013. № 3 (64). С. 62–66.

2. Юркин Д. В., Никитин В. Н. Улучшение вероятностно-временных характеристик протоколов инкапсуляции 802.11 // Информационно-управляющие системы. 2014. № 2 (69). С. 44–49.

3. Никитин В. Н., Юркин Д. В. Влияние механизмов защиты на пропускную способность каналов с ошибками // Защита информации. Инсайд. 2009. № 3 (27). С. 46–51.

4. Емельянов Г. А., Шварцман В. О. Теория передачи дискретной информации. М. : Связь, 1979. 336 с.

5. Захаров А. И. Анализ систем с переспросом // Материалы семинара по кибернетике. Кишинев, 1968. Вып. 5/

6. Мэзон С. М., Циммерман Г. Электронные цепи, сигналы и системы: пер. с англ. Под редакцией П. А. Ионкина. М.: ИИЛ, 1963.

УДК 004.056.5

ИССЛЕДОВАНИЕ ИНЖИНИРИНГА ТРАФИКА В СЕТЯХ MPLS

И. О. Махова[1], И. Ю. Потехин[2], Д. В. Сахаров[1,2]

[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 (Роскомнадзор) по Северо-Западному федеральному округу

Данная статья посвящена технологии инжиниринга трафика на базе MPLS. В статье рассматриваются методы, задачи и способы восстановления трафика. Рассматриваемая технология является актуальной в настоящее время, так как механизм коммутации, основанный на метках, базируется на принципе разделения функций управления и пересылки пакетов, что позволяет значительно увеличивать масштабирование и скорость обработки трафика.

MPLS, Traffic Engineering, LSP-туннель, Virtual Private Network, маршрутизация.

На сегодняшний день отрасли телекоммуникаций стремительно развиваются. Одним из шагов на пути усовершенствования мельтисервисной сети является появление методов многоуровневой коммутации, которая позволяет логически структурировать сеть, не жертвуя ее производительностью. Последним словом развития механизмов маршрутизации и коммутации для магистралей сети интернет является технология многопротокольной коммутации, основанная на метках. Данный механизм основан на принципе разделения функций для управления процессом пересылки пакетов, который значительно улучшает масштабирование и скорость обработки трафика.

Multiprotocol Label Switching (MPLS) представляет собой механизм многопротокольной коммутации по меткам и реализуется следующим алгоритмом. Каждому IP-пакету назначается 32-битная метка между заголовками второго и третьего уровней модели OSI. На основании значения метки, маршрутизатор принимает решение о передачи пакета следующему устройству. Обмен метками может реализовываться как с помощью специального протокола распределения меток (далее-LDP), так и с помощью других протоколов сигнализации в сети, например, протокола резервирования сетевых ресурсов (далее-RSVP).

Для маршрутизации пакетов данных, используются LSR-маршрутизаторы. LSR представляет собой устройство, выполняющее маршрутизацию, основываясь только на значениях меток. Распределение меток между LSR приводит к установлению внутри домена MPLS путей с коммутацией по меткам. Каждый LSR-маршрутизатор содержит таблицу, которая ставит в соответствие паре «входной интерфейс, входная метка», тройку «префикс адреса получателя, выходной интерфейс, выходная метка».

Получая пакет, LSR по номеру интерфейса и значению метки определяет для него выходной интерфейс. Далее, старое значение метки заменяется новым, и пакет отправляется к следующему LSR. Рис. 1 отображает построение LSP-туннеля от входного (*Ingress* LSR) до выходного (*Egress* LSR).

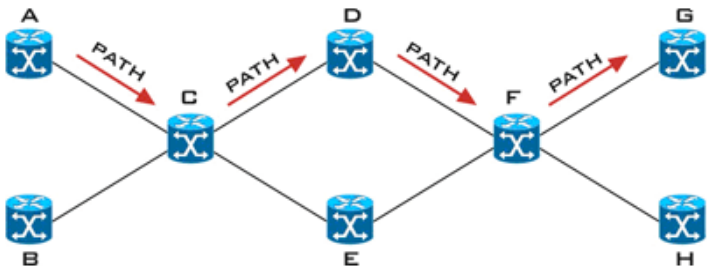


Рис. 1. Построение LSP-туннеля

Для объединения нескольких удаленных пользователей и сайтов клиентов в частную сеть предприятия используется технология Virtual Private

Network (VPN). VPN представляет собой виртуальную частную сеть, которая создается поверх незащищенных сетей. С помощью VPN можно реализовать такие соединения как сеть-сеть, узел-сеть или узел-узел. Такие свойства технологии VPN предоставляют возможность для объединения территориально удаленных друг от друга локальных сетей в единую информационную сеть.

Теперь пойдет речь о MPLS VPN. Сеть MPLS включает в себя две области: сеть клиентов (*Customer Edge Router*) и внутреннюю сеть провайдера (*Provider Edge Router*), которая используется для объединения сетей клиентов. Маршрутизатор, с помощью которого сайт клиента подключается к магистрали провайдера, называется пограничным маршрутизатором клиента (CE). CE может быть соединен с магистральной сетью провайдера с помощью нескольких каналов. Магистральная сеть провайдера представляет собой сеть MPLS, в которой IP-пакеты продвигаются с помощью локальных меток. Сеть MPLS состоит из LSR-маршрутизаторов. В сети провайдера также выделяют пограничные маршрутизаторы (PE), которые представляет собой устройства, присваивающий начальную MPLS-метку пакетам до их отправки на P-маршрутизатор и удаляет эту метку, когда пакеты покидают сеть MPLS. Пограничные маршрутизаторы являются очень важной частью MPLS VPN. На них возлагается главная задача по поддержке VPN – это разграничение маршрутов и данных, которые поступают от разных CE. Также PE служат конечными точками пути LSP (*Label Switch Path*).

Следуя из вышесказанного, можно выделить некоторые преимущества использования VPN на базе MPLS: хорошую масштабируемость, возможность пересечения адресных пространств, подключенных к VPN и изолирование трафика VPN друг от друга на канальном уровне [1]. По умолчанию, процесс MPLS состоит в построении кротчайшего LSP-пути, который выбирает протокол маршрутизации.

MPLS Traffic Engineering используется для создания LSP-туннеля, который расходится с кратчайшем путем. LSP-туннель представляет собой однонаправленный канал следования пакетов, проходящих через сеть MPLS. В этом ему помогают протоколы CR-LDP и RSVP. CR-LDP – является вариантом LDP, в котором определены механизмы создания и поддерживания трактов LSP с явно заданным маршрутом. RSVP- протокол резервирования ресурсов. MPLS/TE поддерживает автоматическую генерацию LSP, где протоколы Open Shortest Pass First (OSPF) и IS-IS (протокол маршрутизации промежуточных систем) используются для распространения информации об имеющихся ресурсах и для ограничения сети. Также LSP можно построить вручную (статически), путем перечисления LSR-маршрутизаторов. Для обмена информацией о маршрутах между маршрутизаторами используется протокол внутренних шлюзов-IGP (*Interior Gateway Protocol*) [2].

На рис. 2 изображено как протоколы IGP и LDP передают маршрутную инфромацию и метки для сети 10.0.0.0/16. Если все LSR-устройства имеют одинаковую IGP-стоимость, то по умолчанию LSP-маршрут будет построен от роутера A, через роутер B и D, до роутера F.

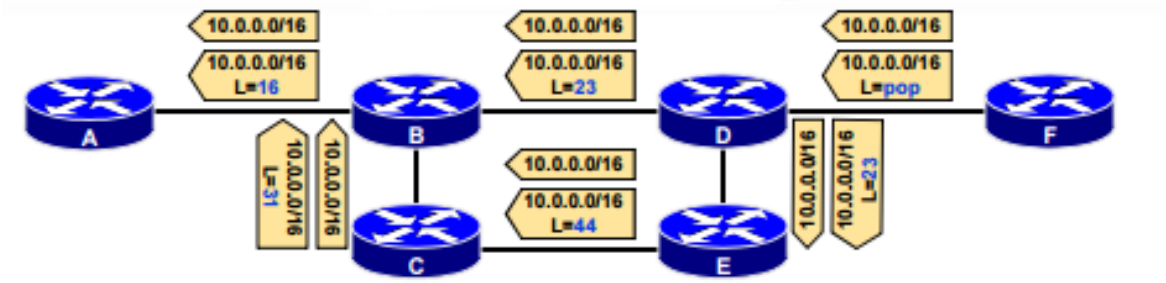


Рис. 2. Организация передачи маршрутной информации

IGP и LDP/TDP создает новый LSP-туннель, основываясь на кратчайшем пути, который определяет протокол IGP. Данный путь будет создан посредством MPLS/TE LSP. После установления соседских отношения между маршрутизаторами A и E, роутер A получает еще одно обновление для сети 10.0.0.0/16 – метку 44.

Маршрут назначения может быть включен в базу данных IGP для дальнейшего вычисления алгоритма Shortest Path First (далее SPF). Суть данного алгоритма Дийкстры заключается в том, что протокол OSPF вычисляет кратчайшие пути между заданным LSR-вершиной графа и всеми остальными вершинами, основываясь на базе данных об условиях использования возможных связей. Результатом работы SPF является таблица, в которой для каждой вершины графа сети MPLS указан список ребер, соединяющих ее со всеми другими вершинами графа, используя кратчайший путь. Исходя из данного алгоритма, можно сказать, что теперь маршрутизатор A может выбирать между двумя имеющимися путями. В зависимости о конфигурации MPLS/TE, роутер A может решить, что наиболее кратчайшим путем в сеть 10.0.0.0/16 является MPLS/TE-туннель.

Для хранения маршрутов и исходящих интерфейсов используется FIB-таблицы. Рис. 3 отображает содержимое FIB и LFIB таблиц после того, как IGP, LDP и RSVP распространили маршрутную информацию и метки.

Когда маршрутизатор A пересылает пакет в сеть назначения 10.0.0.0/16, он должен внести его в LSP для данной сети. Однако, этот LSP идет по другому туннелю. Поэтому к отправляемому пакету должны быть прикреплены 2 метки: верхняя метка (54) используется для LSP, который был построен с помощью протокола RSVP; вторая метка (44) была постро-

ена с помощью LDP и представляет собой LSP для сети 10.0.0.0/16. Маршрутизатор B просто пересылает пакет на основе верхней метки (метка 19 заменяет метку 54). Роутер C пересылает пакет на основе верхней метки, которая также удаляется (*pop actions*). Pop-label – это операция удаления метки (узел получает пакет MPLS и убирает верхнюю метку (*top label*) перед дальнейшей передачей) [3]. Теперь пакет содержит только одну метку. Маршрутизатор E пересылает пакет на основе оставшейся метки (44) и заменяет ее на метку 23. Маршрутизатор D пересылает пакет на основе метки 23, затем удаляет ее (*Penultimate Hop Popping*). Роутер F пересылает пакет на основе адреса назначения, который хранится в IP-заголовке.

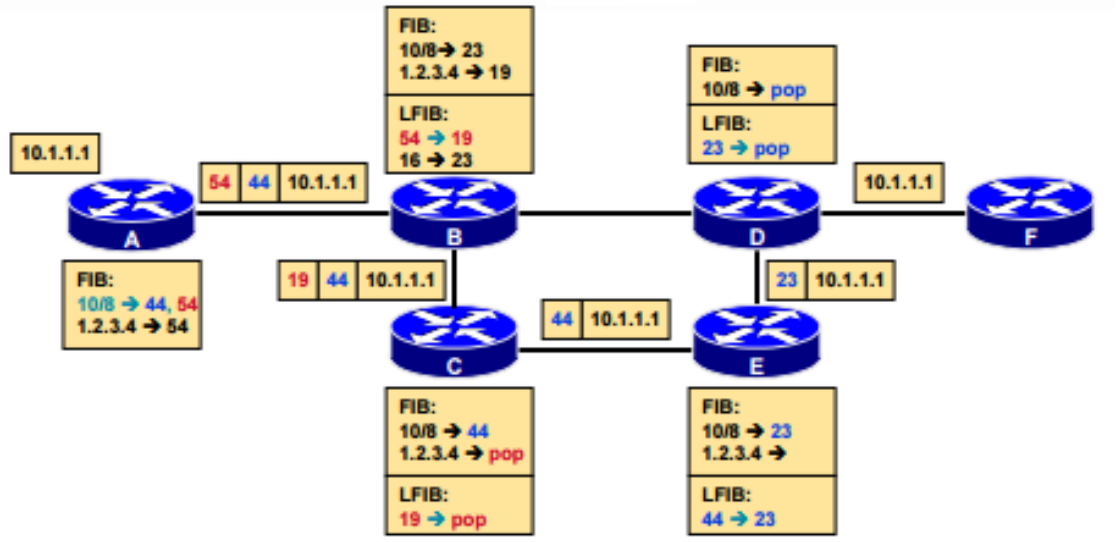


Рис. 3. Характеристика FIB и LFIB таблиц

Как видно из предыдущих примеров, MPLS Traffic Engineering может быть использован для балансировки нагрузки на LSP-путь [4].

В данной статье был рассмотрен механизм многопротокольной коммутации, основанный на метках, и приведены сравнительные характеристики протоколов распространения меток: RSVP и LDP. Исходя из данной статьи, можно сделать вывод, что протокол MPLS является удобным средством организации VPN-сетей, с помощью которого обеспечивается их безопасность. Применение технологии MPLS привело к фундаментальному изменению структуры сети интернет и оказало существенное влияние на механизмы передачи IP- пакетов [5].

Список используемых источников

1. Awduche D., Berger L., Gan D. RSVP-TE: Extentions to RSVP for LSP Tunnels // RFC 3209, Dec. 2001. 26 с.

2. Гринфильд Д. Глобальная служба MPLS: опережая время // Журнал сетевых решений LAN. Март 2002. 134 с.

3. Олвейн В. Структура и реализация современной технологии MPLS. М. : Вильямс, 2004. 480 с. ISBN 5-8459-0633-4.

4. 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.

5. Красов А. В., Левин М. В., Цветков А. Ю. Метод управления трафиком в гибридной программно-определяемой сети // Информационные технологии и телекоммуникации. 2016. Т. 4. № 2. С. 53–63.

УДК.621.391

ТЕСТИРОВАНИЕ ЯДРА СЕТИ SDN НА БАЗЕ КОММУТАТОРОВ MIKROTIK

А. С. Мутханна, А. А. Хакимов

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

SDN – это идеология построения сетей, в которой весь интеллект сети вынесен на отдельную аппаратную/программную базу, а все управление трафиком происходит на основе специальных протоколов (например, OpenFlow), которые оперируют понятием поток (flow) и могут совершать различные действия с ним (разрешить, запретить, перенаправить, переписать поля в пакетах и т. д.). Фактически, на контроллере определяется политика управления сетью на основе заданных правил, а также работы специализированных приложений (например, эмулирующих работу STP или протоколов маршрутизации). Конечный результат передается на коммутаторы по протоколу OpenFlow в виде flow-таблиц, содержащих информацию о том, куда, как и какой трафик передавать. С одной стороны, такой подход дает большую гибкость в управлении сетью, с другой существенно упрощает администрирование, отчасти и архитектуру сети. В нашей работе на базе модельной сети СПбГУТ подняли сеть, где ядро состояло из трёх логических коммутаторов производителя mikrotik поддерживающие протокол openflow v1.0. Создав сеть на базе контролера opendaylight мы протестировали скорость составления коммутационной таблицы для коммутаторов. работоспособность контролера на разные виды трафика в том числе для трафика IoT. Также анализировали поведение контролера на работу сервиса IoTDM поверх сети SDN.

OpenFlow, SDN, mikrotik, коммутатор.

Введение

Статья посвящена тестированию системы менеджмента Интернет Вещей на базе ядра сети SDN [1] и взаимодействию трафика Интернет Вещей и SDN коммутаторов компании Mikrotik. В качестве метода исследования

поведения как системы менеджмента, так и сетевой инфраструктуры проводилось тестирование трафиком Интернета Вещей, генерируемого разработанными генераторами на базе спецификаций партнерского проекта oneM2M [2, 3]. В ходе тестирования сетевой инфраструктуры были определены такие параметры, как: количество одновременно поддерживаемых сессий коммутатором Mikrotik, при использовании различных протоколов транспортного уровня, предложена рекомендация по динамическому изменению виртуальных буферов.

С целью исследования влияния сети SDN на параметр RTT трафика большого количества Интернет Вещей и условии передачи его в совокупности с гетерогенным трафиком в сети, был проведен натурный эксперимент на разработанной модели, которая в свою очередь отражала возможную схему распределения определенной системы мониторинга и управления для массивного количества Интернета Вещей [4, 5, 6].

Постановка задачи

В рамках исследования взаимодействия трафика Интернет Вещей с сетью SDN и при условии передачи его вместе с гетерогенным трафиком, была сформирована задача – провести тестирование сети SDN на предмет быстроты организации сетевой инфраструктуры при первичном подключении коммутаторов, организации буферов коммутатора (рис. 1).

Рис. 1. Архитектура лабораторного стенда

Лабораторный стенд состоит из:
- контроллер – OpenDaylight Berillium SR4;
- коммутаторы – Microtik с поддержкой протокола openflow v.1.1;
- сервер oneM2M – IoTDM (*OpenDaylight Boron* SR1);
- Cisco Catalyst 3750;
- генераторы трафика IoT (*mqtt, coap, http*);
- генератор iperf3.

В качестве генератора нагрузки для тестирования ядра сети SDN применялся генератор iperf3, позволяющий гибко настраивать параметры трафика. В данном тесте генератор был настроен таким образом, чтобы сымитировать нагрузку трафиком IoT, это отражалось в установленных размерах пакетов: не более 190 байт.

В процессе проводимого тестирования производилось увеличение количества сессий, одновременно проходящих через каждый коммутатор. Тестирование производилось с использованием протоколов: UDP и TCP.

Результаты тестирования

Результаты тестирования отображены на рис. 2 и 3, при чем каждый из графиков отображает зависимость на каждом из коммутаторов.

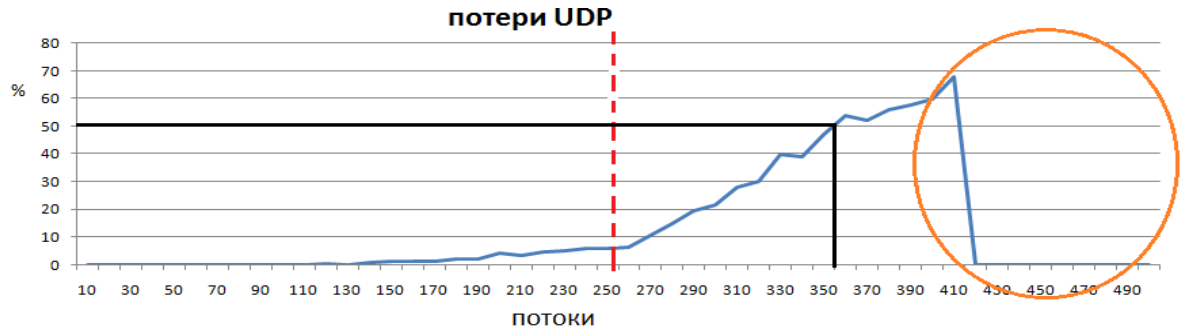


Рис. 2. График потерь пакетов udp от увеличения количества сессий

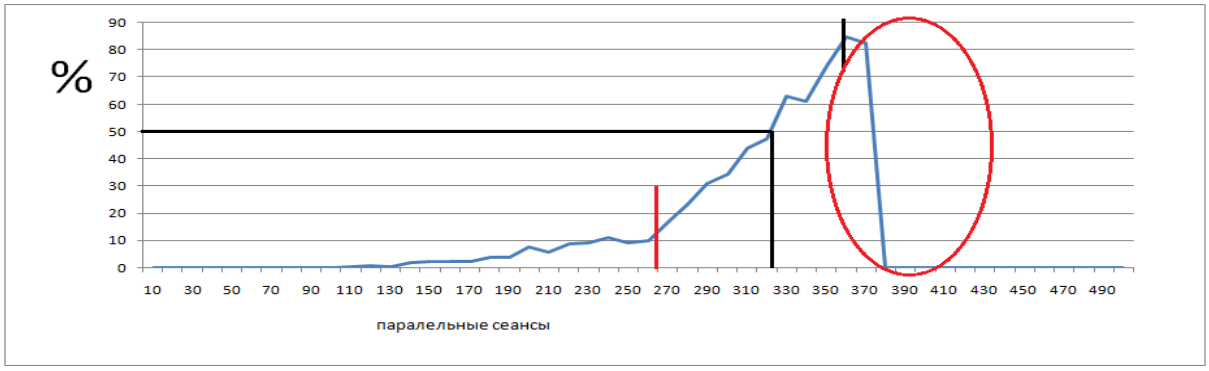


Рис. 3. График количества оборванных сессий в сети при увеличении их количества

Как видно по графикам, отображенным на рис. 2 и 3, при увеличении количества соединений, резко возрастают потери после определенного значения количества одновременных соединений на каждом из SDN коммутаторов. При этом можно сделать вывод, что при использовании TCP, количество одновременных возможных соединений меньше (~360 на пике), чем при использовании протокола UDP (~ 400–410 на пике). Обрыв графиков означает выход из строя сетевой инфраструктуры (выключение коммутаторов Mikrotik и их незапланированная перезагрузка). По результатам

теста можно сделать вывод: такой тип коммутаторов возможен только при организации внутренних корпоративных сетей небольшого размера. Так же после изучения реакции коммутаторов на трафик подобного типа, сделали вывод по вопросу использования буферов на SDN коммутаторах. Для тонкой настройки объема буфера в сетевых узлах используют формулу $B = P$ * RTT, где B – размер буфера, P – пропускная способность, а RTT – Round Trip Time. С помощью этой формулы можно легко настроить оптимальный размер буфера (очереди). Но данная формула не учитывает количество параллельных потоков, которые могут быть разные по типу (независимые друг от друга). В классических сетях используют дополнение к этой формуле:

$$B=\frac{RTT*P}{\sqrt{N}},$$

где N – количество независимых сеансов.

Заключение

На базе модельной сети СПбГУТ тестировали ядро сети, которая состоит из трёх логических коммутаторов производителя mikrotik поддерживающие протокол openflow v1.0. Создав сеть на базе контролера opendaylight была протестирована скорость составления коммутационной таблицы для коммутаторов. работоспособность контролера на разные виды трафика в том числе для трафика IoT. Также анализировали поведение контролера на работу сервиса IoTDM поверх сети SDN.

По результатам тестирования доказали то что такой тип коммутаторов возможен только при организации внутренних корпоративных сетей небольшого размера. Так же после изучения реакции коммутаторов на трафик подобного типа, сделали вывод по вопросу использования буферов на SDN коммутаторах.

Список используемых источников

1. Vladyko A., Muthanna A., Kirichek R. Comprehensive sdn testing based on model network // Lecture notes in computer science. 2016. PP. 539–549.

2. Jaeseok Yun. Interoperability between IoT Platforms // Workshop on the Future of IoT Standard Technology, Dec. 2015.

3. Onem2m [Электронный ресурс]. URL: URL:http://www.onem2m.org/about-onem2m/why-onem2m (дата обращения 10.12.2016).

4. Radek Fujdiak, Pavel Masek, Petr Mlynek, Jiri Misurec, Ammar Muthanna: Advanced optimization method for improving the urban traffic management. FRUCT 2016: 48–53.

5. Хакимов А. А., Мутханна А. С., Кулик В. А., Киричек Р. В. Анализ производительности шлюза умного дома на базе облачной платформы alljoyn // Информационные технологии и телекоммуникации. 2016. № 2. С. 77–85.

6. Мутханна А. С., Хакимов А. А. Сравнение протоколов web-вещей // Информационные технологии и телекоммуникации. 2015. № 4 (12). С. 97–107.

УДК 621.39

ДИНАМИЧЕСКОЕ НАЗНАЧЕНИЕ ПОЛОСЫ ПРОПУСКАНИЯ В СЕТЯХ PON

А. В. Новиков, А. Р. Салтыков

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

Динамическое назначение полосы пропускания, в пассивных оптических сетях представляет собой один из ключевых аспектов, обеспечивающих эффективность использования полосы пропускания в восходящем потоке пассивных оптических сетей. В статье произведено исследование организации процедуры DBA для двух основных стандартов пассивных оптических сетей – GPON (ITU-T G.984) и EPON (IEEE 802.3ah).

DBA, GPON, EPON, ONT, OLT.

Структура сетей пассивных оптических сетей (PON) не позволяет абонентским устройствам ONT анализировать трафик друг друга в восходящем направлении.

В связи с этим вводится понятие динамического назначения полосы пропускания, представляющего собой механизм или алгоритм динамического распределения полосы пропускания для быстрого перераспределения полосы пропускания на основании требований службы текущего пользователя. Коэффициент использования полосы пропускания сети PON может быть увеличен посредством динамической настройки полосы пропускания в соответствии с требованиями абонентских терминалов ONT.

DBA в сетях GPON

Процедура DBA (*Dynamic Bandwidth Allocation*) управляется со стороны OLT, назначающего полосу пропускания для восходящего потока. Поскольку нисходящий поток является широковещательным (*broadcasting*), механизм DBA для него неработоспособен. Использование механизма множественного доступа с временным разделением каналов в восходящем направлении требует, чтобы OLT планировал передачу трафика от каждого ONT в отдельности во избежание коллизий. По сути, каждый ONT получает grant (разрешение), в котором указывается начало и конец передачи. В сетях GPON [1] разрешения передаются в заголовках кадров в нисходящем направлении. Карта распределения полосы пропускания (BW Map) в заголовках данных кадров определяет контейнеры передачи (T-CONT), а также начало и конец передачи: (*Alloc-ID, Start, End*) для каждого гарантированного окна (таймслота) в восходящем направлении (рис. 1).

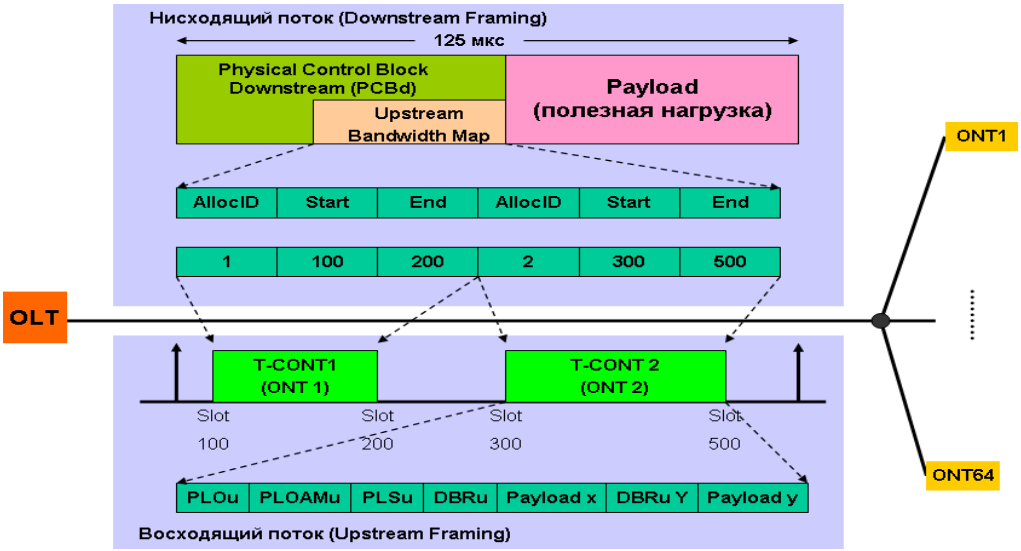


Рис. 1. Распределение полосы пропускания в восходящем потоке GPON (пример T-CONT1 и T-CONT2)

Алгоритмы DBA в GPON [2] делятся на две категории – SR-DBA (*Status Reporting* DBA) и NSR-DBA (*Non Status Reporting* DBA). В SR-DBA, основанном на отчете о статусе, T-CONT показывает (индицирует) количество пакетов в буфере ONT, ожидающих своей отправки. Чтобы определить, какое количество трафика назначить для ONT, OLT необходимо знать статус всех T-CONT, относящихся к ONT. Как только OLT принимает эту информацию, то может назначить полосу пропускания соответствующим образом. Когда ONT не имеет информации, ожидающей передачи, оно, при получении разрешения (GRANT) отправляет пустую (*idle*) ячейку в восходящем направлении, чтобы индицировать, что его буфер пустой. Это информирует OLT о том, что разрешения (GRANTs), изначально предназначенные для данного T-CONT, могут быть использованы для других T-CONTs. Если ONT имеет длинную очередь пакетов, ожидающих отправки в его буфере, OLT может назначить для данного ONT несколько T-CONT.

NSR-DBA обеспечивает назначение полосы пропускания без отчета о статусе буфера ONT, используя механизм мониторинга трафика со стороны OLT.

DBA в сетях EPON

В сетях EPON [3] за процедуру DBA отвечает протокол MPCP (*Multi Point Control Protocol*), работающий на уровне управления средой доступа (MAC – уровень).

Сообщение GATE используется, чтобы информировать каждый ONT о его времени ожидания (idle time) и размере окна передачи трафика (*window*

size) – времени использования восходящего потока. OLT посылает сообщение GATE каждому ONT последовательно в соответствии с размером окна и задержкой распространения (*propagation delay*). Размер окна для каждого ONT считается в соответствии с его требованиями. Требования от ONT приходят к OLT сообщениях REPORT в начале и конце окон в восходящем направлении. Необходимость в полосе пропускания считается в соответствии с загруженностью буфера ONT и текущим окном передачи трафика.

Существует множество критериев распределения полосы пропускания в сетях EPON (рис. 2).

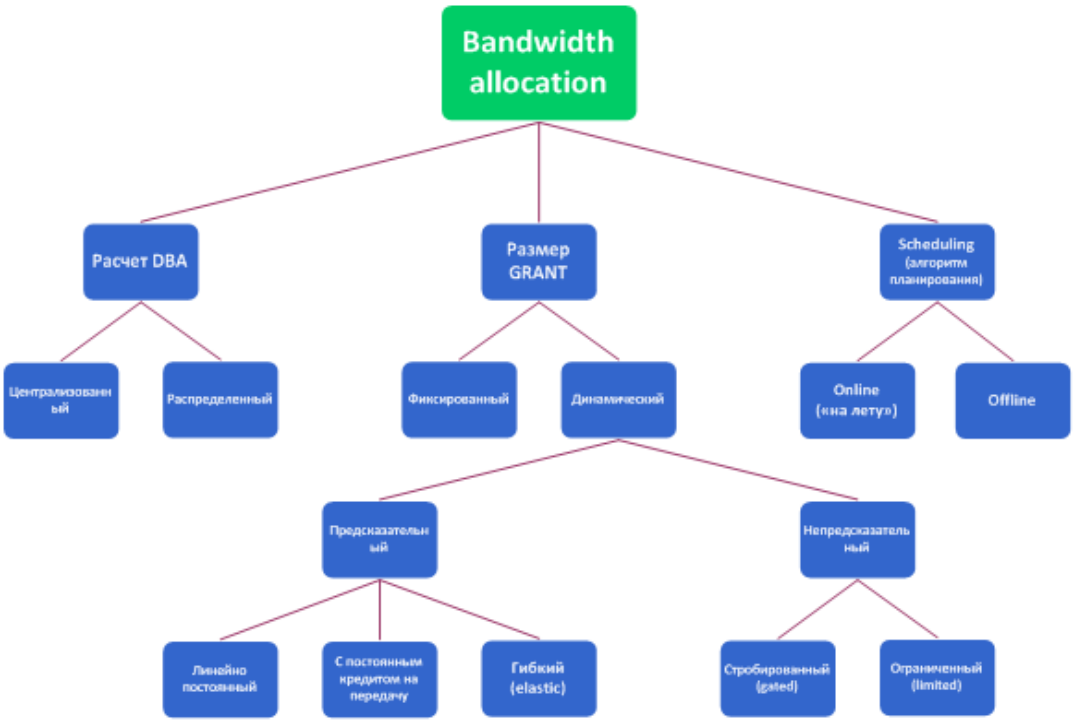


Рис. 2. Блок-диаграмма критериев распределения полосы пропускания в EPON

Из блок-диаграммы видно, что OLT вычисляет полосу пропускания как методом централизованного планирования, так и методом распределенного планирования при участии OLT и ONT. Во втором случае полоса пропускания считается самим ONT, хотя OLT также может выполнить эту функцию.

В связи с вышеизложенным далее рассматривается несколько основных алгоритмов DBA, используемых в EPON.

Алгоритм IPACT

IPACT – Interleaving Polling with Adaptive Cycle Time – чередование опроса с автоматически изменяющимся временем цикла – один из самых первых алгоритмов, предложенных еще в 2002 г. одним из основателей стандарта EPON Гленом Крамером [4, 5].

IPACT использует метод чередования опроса, при котором каждый последующий ONT опрашивается перед тем, как закончится передача предыдущего ONT, чтобы использовать канал наиболее эффективно (рис. 3). Время цикла подстраивается под требования к ПП от ONT. Определение максимального окна передачи (*Maximum Transmission Window* – MTW) не позволяет одному ONT занимать всю полосу пропускания.

Таким образом, перед тем, как OLT примет сообщение REPORT от ONT-3, он уже знает, когда придет последний информационный бит от ONT-3. Поэтому OLT начинает генерировать и отправлять сообщение GATE в сторону ONT-1 для следующего цикла опроса в таком порядке, что первый бит данных от ONT-1 прибывает сразу же после последнего бита данных от ONT-3.

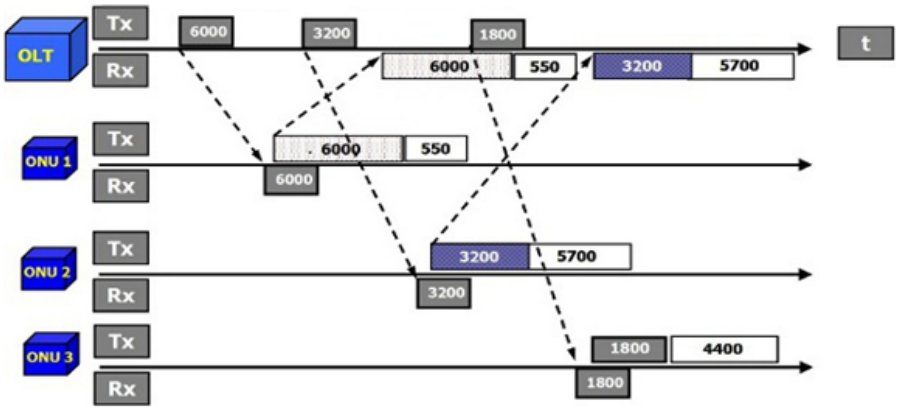


Рис. 3. Механизм предоставления полосы пропускания в IPACT

Алгоритм offline DBA

В данном алгоритме OLT ожидает сообщения REPORT от всех ONT в системе. Затем отправляет сообщения GATE каждому ONT для распределения в следующем цикле (рис. 4).

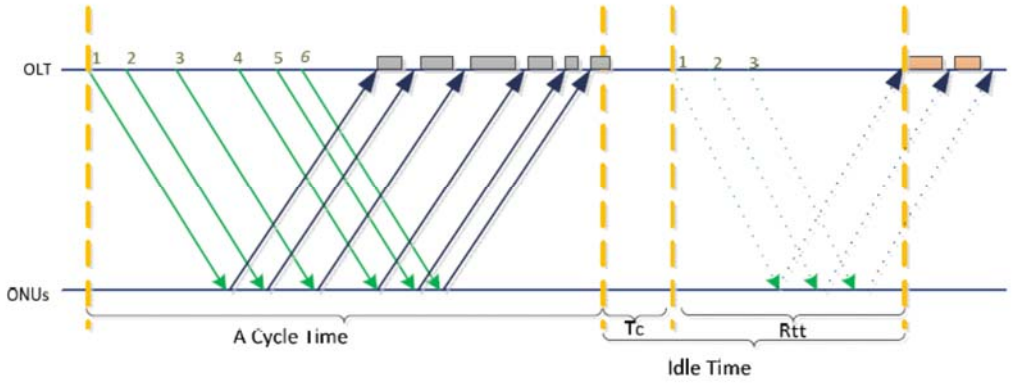


Рис. 4. Механизм предоставления полосы пропускания в offline DBA

Здесь OLT получает все запросы от ONT перед началом обслуживания. Таким образом, OLT может справедливо распределить избыточную полосу между высоконагруженными ONT.

Как только OLT заканчивает обслуживание всех ONT в системе, он не отправляет сообщение GATE в течение времени обработки, чтобы обработать все ответы от ONT.

Канал в восходящем направлении снова начинает использоваться, как только ответ от первого обслуженного ONT приходит на OLT.

Алгоритм Half Cycle DBA (hcDBA)

Алгоритм hcDBA направлен на обеспечение промежуточного решения между online и offline DBA алгоритмами, наследуя преимущества обоих. В offline режиме, вместо расчета в конце полного цикла, принимается расчет в ходе половины цикла (рис. 5). Таким образом, проблема незанятого периода времени, который происходит во время расчетов отправки сообщений OLT, преодолевается. Это алгоритм называется «алгоритм полуциклического динамического распределения пропускной способности».

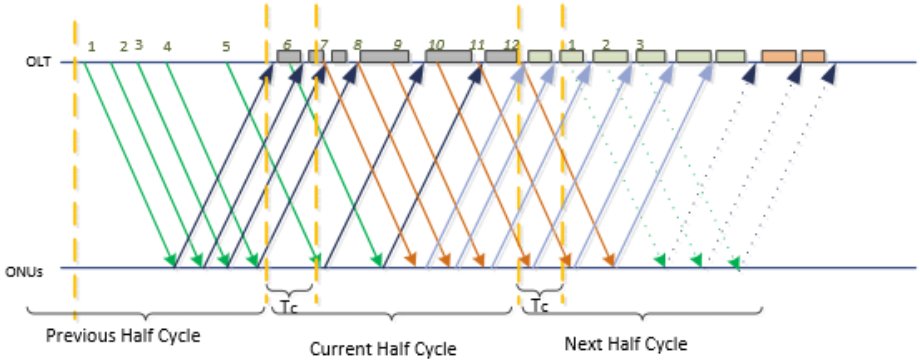


Рис. 5. Механизм предоставления полосы пропускания в hcDBA

В методе hcDBA, если OLT получает сообщения REPORT более чем от половины ONT, он выделяет полосу пропускания для половины ONT, не получая все сообщения REPORT. Если OLT не получил сообщения REPORT от половины ONT, то OLT обращается к режиму online DBA, OLT отправляет GATE сообщение для следующего ONT в порядке расписания.

Выводы

DBA в сетях GPON реализуется с двумя основными способами: на основании отчетов ONT (*Status Reporting*) и автоматически (*Non-Status Reporting*).

DBA в сетях EPON имеет множество способов реализации. Авторами приведена их классификация, а также в качестве примеров рассмотрены механизмы IPACT, offline DBA, hcDBA.

Список используемых источников

1. Recommendation G.984.1. Gigabit-Capable Passive Optical Networks (G-PON): General Characteristics. ITU-T, Geneva, Switzerland, 2008. 43 p.

2. Karamitsos Loannis, Al-Arfai Khalid. Bandwidth Allocation DBA (BA-DBA) Algorithm for xPON Networks // International Journal of Computer Applications. July 2012. V. 50, № 12. PP. 42–46.

3. Kramer G. Ethernet Passive Optical Networks. New York : McGraw-Hill, 2005. 307 p.

4. Kramer G., Mukherjee B., Pesavento G. Interleaved Polling with Adaptive Cycle Time (IPACT): a Dynamic Bandwidth Distribution Scheme in an Optical Access Network // Photonic Network Communications. 2002. V. 4, № 1. PP. 89–107.

5. Lannoo B., Verslegers L., Colle D., Pickavet M., Demeester P., Gagnaire M. Thorough analysis of the IPACT Dynamic Bandwidth Allocation Algorithm for EPONs // 4th International Conference on Broadband Communications, Networks and Systems Photonic, 2007, USA. Proceedings of the conference, 2010. V. 1–2 PP. 486–494.

Статья представлена заведующим кафедрой, кандидатом технических наук, доцентом С. Ф. Глаголевым.

УДК 621.396

ИССЛЕДОВАНИЕ ВЛИЯНИЯ ПАРАМЕТРОВ БЕСПРОВОДНЫХ САМООРГАНИЗУЮЩИХСЯ СЕТЕЙ СВЯЗИ НА КАЧЕСТВО ОБСЛУЖИВАНИЯ

А. И. Парамонов, Б. Х. Чинь

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

В статье рассмотрены основные параметры качества обслуживания трафика в беспроводных самоорганизующихся сетях связи. Приведён анализ зависимости распределения длины маршрута (по расстоянию и по скачкам) от структурных параметров БСС сети на базе разработанной имитационной модели в Mathcad и с помощью инструмента COOJA в операционной системе Contiki. Также приведён анализ эффективности работы протокола RPL при различной плотности размещения узлов в БСС с помощью моделирования в операционной системе Contiki.

беспроводная самоорганизующаяся сеть, длина маршрута, Mathcad, операционная система Contiki, COOJA, RPL.

Беспроводные самоорганизующиеся сети (БСС) – децентрализованные беспроводные сети, не имеющие постоянной структуры. БСС характеризуются динамическими изменениями топологии, ограниченной пропускной способностью, емкостью батарей (аккумуляторов) в узлах, неоднородностью ресурсов узлов, безопасностью и др. [1]. Архитектура БСС, как правило, имеет кластерную организацию, при этом возможна организация как одношаговой (между членом кластера и головным узлом), так и многошаговой маршрутизации (между головными узлами кластеров). Многошаговая маршрутизация используется также в однородной БСС без кластеризации. Поскольку число узлов в зоне обслуживания БСС может достигать десятков тысяч, то задача выбора протокола маршрутизации, обеспечивающего меньшее число шагов, а значит и меньшую задержку, является важной при проектировании и планировании БСС. Кроме того, параметры качества обслуживания БСС, такие как время доставки пакета, потери, доля транзитных узлов, нагрузки на транзитные узлы и др. также зависят от связности сети [2, 3]. Параметры качества обслуживания также зависят от длины маршрутов в БСС [2, 4].

В статье на базе разработанной имитационной модели в Mathcad и с помощью имитационного моделирования в среде COOJA, поддерживаемой ОС Contiki и разработанной специально для БСС, проведено анализ зависимости распределения длины маршрута (по расстоянию и по скачкам) от плотности размещения узлов в БСС. Кроме того, также приведён анализ эффективности работы протокола RPL (*Routing Protocol for Low energy and Lossy networks*), который разработан для сетей с низким энергопотреблением и потерями, при разных плотностях узлов БСС.

Описание модели

Для моделирования была разработана имитационная модель в Mathcad, в которой был реализован алгоритма Флойда-Уоршелла [5] для нахождения кратчайших маршрутов между всеми узлами сети. Для имитационного моделирования также были использованы инструменты разработки, поставляемые с ОС Contiki.

Исследуемая имитационная модель в Mathcad строится следующим образом: (I) узлы распределяются случайным образом по некоторой заданной территории; (II) задается радиус связи R, который одинаков для всех узлов сети, а зона связи узла представляет собой круг; (III) каждый из узлов должен иметь возможность функционировать как оконечный и так транзитный узел.

На рис. 1 и рис. 2 приведены соотвественно примеры найденной матрицы длин маршрутов (по расстоянию и по скачкам). В данной статье,

используются два критерия выбора маршрута: по суммарной длине и числу скачков в маршруте.

	1	2	3	4	5	6	7
1	0	$1{\cdot}10^{307}$	28.049	85.64	64.793	76.524	31.38
2	$1{\cdot}10^{307}$	0	$1{\cdot}10^{307}$	$1{\cdot}10^{307}$	68.634	38.557	$1{\cdot}10^{307}$
3	28.049	$1{\cdot}10^{307}$	0	63.678	66.11	104.573	23.612
4	85.64	$1{\cdot}10^{307}$	63.678	0	85.408	162.163	74.092
5	64.793	68.634	66.11	85.408	0	107.191	86.429
6	76.524	38.557	104.573	162.163	107.191	0	107.903
7	31.38	$1{\cdot}10^{307}$	23.612	74.092	86.429	107.903	0
8	39.163	$1{\cdot}10^{307}$	26.616	69.353	92.133	115.686	8.09
9	65.472	$1{\cdot}10^{307}$	93.521	151.112	130.265	58.553	96.852
10	62.474	$1{\cdot}10^{307}$	90.523	148.113	127.267	58.93	88.326
11	90.853	71.73	83.533	112.142	26.734	110.287	107.145
12	61.582	$1{\cdot}10^{307}$	89.098	147.222	126.375	67.856	84.009
13	136.762	117.639	95.464	65.224	66.298	156.196	119.075
14	$1{\cdot}10^{307}$	$1{\cdot}10^{307}$	$1{\cdot}10^{307}$	$1{\cdot}10^{307}$	$1{\cdot}10^{307}$	$1{\cdot}10^{307}$	88.409
15	80.604	$1{\cdot}10^{307}$	108.654	166.244	145.398	157.128	84.206

Рис. 1. Пример найденной матрицы длин маршрутов по расстоянию

	1	2	3	4	5	6	7
1	1	1	2	2	2	2	1
2	1	1	2	2	2	2	1
3	2	2	1	1	1	1	1
4	2	2	1	1	2	2	2
5	2	2	1	2	1	1	1
6	2	2	1	2	1	1	2
7	1	1	1	2	1	2	1
8	$1{\cdot}10^{307}$	$1{\cdot}10^{307}$	2	2	2	2	3
9	2	3	4	2	4	4	3
10	2	2	4	4	4	4	3
11	1	1	1	2	2	2	1
12	2	2	4	2	4	4	3
13	1	2	2	2	3	3	2
14	2	1	2	3	2	3	2
15	3	3	5	5	5	5	4
16	2	1	1	2	1	2	...

Рис. 2. Пример найденной матрицы длин маршрутов по скачкам

Для анализа эффективности работы протокола RPL, мы использовали инструменты разработки, поставляемые с ОС Contiki. Данная операционная система поддерживает современные протоколы связи для маломощных сетей: 6LoWPAN, RPL, CoAP. Contiki является операционной системой с открытым кодом, она предназначена для встраиваемых систем, в частности, для умных устройств (*Smart Objects*). Моделирование производилось с помощью инструмента COOJA (входит в состав ОС *Contiki*). Для построения сети на базе RPL использовалась реализация протокола из ОС Contiki.

Во всех сценариях маршрутизатор располагался в центре сенсорного поля, измерялось количество промежуточных узлов для оценки влияния плотности узлов на распределение длины маршрута в БСС. Сенсорное поле представляет собой квадрат, ширина которого увеличивалась от 100 до 200 м по мере увеличения количества узлов. Результаты моделирования для одной из моделей для протокола RPL показаны на рис. 3, модель содержит 100 узлов, размещенных случайным образом на поле 200 на 200 м.

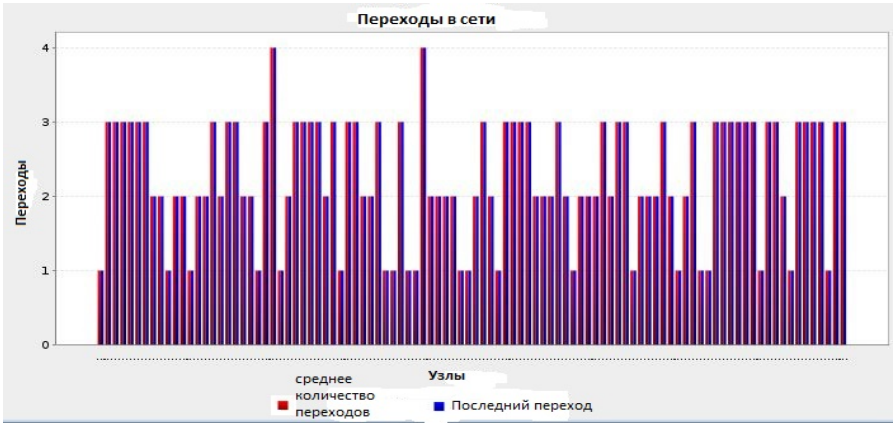


Рис. 3. Зависимости количества скачков от числа узлов в сети

Результаты моделирования

1. Зависимость распределения длины маршрута (по расстоянию и по скачкам) от плотности размещения узлов в БСС с помощью моделирования в Mathcad.

При радиусе связи R = 50 м и поле 200×200 м, получены графики распределения длины маршрута по расстоянию с участием 50 и 100 узлов, соответственно показаны на рис. 4 и рис. 5.

При радиусе связи R = 50 м и поле 200×200 м, получены графики распределения длины маршрута по скачкам с участием 50 и 100 узлов, соответственно показаны на рис. 6 и рис. 7.

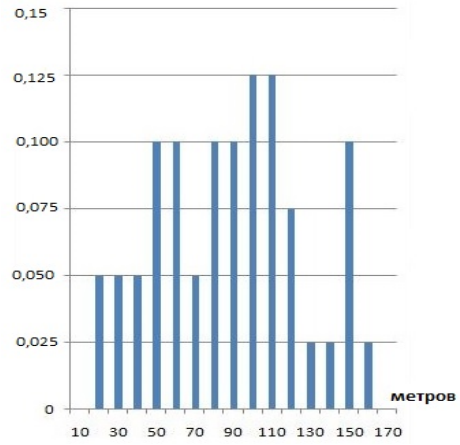


Рис. 4. Распределение длины маршрута по расстоянию с 50 узлами

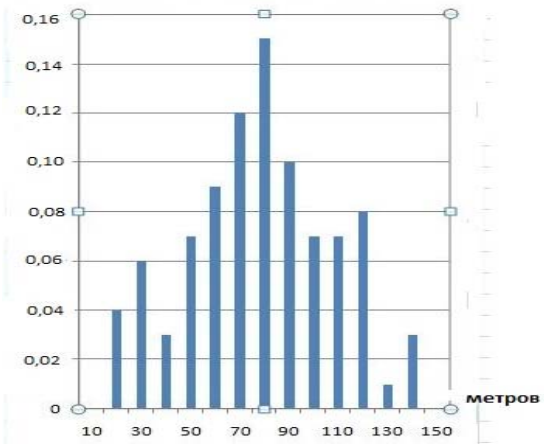


Рис. 5. Распределение длины маршрута по расстоянию с 100 узлами

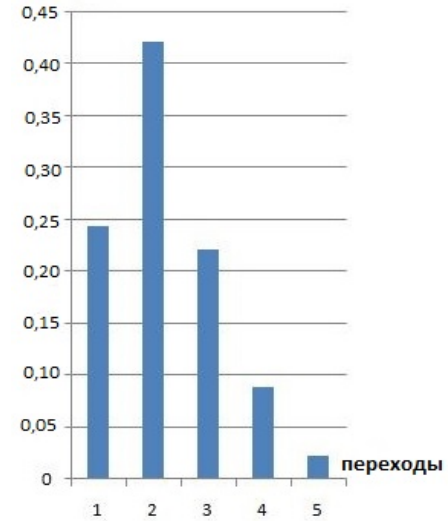


Рис. 6. Распределение длины маршрута по скачкам с 50 узлами

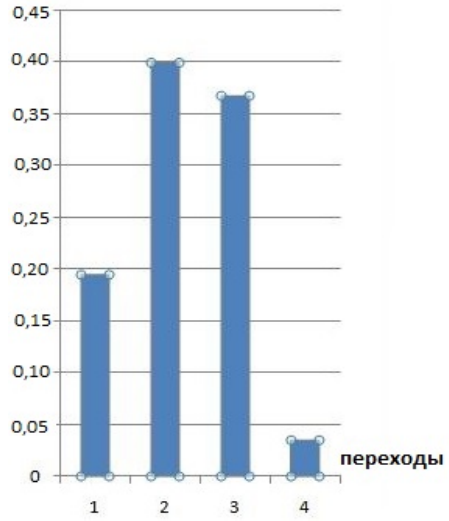


Рис. 7. Распределение длины маршрута по скачкам с 100 узлами

2. Эффективность работы протокола RPL при разных плотностях узлов в БСС с помощью моделирования в ОС Contiki.

На рис. 8 и рис. 9 показаны графики распределения длины маршрута по скачкам с участием 50 и 100 узлов (R = 50 м, поле 200 на 200 м).

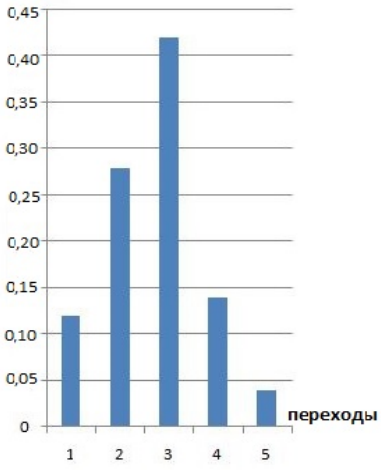


Рис. 8. Распределение длины маршрута по скачкам с 50 узлами

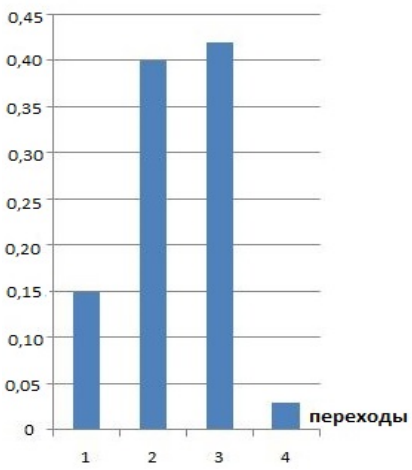


Рис. 9. Распределение длины маршрута по скачкам с 100 узлами

На рис. 10 и рис. 11 показаны графики распределения длины маршрута по скачкам с полями 100 на 100 и 200 на 200 м (R = 30 м с 100 узлами).

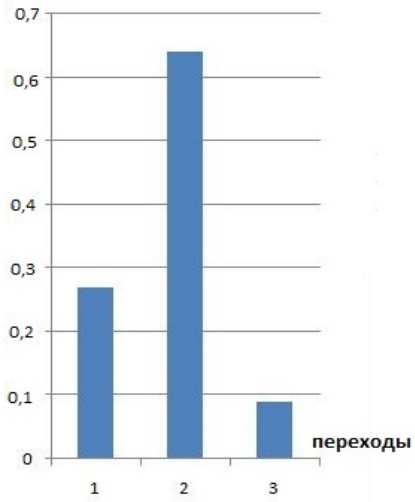


Рис. 10. Распределение длины маршрута по скачкам с площадью 100×100 м

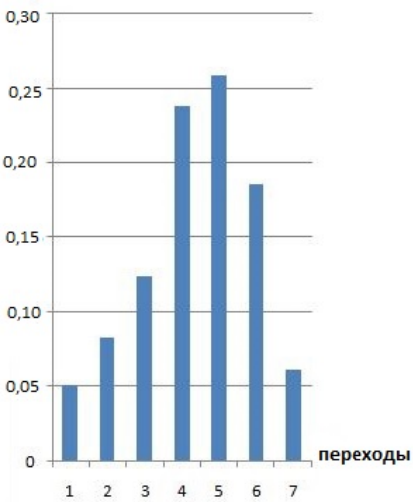


Рис. 11. Распределение длины маршрута по скачкам с площадью 200×200 м

Выводы

1. Структурные параметры БСС сети (число узлов и область размещения узлов) влияют на распределение длины маршрута в БСС сети.

2. С ростом плотности размещения узлов, длины маршрута (по расстоянию и по скачкам) уменьшаются, что приводит к снижению задержки доставки сообщений, т. е. к повышению качества обслуживания трафика в БСС сети.

3. Результаты моделирования для протокола RPL на ОС Contiki схожи с результатами моделирования в Mathcad и показывают, что длина маршрута по скачкам уменьшается с увеличением плотности размещения узлов, что демонстрирует эффективность функционирования протокола RPL.

Список используемых источников

1. Киричек Р. В., Парамонов А. И., Прокопьев А. В., Кучерявый А. Е Эволюция исследований в области беспроводных сенсорных сетей // Информационные технологии и телекоммуникации. 2014. № 4 (8). С. 29–41.

2. 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.

3. Окунева Д. В., Парамонов А. И. Анализ связности ББС при различных распределениях ее узлов // 71-я Всероссийская научно-техническая конференция, посвященная Дню радио Труды конференции. 2016. С. 179–180.

4. Dao N., Koucheryavy A., Paramonov A. Analysis Of Routes In The Network Based On A Swarm Of UAVS // Lecture Notes in Electrical Engineering. 2016. Т. 376. PP. 1261–1271.

5. Кристофидес Н. Теория графов. Алгоритмический подход. М. : Мир,1978. 430 с.

УДК 4.056

РАЗРАБОТКА УСТРОЙСТВА МОДЕЛИРОВАНИЯ КАНАЛА СВЯЗИ СТАНДАРТА GSM НА БАЗЕ ARDUINO И ОДНОПЛАТНОГО КОМПЬЮТЕРА RASPBERRY

А. Ю. Решетов, О. Б. Филиппов, С. И. Штеренберг

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

В статье рассматривается способы представления элементов внедрения стандарта GSM в спроектированный канал связи, построенный на основе микроконтроллеров Arduino и одноплатных компьютеров Raspberry. Целью данной работы является создание модуля для проведения экспериментальных работ по обеспечению безопасности в стандарте GSM.

Arduino, Raspberry, защита информации, GSM, RFID-считыватель.

В начале повествования проекта следует рассказать о стандарте GSM. Данный термин «безопасность» понимается как исключение несанкционированного использования системы и обеспечение секретности переговоров

подвижных абонентов. Определены следующие механизмы безопасности в стандарте GSM:

– аутентификация;
– секретность передачи данных;
– секретность абонента;
– секретность направлений соединения абонентов.

Защита сигналов управления и данных пользователя осуществляется только по радиоканалу. Режимы секретности в стандарте GSM определяются Рекомендациями, приведенными в таблице.

ТАБЛИЦА. Режимы секретности в стандарте GSM

Стандарт	Аспекты секретности	Описание
GSM 02.09	Характеристики безопасности	Определяет характеристики безопасности, применяемые в сетях GSM. Регламентируется их применение в подвижных станциях и сетях
GSM 03.20	Секретность, связанная с функциями сети	Определяет функции сети, необходимые для обеспечения характеристик безопасности, рассматриваемых в рекомендациях GSM 02.09
GSM 03.21	Алгоритмы секретности	Определяет криптографические алгоритмы в системе связи
GSM 02.17	Модули подлинности абонентов (SIM)	Определяет основные характеристики модуля SIM

Основная теория входит в главный модуль общего проекта адаптивных саморазвивающихся систем, описанных в работах [1, 2, 3]. Суть общего проекта, создаваемого на кафедре защищённых систем связи СПбГУТ, шагнула значительно дальше после выполнения научно исследовательской работы на тему «Программно-аппаратный комплекс средств защиты информации на основе самомодифицирующихся приложений SSP_AI (*Stanislaw Shterenberg program – Artificial intelligence*)» [4]. В ней упоминался проект «SSP_AI», а именно – комплекс адаптивных саморазвивающихся систем и программно-аппаратных средств по защите информации. Первоначально, среда «SSP_AI» – это ничто иное как база для расширения различных программных модулей и систем, в своем предназначении, объединяющихся в единую концепцию по развитию средств систем защиты информации (далее – СЗИ), которые нацелены на полное самоуправление и минимизацию задач оператора информационной безопасности. Одна из частей проекта – создание комплекса «dron_SSP». Это ни что иное как примитивный роботизированный комплекс, завязанный на управление центральной адаптивной системой «SSP_AI_1.0» (1.0 – это указание версии программного обеспечения). Сама часть «dron_SSP», как и весь проект «SSP_AI» в настоящей статье рассмотрены не будут.

Основной уклон в статье делается именно на попытке защищенной и ускоренной синхронизации данных различных модулей программно-аппаратной системы по основным каналам связи. За основу практического проектирования (а настоящая статья именно о практической проблематике выполнения проекта) взяты распространенные и наиболее популярные микроконтроллеры Arduino и одноплатные компьютеры Raspberry.

Одноплатный компьютер Raspberry Pi 3 Model B, внедряемый в рамках проекта позволил осуществить базовый опыт по обработке примитивных действий программного комплекса SSP_SMC. Для установки операционной системы Windows 10 IoT Core понадобилось дополнительно приобрести microSD-карту с операционной системой Raspbian (8 ГБ, Класс 10). При этом изначально прошитая операционная система Raspbian была заменена на Windows 10 IoT Core.

Остальные компоненты по второй части проекта при формировании модуля dron_SSP понадобились для составления функциональной части проектирования (летательный аппарат mjx-600h, GSM/GPRS shield, считыватель RFID/RC522). На них проходил тест по передачи данных в исполняемые модули программ, запускаемых на Arduino.

В завершающей стадии проекта, была предложена имитационная модель передачи данных на платформенные приложения (планшеты на Android). Здесь также задействовалась плата Raspberry Pi 3 Model B и монитор DEXP 21.5 «M2171 (IPS, LED, FHD, 1920x1080)». Для управления комплексом применялась Клавиатура Qwerty Pad.

Присоединение самого GSM осуществлялось по схеме, представленной на рис. 1.

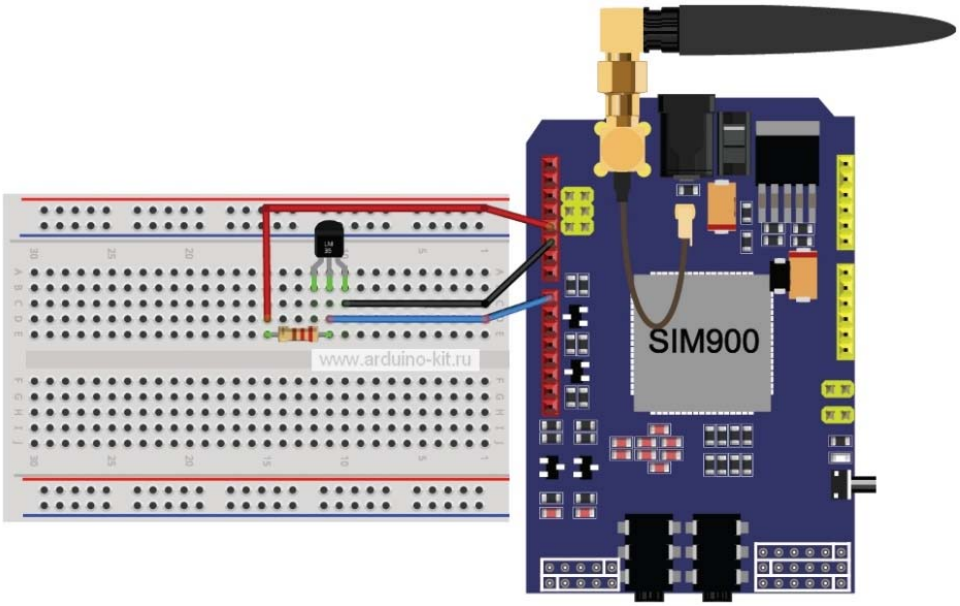


Рис. 1. Схема подключения модуля GSM/GPRS shield и датчика LM335.
Шилд SIM900 установлен на Arduino UNO.

GSM/GPRS shield на базе модуля SIMCom SIM900 выпускают несколько производителей, и платы имеют незначительные отличия. Также на некоторых платах расположены: слот для SIM-карты, стандартные порты 3,5 мм для аудиовхода и выхода и разъём для внешней антенны. На плате GSM/GPRS shild имеется несколько перемычек, позволяющих выбрать тип serial-соединения (*hardware* или *software*). GSM/GPRS shield имеет два способа включения – аппаратный (кратковременное нажатие кнопки PWRKEY) и программный (используется один из выходов *Arduino*) [6].

Защита GSM сетей обеспечивается тремя алгоритмами, использующими алгоритм шифрования RSA: A3 – алгоритм, отвечающий за аутентификацию и предупреждающий клонирование, A5 – алгоритм шифрования голосового трафика, и A8 – алгоритм генерации ключа из результата работы A3 в ключ A5, причем алгоритмы A3 и A8 чаще всего представляют собой обыкновенную хэш-функцию. Алгоритм A5 имеет несколько модификаций – A5/0 (без шифрования), A5/1 (для избранных стран), A5/2 (сильно ослабленная версия, используется в том числе и в России) и A5/3 (разработан с цель заменить A5/1, однако используется только в 3GPP сетях) [5]. Схема аутентификации пользователя и шифрования приведена на рис. 2.

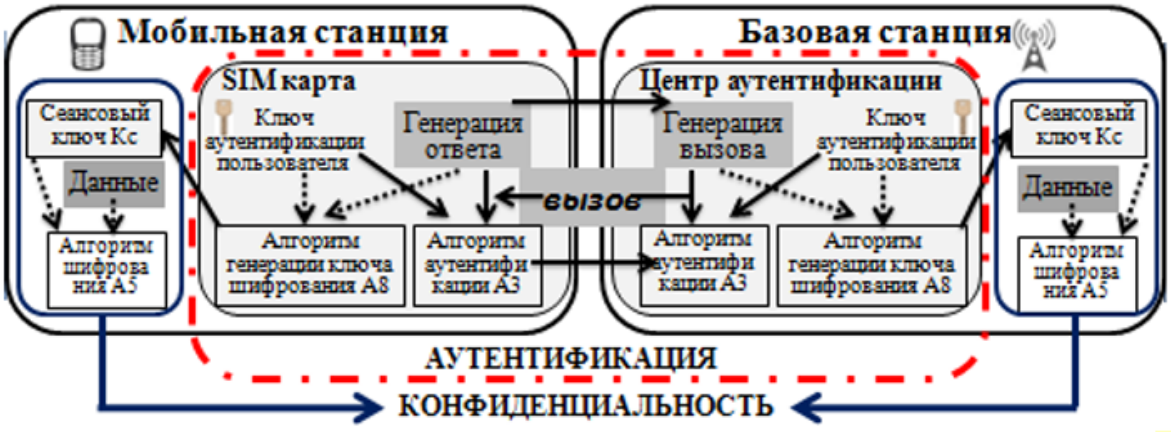


Рис. 2. Схема аутентификации пользователя и шифрования стандарта GSM

Как видно из представленной схемы, мобильные станции (телефоны или планшеты) снабжены смарт-картой, содержащей A3 и A8, а в самом телефоне имеется ASIC-чип с алгоритмом A5. Базовые станции также снабжены ASIC-чипом с A5 и «центром аутентификации», использующим алгоритмы A3 и A8 для идентификации мобильного абонента и генерации сеансового ключа. Данная архитектура при надлежащем исполнении и надежных алгоритмах должна была обеспечить надежную защиту от перехвата [5].

Для добавления функций смарт-карты был реализован в проект считыватель RFID/RC522 (рис. 3).

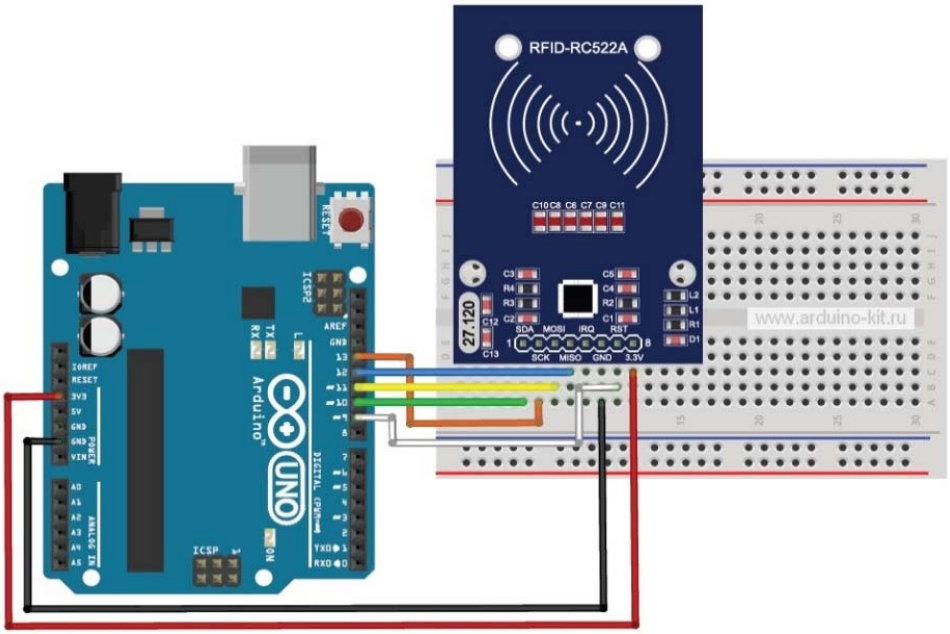


Рис. 3. Схема подключения модуля RFID-считывателя RC522C к Arduino

Идентификация объектов производится по уникальному цифровому коду, который считывается из памяти электронной метки, прикрепляемой к объекту идентификации. Считыватель содержит в своем составе передатчик и антенну, посредством которых излучается электромагнитное поле определенной частоты. Попавшие в зону действия считывающего поля радиочастотные метки «отвечают» собственным сигналом, содержащим информацию. Сигнал улавливается антенной считывателя, информация расшифровывается и передается в компьютер для обработки. Подавляющее большинство современных систем контроля доступа (СКД) использует в качестве средств доступа идентификаторы, работающие на частоте 125 кГц. Это проксимити-карты доступа (только чтение), самыми распространенными являются карты EM-Marin, а также HID, Indala. Карты этого стандарта являются удобным средством для внедрения в наш проект [6].

В конечном итоге, имея сборки модуля GSM/GPRS shield и модуля RFID-считывателя RC522C, а также в основе микрокомпьютер Raspberry Pi 3, возможно воплотить полную схему (рис. 4).

В общем своём смысле данная схема описывает, что общее конфигурирование dron_SSP происходит на компьютере Raspberry (установлена операционная система Windows 10 IoT Core). Благодаря простой прошивке, устанавливаются стандартные требования для модулей GSM/GPRS shield и RFID-считывателя RC522C. После чего пользователь может с планшета или мобильного устройства посылать основные команды на микроконтроллер. Канал связи защищен стандартными способами, описанными ранее и потому добавлен RFID-считыватель, по которому пользователь должен себя идентифицировать.

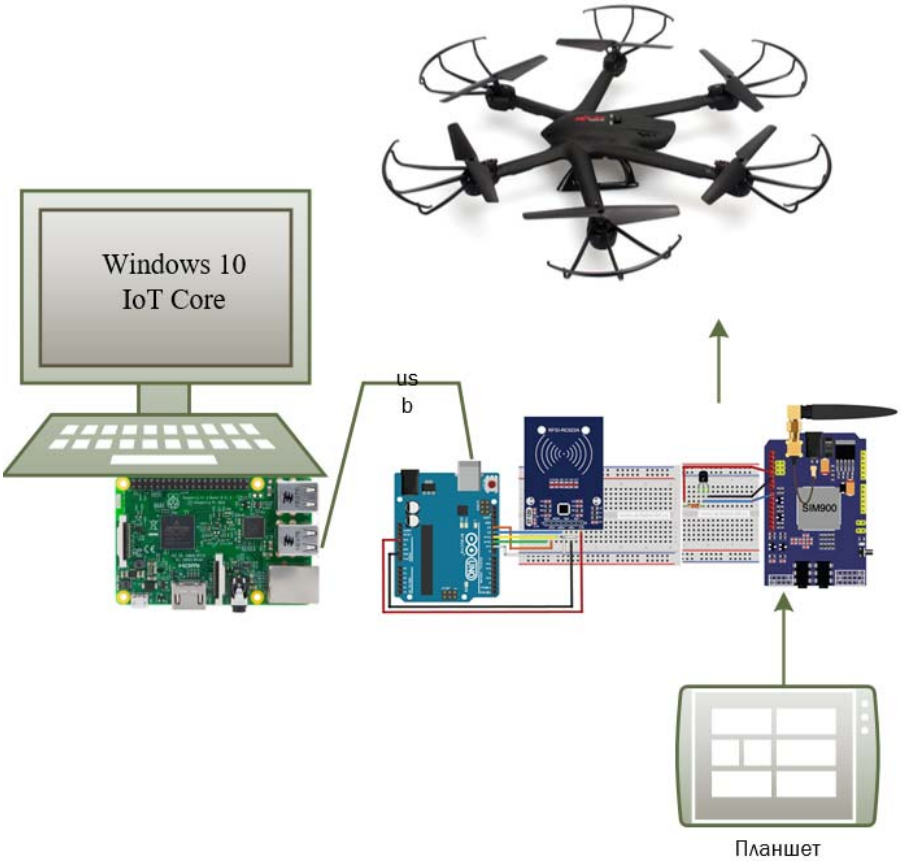


Рис. 4. Общая схема примитивной стадии развитии проекта dron_SSP

В качестве проверки сигнала добавлен летательный аппарат, на котором есть системы GSM/GPRS. Оператор минимизирует затраты на приобретение радиоуправляемых деталей, а также исключает риск перехвата летательного аппарата по средствам радио-подавления сигнала. Все управление сосредотачивается на планшете пользователя, и он может спокойно, не опасаясь разного рода перехвата совершать маневры летательного дрона.

Список используемых источников

1. Штеренберг С. И. Методика применения в адаптивно системе локальных вычислительных сетей стеговложения в исполнимые файлы на основе самомодифицирующегося кода // Системы управления и информационные технологии. 2016. Т. 63. № 1. С. 51–54.

2. Андрианов В. И., Романов Г. Г., Штеренберг С. И. Экспертные системы в области информационной безопасности // Актуальные проблемы инфотелекоммуникаций в науке и образовании. IV Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 2 томах. 2015. С. 193–197.

3. Штеренберг С. И. Общее представление проекта адаптивной интеллектуальной системы A_RPA. // Наукоемкие технологии в космических исследованиях Земли. 2015. Т. 7. № 5. С. 50–57.

4. Штеренберг С. И. Программно-аппаратный комплекс средств защиты информации на основе самомодифицирующихся приложений SSP_AI (Stanislaw Shterenberg program – Artificial intelligence): отчёт о НИР/ Сборник трудов «Двадцать первая Санкт-Петербургская ассамблея молодых ученых и специалистов». СПб. 2016. 190 с.

5. Михайлова А. Ю., Борисов А. П. Разработка устройства моделирования канала связи стандарта GSM для обучения студентов направления 10.03.01 «Информационная безопасность»: материалы XII Всероссийской научно-технической конференции студентов, аспирантов и молодых ученых «Наука и молодежь». Горизонты образования выпуск № 17 2015. С. 15.

6. Уроки и проекты Arduino [Электронный ресурс]. URL: http://arduino-kit.ru/textpage_ws/pages_ws/uroki-i-proektyi-arduino (дата обращения 04.02.2017).

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

УДК 004.056.53

ВЫЯВЛЕНИЕ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ

И. Е. Пестов, Д. В. Сахаров, И. Ю. Сергеева, И. С. Чернобородов

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

На протяжении всей истории развития компьютерной техники актуальной проблемой всегда оставалась безопасность информационных систем и хранилищ данных. Существуют различные методы и подходы к оценке угроз информационных систем, но не всегда можно четко определить, какие нужно использовать, так как не существует одного метода, который бы подходил ко всем информационным системам. В работе исследуются различные подходы к оценке угроз информационных систем, проводится сравнение методов и описание их применения.

информационная безопасность, пентест, анализ, угрозы, информационные системы.

В настоящий момент, для выявления угроз информационной системы используется два подхода. Первый подход – это аудит информационной системы. Аудит – независимая оценка текущего состояния системы информационной безопасности, устанавливающая уровень ее соответствия определенным критериям, и предоставление результатов в виде рекомендаций [1]. Аудит позволяет получить наиболее полную и объективную оценку защищенности информационной системы, локализовать имеющиеся проблемы и разработать эффективную программу построения системы обеспечения информационной безопасности организации.

Можно выделить следующие основные виды аудита информационной системы: экспертный аудит безопасности, в ходе которого выявляются недостатки в системе мер защиты информации на основе опыта экспертов, участвующих в процедуре обследования; оценка соответствия рекомендациям международного стандарта ISO 17799, а также требованиям руководящих документов ФСТЭК (Гостехкомиссии); инструментальный анализ защищенности информационной системы, направленный на выявление и устранение уязвимостей программно-аппаратного обеспечения системы; комплексный аудит, включающий в себя все вышеперечисленные формы проведения обследования [2].

Первым и самым важным шагом в любом аудите является определение типа информационной системы. Информационные системы классифицируются по различным признакам, но есть два основополагающих: значимость обрабатываемой информации и масштаб информационной системы [3]. После определения типа информационной системы определяется класс защищенности, который зависит от уровня значимости информации и степени возможного ущерба, который может возникнуть при утечке информации. Следующим шагом будет определение структурно-функциональных характеристик информационной системы [4].

Результатом проведения аудита всегда должно быть формирование модели угроз. Модель угроз содержит в себе следующие пункты: описание информационной системы и ее структурно-функциональных характеристик, возможности нарушителей (модель нарушителя), возможные уязвимости информационной системы, способы реализации угроз, последствия от нарушения безопасности [5].

Пентест – это тест на проникновение в сеть или информационную систему. Во время подобного теста специалист-тестировщик устраивает псевдоатаку на информационную систему или сеть, инсценируя действия реальных злоумышленников или атаку, проводимую каким-то вредоносным программным обеспечением без непосредственного участия самого взломщика. Целью данных тестов является, конечно же, в первую очередь, выявление слабых мест в защите информационной системы и выявление угроз, с последующим их описанием.

Существует два типа тестов: тестирование «чёрного ящика» и тестирование «белого ящика». В первом случае, специалисты, проводящие тестирование, не имеют в своем распоряжении информации о внутреннем устройстве защиты и даже об инфраструктуре информационной системы или сеты. Во втором случае, напротив, им доступна практически вся подобная информация.

Данные, полученные при пентесте, можно интерпретировать в контексте любого другого высокоуровневого документа, содержащего технические критерии и рекомендации к системе управления информационной безопасности [6].

В качестве итогов следует сформулировать следующее: аудит начинается с анализа рисков и угроз информационной безопасности. Он призван выявлять наиболее опасные угрозы с точки зрения системы защиты. Аудит должен дать вразумительный ответ на вопрос «если где-нибудь взломают защиту, то насколько предприятие подвержено риску после эксплуатации уязвимостей?» [7]. Аудит – это более комплексный и документированный метод выявления угроз, по сравнению с пентестом этот метод используется гораздо чаще.

Тесты на проникновение можно считать менее комплексным методом поиска уязвимостей чем аудит, но более эффективным за счет того, что специалист может выстроить модель злоумышленника и провести независимое исследование информационной системы. Задача специалиста – ответить на вопросы «как проще всего попасть вовнутрь системы, нарушить работоспособность или что-нибудь получить?» и «какова минимальная цена эксплуатации уязвимости?».

Список используемых источников

1. Аудит информационной безопасности. Анализ защищенности систем и приложений [Электронный ресурс] // Pentestit [сайт]. Режим доступа: https://www.pentestit.ru/audit/ (дата обращения 25.03.2017).

2. Аудит информационной безопасности – основа эффективной защиты предприятия [Электронный ресурс] // Dialognauka [сайт]. Режим доступа: http://dialognauka.ru/press-center/article/4753/ (дата обращения 25.03.2017).

3. Бухарин В. В., Липатникова В. А., Сахаров Д. В. Метод управления информационной безопасностью организации на основе процессного подхода // Информационные системы и технологии. 2013. № 3 (77). С. 102–109.

4. Андрианов В. И., Красов А. В., Липатников В. А. Инновационное 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». СПб., 2012. 396 с.

5. Методика определения угроз безопасности информаци в информационных системах [Электронный ресурс] // fstec [сайт]. Режим доступа: http://fstec.ru/component/attachments/download/812 (дата обращения 25.03.2017).

6. Правила пентеста: аудит по стандарту PCI DSS [Электронный ресурс] // Хакер [сайт]. Режим доступа: https://xakep.ru/2009/09/22/49549/ (дата обращения 25.03.2017).

7. Пентест или аудит? [Электронный ресурс] // SecurityLab [сайт]. Режим доступа: http://www.securitylab.ru/blog/company/nosecure-info/9185.php (дата обращения 25.03.2017).

УДК 004.056

АНАЛИЗ УЯЗВИМОСТЕЙ ПРОЦЕССОВ ОБРАБОТКИ ИНФОРМАЦИИ В ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

Д. В. Сахаров, И. Ю. Сергеева, Т. Р. Терегулов

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

Произведен обзор потенциальных уязвимостей, влияющих на процессы обработки информации в государственных информационных системах. Идентифицированы уязвимости, произведена оценка уровня вероятности реализации угрозы с использованием соответствующей уязвимости. Также представлена классификация уязвимостей. Описана частная модель угроз, в которой отражены возможные последствия реализации угрозы.

уязвимости, угрозы информационной безопасности, анализ рисков, модель угроз, государственные информационные системы.

Введение

На сегодняшний день не существует полностью защищенных информационных систем. В любой информационной системе можно найти уязвимости, они могут быть связаны с ошибкой программирования, неправильной конфигурацией средств защиты, отсутствие установленных модулей обновления и т. д.

В большинстве случаев уязвимости ликвидируются уже после обнаружения факта их использования. К тому моменту как та или иная уязвимость ликвидирована, ущерб, порождённый ею, часто уже является значительным. Связано это с экономической нецелесообразности ликвидации уязвимости, которая не может привести к значительному ущербу. Показателем того как много критичных уязвимостей можно считать обилие обновлений и исправлений разработчиками программного обеспечения.

Так как государственные информационные системы создаются в целях реализации полномочий государственных органов и обеспечения информации между этими органами, а также в иных установленных федеральными законами целях, то приоритетным направлением обеспечения безопасности будет обеспечение конфиденциальности и целостности информации. В связи с этим уязвимости, которые могут повлечь за собой нарушение конфиденциальности и целостности информации являются самыми серьёзными.

Понятие уязвимости

Под уязвимостью информационной системы понимают недостаток (слабость) программного (программно-технического) средства или информационной системы в целом, который (которая) может быть использована для реализации угроз безопасности информации [1].

Эти слабости могут быть использованы одной или несколькими угрозами, являющимися причиной нежелательных инцидентов. Уязвимость сама по себе не наносит ущерба, это только условие или набор условий, позволяющих угрозе причинить ущерб активам [2].

Получается создать систему, не содержащую уязвимостей, объективно невозможно. Это связано с тем, что на практике устранение одной уязвимости порождает другую уязвимость.

Угрозы и уязвимости должны объединиться для того, чтобы стать причиной инцидентов, которые могут причинить ущерб активам. Поэтому необходимо четко определять взаимосвязь между угрозами и уязвимостями.

В структуре информационной системы, основным элементом обработки информации является программное обеспечение (системное, прикладное). В связи с этим мы рассмотрим уязвимости программного обеспечения. Для более подробного анализа уязвимостей требуется их классификация.

Классификация уязвимостей программного обеспечения.

1) По типу ПО:

– системное ПО;

– Прикладное программное обеспечение.

2) По этапу жизненного цикла программного обеспечения, на котором возникает уязвимость:

– уязвимости, возникающие на этапе проектирования программного обеспечения;

– реализации программного обеспечения;

– инсталляции и настройки программного обеспечения.

3) По причине возникновения уязвимости:

– недостатки механизмов аутентификации;

– недостатки защиты учетных записей;

– наличие функций, позволяющих выполнять деструктивные действия;

– отсутствие проверки корректности входных данных.

4) По характеру последствий от реализации атак:

– уязвимости, используемые для переполнения буфера;

– уязвимости, используемые для подбора пароля или идентификатора;

– уязвимости, используемые для изменения прав доступа;

– уязвимости, используемые для реализации атаки «Отказ в обслуживании».

Понятие угрозы

Угроза – это возможная опасность (потенциальная или реально существующая) совершения какого-либо деяния (действия или бездействия), направленного против объекта защиты (информационных ресурсов), наносящего ущерб собственнику, владельцу или пользователю, проявляющегося в опасности нарушения конфиденциальности, целостности и(или) доступности информации.

Если про угрозы можно сказать, какая из них направлена на какое свойство информации – доступность, конфиденциальность или целостность, то одна уязвимость может привести к множеству угроз безопасности, неоднородных по направленности [3].

Очевидно, что так же дело обстоит и с ущербом: одна уязвимость может привести к различным степеням ущерба для системы в зависимости от её реализации.

Напомним, что угроза безопасности может быть реализована не только злонамеренно. Непреднамеренная реализация угроз составляет значительную часть общего числа реализованных угроз [4].

Кроме искусственных угроз, существуют еще и естественные, которые, по большому счету, тоже являются последствиями уязвимостей.

Таким образом, можно подтвердить вывод, что любая угроза безопасности информации реализуется путем эксплуатации конкретной уязвимости информационной системы [5].

Вероятность реализации угрозы Р – это возможность осуществления угрозы по отношению к любой системе, процессу или ресурсу.

Вероятность реализации угрозы можно рассматривать как функцию трех переменных: вероятности существования угрозы безопасности ($Р_у$), вероятности существования уязвимости (незащищенность) системы безопасности ($Р_{нз}$) и вероятности наличия потенциальных сил по этой угрозе для воздействия на систему безопасности ($Р_с$). Тогда вероятность реализации угрозы можно рассчитать:

$$Р = Ру * Рнз * Рс.$$

Если любая из этих переменных приближается к нулю, то и вероятность реализации угрозы будет также стремиться к минимуму. Уровень вероятности реализации угрозы можно оценивать по качественному и количественному методу.

Выводы

Как видим, уязвимости – постоянные атрибуты любой информационной системы, не существует информационных систем, не содержащих уязвимости, существуют только защищенные – по отношению, к которым вероятность возникновения актуальных угроз безопасности информации является приемлемой.

При этом, любая угроза безопасности информации реализуется путем эксплуатации конкретной уязвимости информационной системы.

В данной статье описана классификации уязвимостей программного обеспечения, сформирована частная модель угроз.

Список используемых источников

1. ГОСТ Р 56546-2015 Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем.

2. Астахов А. М. Искусство управления информационными рисками. М.: ДМК Пресс, 2010. 312 с.

3. Андрианов В. И., Красов А. В., Липатников В. А. Инновационное управление риска-ми 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». СПб., 2012. 396 с.

4. ГОСТ Р ИСО 17776-2010 Руководящие указания по выбору методов и средств идентификации опасностей и оценки риска.

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.

УДК № 004.056.55:003.26

УНИВЕРСАЛЬНЫЙ МЕТОД ЗАЩИТЫ БЛОКОВЫХ ШИФРОВ ОТ ПОБОЧНЫХ АТАК ПО ЦЕПЯМ ПИТАНИЯ

С. В. Тихонов

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

Предлагается новый метод защиты аппаратно-реализованных блоковых шифров от побочных атак по цепям питания разностного типа (DPA). Алгоритм шифра дополняется двумя защищёнными преобразованиями: перед шифрованием и после него.

За счёт простоты преобразований, обеспечивается высокая скорость работы при минимальных требованиях к дополнительным аппаратным ресурсам. При этом метод является универсальным и применим к защите любых блоковых шифров.

секретный ключ, аппаратная реализация шифра, S-box, атака по цепи питания, разностный анализ мощности (DPA).

Предлагается (рис., *а*) перед операцией шифрования $E(\cdot)$, реализуемой на чипе обычным незащищённым способом, производить защищённую от DPA предобработку $P(\cdot)$ шифруемого сообщения $m(i)$ с использованием дополнительного (достаточно длинного) секретного ключа k_{ADD}, и такую же операцию производить с полученной криптограммой (для предотвращения возможности проведения атаки DPA начиная с последнего раунда).

Преобразования предобработки и постобработки, должны обладать следующими тремя свойствами:

1) защищённость от DPA;

2) отсутствие возможности за разумное время произвести расчёт каких-либо бит комбинаций $m'(i)$ и $e'(i)$ только по известным комбинациям $m(i)$ и $e''(i)$;

3) однозначность и обратимость преобразований.

При соблюдении этих условий, злоумышленник окажется не в состоянии за реализуемое время найти биты входа или выхода защищаемого шифра. Следовательно, пропадает возможность произвести расчёт результата выполнения любых промежуточных операций защищаемого шифра, путём перебора небольших частей его ключа. Поэтому успешная реализация атаки DPA к такой системе окажется невозможной.

В качестве операций, составляющих узлы предобработки и постобработки, могут быть выбраны различные защищённые от DPA преобразования, достаточно просто реализуемые на конкретном чипе. Наиболее перспективной структурой представляется следующий алгоритм:

1) разбивка входа узла предобработки $m(i)$ на подблоки $m_l(i)$;

2) многократная итерация операции сложения по mod2 каждого подблока $m_l(i)$ с соответствующим подблоком дополнительного ключа k_{ADD} и табличного нелинейного преобразования (рис., *б*);

3) склеивание подблоков, для последующей подачи полученной комбинации на вход шифра.

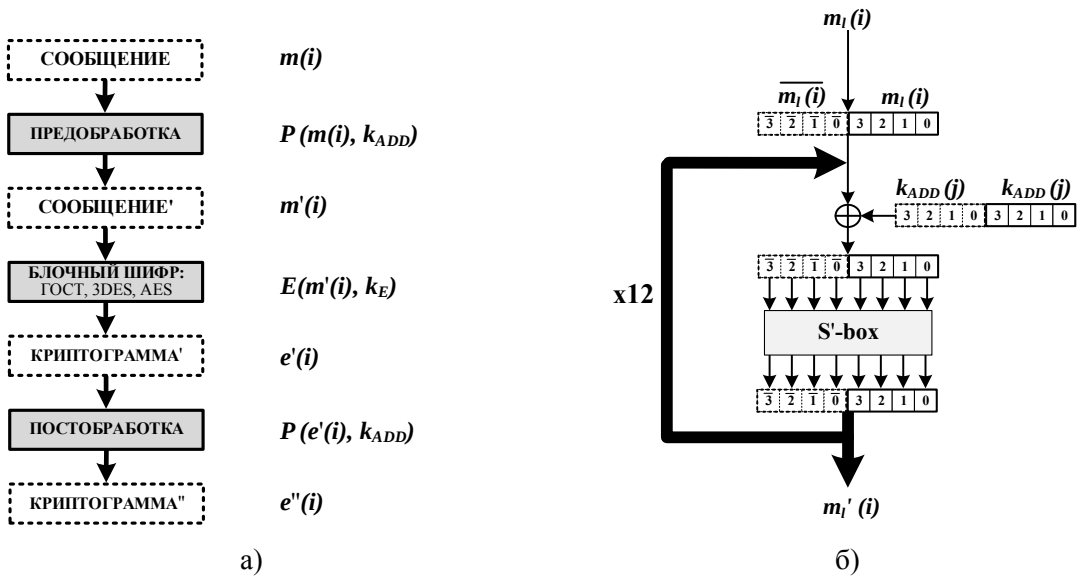


Рисунок. Блок-схема предлагаемого метода защиты от DPA: а) общая структура; б) предлагаемая структура преобразований предобработки/постобработки

В статье [1] недавно был предложен весьма перспективный метод защиты от DPA операций сложения по mod2 и табличного нелинейного преобразования, названный *программной балансировкой*. Идея метода основывается на особенности работы многоразрядных (например, 8-ми, 16-ти рядных) чипов, которая заключается в том, что при выполнении операций над комбинациями, длина которых соответствует разрядности чипа, все их биты обрабатываются параллельно (одновременно). Поэтому, возможно определить энергопотребление, затрачиваемое чипом лишь на обработку комбинации в целом, а не отдельных её разрядов. Отсюда, предлагается такая модификация реализации операций сложения по mod2 и табличного преобразования, чтобы комбинации, обрабатываемые на каждом такте работы чипа, состояли из одинакового количества нулей и единиц (т. е. имели одинаковый вес Хэмминга). Это достигается за счёт одновременной о бработки вместе с «полезной» (информационной) комбинацией, комбинации инвертированной к ней (балансирующей). Отсюда при любом значении информационных бит, балансирующие биты будут уравновешивать вес Хэмминга обрабатываемой комбинации, поддерживая таким образом энергопотребление чипа на постоянном уровне.

При реализации метода защиты на 8-ми разрядном чипе предполагается разбивать блоки $m(i)$ и $e'(i)$ на 4-х битовые подблоки $m_l(i)$ и $e_l'(i)$, каждый из которых после балансировки будет иметь длину в 8 бит. Над каждым таким подблоком совершается 12 итераций преобразований с дополнительным ключом. При этом ключ k_{ADD}, длиной 48 бит необходимо разбить на 12 равных 4-х битовых частей $k_{ADD}(j)$, где $j = 1, ..., 12$ – на каждой итерации

в рамках преобразования одного подблока $m_l(i)$ необходимо использовать отдельный подблок ключа $k_{ADD}(j)$. При этом обработку разных подблоков $m_l(i)$ и $e_l'(i)$ допустимо производить с использованием одного и того же ключа k_{ADD}. В качестве нелинейного преобразования допустимо использовать операцию нахождения обратного элемента в конечном поле.

Реализация криптографических атак на узлы предобработки/постобработки будет невозможной ввиду того, что злоумышленнику оказываются неизвестны комбинации $m'(i)$ и $e'(i)$. Реализация атак DPA с использованием этих комбинаций принципиально окажется возможной, но в процессе этого потребуется перебрать 2^{48} вариантов ключа, что на практике можно считать невыполнимой задачей.

Важно отметить очевидную особенность описанного подхода, заключающуюся в том, что структура алгоритма защищаемого шифра не имеет никакого значения – это может быть любой блоковый шифр. А так как преобразования предобработки и постобработки не затрагивают алгоритм защищаемого шифра, то его устойчивость любым другим атакам, оказывается не ниже чем у стандартного алгоритма.

Предложенный метод защиты был реализован автором для защиты шифра «Кузнечик» на 8-ми разрядном микроконтроллере PIC, при этом скорость шифрования снизилась всего в полтора раза по сравнению с незащищённой реализацией, также потребовался на 20 % больший объём памяти программ (для хранения дополнительного кода программы, реализующего преобразования предобработки и постобработки), а также 256 байт памяти EEPROM для хранения дополнительного ключа, и таблицы нелинейного преобразования. В целом требования предлагаемого метода защиты к дополнительным аппаратным ресурсам чипа можно считать весьма небольшими по сравнению с известными аналогами (например, методом маскировки).

Список используемых источников

1. Arora A., Ambrose J. A., Peddersen J., Parameswaran S. A double-width algorithmic balancing to prevent power analysis Side Channel Attacks in AES // IEEE Computer Society Annual Symposium on VLSI. 2013. PP. 76–83.

УДК 654.9, 681.5

ИМИТАЦИОННАЯ МОДЕЛЬ СИСТЕМЫ DPI НА ОСНОВЕ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ OMNET++

В. В. Фицов

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

В данной статье рассмотрены вопросы разработки и использования имитационной модели системы DPI. В качестве среды моделирования применяется ПО Omnet++. При построении имитационной модели учитывается общая архитектура системы DPI. Приведены алгоритмы модели.

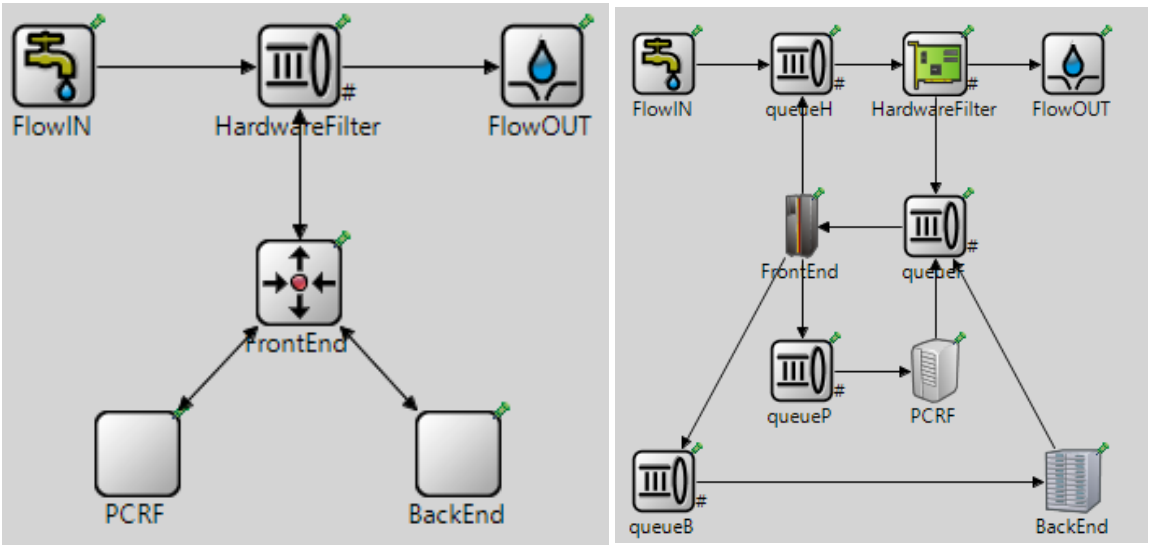
DPI, QoS, Omnet++, система массового обслуживания (СМО), сигнатура.

Введение

Система DPI (*Deep Packet Inspection*, глубокого анализа пакетов) распознает приложения по потоку пакетов, а затем, при необходимости, блокирует или ограничивает для них скорость передачи в соответствии с индивидуальными политиками (тарифными планами). При этом ведется всеобъемлющая статистика по передаваемому трафику. DPI используется на сетях ТрансТелеКом, Ростелеком, Мегафон, МТС, Билайн, Yota, МГТС [1]. Полноценная система DPI достаточно дорогостоящее удовольствие, и кроме того ее стоимость пропорционально возрастает числу необходимых каналов [2]. Применение имитационной модели сетевой конфигурации DPI системы позволит определить аппаратные характеристики системы соответствующие пользовательской нагрузке. А также разработать методику распределения аппаратных ресурсов в режиме реального времени.

DPI – сеть массового обслуживания (СеМО)

Имитационная модель (ИМ) должна отражать архитектуру системы DPI. Ранее в [1] была определена и использована архитектура функциональной модели DPI в построении ИМ GPSS, а теперь и Omnet++. Архитектура состоит из нескольких серверов (систем массового обслуживания, СМО), которые в свою очередь создают СеМО. К ним относятся аппаратный фильтр (*Hardware* Filter, HF) совместно с Bypass как СМО1, Front-End (FE), PCRF (Policy and Charging Rules Function) и Back-End (BE) (рис. 1).



a) b)

Рис. 1. Визуализация ИМ DPI в Omnet++: a) без очередей b) с очередями

HF применяет политики (блокировка, ограничение, пропуск) и ведет статистику. FE проводит глубокий анализ пакетов потоков трафика. PCRF принимает решения о применении политики и возвращает ее номер. BE хранит методы исполнения политики, статистику и сигнатуры. Одним из режимов работы DPI, является анализ трафика, после его прохождения, что позволяет снизить возникающую на DPI задержку. После определения приложения от которого поступает трафик, применяются соответствующие политики. Таким образом с момента пропуска трафика до момента применения политик возникает задержка (*Тзп*) (см. рис.3.b ниже).

Пакет имитационного моделирования Omnet++

При расчете параметров инфокоммуникационных систем и сетей успешно применяются методы программного моделирования (ПО network simulator-2 (ns-2), ns-3, OpNet simulator, AnyLogic, GPSS World, Scilab, CPN Tools [3], Omnet++). После построения ИМ в GPSS, был использован Omnet++.

Как и GPSS, Omnet++ использует дискретно-событийный подход и набор законов распределения для определения и обработки трафика [4]. Свободное программное обеспечение Omnet++ используется для моделирования проводных и беспроводных сетей и их протоколов, сетей с очередями, аппаратного распределения ресурсов (в т. ч. многопроцессорных систем), проверки аппаратной архитектуры, оценки производительности ПО [4]. Omnet++ ориентирован на моделирование с применением очередей и событий, применяет конечные автоматы, имеет методы инкапсуляции и поддерживает сетевые протоколы. Является иерархическим, модульным

и обьектно-ориентированным. Полностью основан на языке C++, с интегрированной средой разработки. В отличие от GPSS и других пакетов моделирования, Omnet++ имеет свой графический интерфейс разработки и выполнения моделирования. Для Omnet++ существуют крупные пакеты, расширяющие возможности моделирования. The INET Framework позволяет применять сетевые протоколы Ethernet, IP, UDP, TCP, SCTP, HTTP, MPLS, OSPF, WiFi, и пр. OverSim – уровни приложений (P2P, overlay protocols). Castalia – сети с низким электропотреблением (Sensor net, BAN, и пр.). MiXiM – нижние уровни и сети (MAC, PHY, Sensor net, BAN, Ad-hoc net, VANET) [5].

Имитационная модель

При построении ИМ в Omnet++ используются несколько типов файлов. Описание структуры сети содержится в *.ned, алгоритмы работы модулей в стандартных файлах языка C++ *.cc и *.h, параметры запуска симуляции в файле *.ini. Результаты представлены как скалярные (*.sca) и векторные (*.vec) величины [6], графики и диаграммы (*.anf) и диаграмма переходов сообщения (*.elog).

В файле инициализации *.ini указываются время моделирования (реальное и в симуляции), а также набор различных параметров запуска. Число заявок, законы распределения поступления и обработки заявок.

Например, законы распределения сообщений при генерации и обработке. Omnet++ содержит 20 распределений [4]: Равномерное, Дискретное равномерное, Бета (I), Гамма (III), Эрланга, Хи-квадрат, Экспоненциальное (X), Пуассоновское, Нормальное (Гаусса (XI)), Логнормальное, Усеченное нормальное, Парето, Вейбулловское, Биномиальное, Паскаля, Геометрическое, Треугольное, Бернулли, Коши, Студента T. По сравнению с GPSS Word, где имеется 25 распределений, отсутствуют: Пирсона VI, Лаплассово, Логлаплассово, Обратное гаусса, Обратное Вейбулловское, Логистическое, Логлогистическое и Extreme A,B. Принято считать, что трафик пакетных сетей лучше других описывают распределения: Логнормальное, Парето, Вейбулловское, Гамма, Гиперэкспоненциальное 2го порядка и пр. [7].

Для описания взаимосвязи объектов симуляции применяется файл *.ned, в котором указывается расположение СМО, соединения, задержки в канале и статистические параметры (рис. 1). Например, для PCRF указывается вход fromFE, куда поступают запросы FE, и выход toFE, по которому отправляются ответы. Так же указаны данные по очередям.

В разработанной модели DPI для каждой СМО, а также для генератора и терминатора сообщений использовался отдельный файл на языке C++. Например, основные функции PCRF описываются 25 строчками кода, что в 2,5 раза больше чем в GPSS. Алгоритм работы ИМ DPI, разработанный

и описанный в [1] для GPSS, использовался в Omnet++ (рис.2). На языке C++ с применением библиотек Omnet++ был разработан обмен различными сообщениями, потеря сообщений и повторная передача.

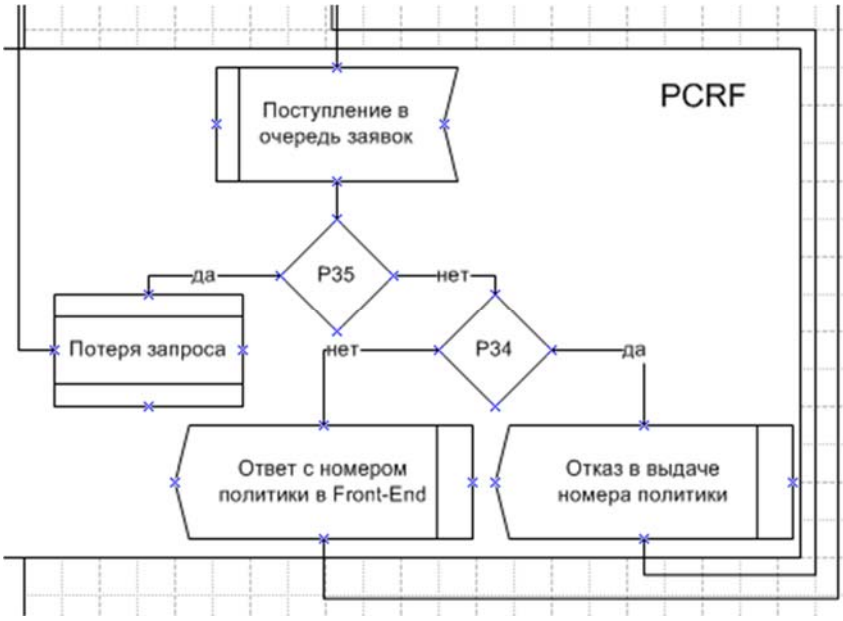


Рис. 2. Фрагмент алгоритма DPI для сервера PCRF

FE может запросить номер политики у PCRF, тогда запрос поступает в очередь и обрабатывается. В ИМ заданы вероятности результатов обработки заявки: P35 вероятность потери запроса в канале, а P34 вероятность отказа в выдаче номера политики. В последнем случае FE дает указания на HF по-умолчанию.

По результатам моделирования в файлы *.sca и *.vec записываются значения переменных, а для векторных переменных число отсчетов, средние значение, стандартное отклонение и вариация. По таким переменным в Omnet++ строится диаграмма (рис. 3*a*) или график в *.anf. Так же строится диаграмма переходов сообщения по СМО в течении моделирования *.elog (рис. 3*b*).

В результате работы ИМ можно получить число заявок и данные по очередям. Число входящих и обработанных системой заявок, запросов к каждой из СМО, ответов, отказов, потерянных сообщений и повторных передач между СМО (рис. 3*a*). Средние значения времени поступления заявки, общего времени в очереди (ожидание, обработка), общего числа заявок в очереди (без ожидания, с ожиданием).

ИМ позволит подтвердить интенсивность возрастания *Тзп* в результате увеличения плотности поступления заявок в СеМО, а также оценить влияние скорости обработки заявок на серверах DPI. Результаты имитации могут

быть использованы для эффективного распределения аппаратных ресурсов между серверами системы DPI, в том числе в режиме реального времени.

a) b)

Рис. 3. Визуализация результатов в Omnet++: a) диаграмма числа заявок в PCRF; b) диаграмма переходов

Список используемых источников

1. 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 : сб. науч. ст. 2016. С. 539–545.

2. Фицов В. В. О внедрении DPI // Вестник связи. 2016. № 11. С. 25–28.

3. Королькова А. В., Кулябов Д. С. Моделирование информационных процессов : учеб. пос. РУДН. М., 2014. 191 с. ISBN 978-5-209-05772-7.

4. Varga A. OMNeT++ Simulation Manual Version 5.0 [Электронный ресурс] // Copyright OpenSim Ltd., 2016. PP. 160-161. URL: https://omnetpp.org/doc/omnetpp/InstallGuide.pdf (дата обращения 30.03.2017).

5. Wehrle K., Gunes M., Gross J. Modeling and Tools for Network Simulation // Springer Science & Business Media, 2010. PP. 37–38.

6. Foreest N. Simulation Queuing Networks with OMNet++, in Tutorial of OMNet++ Simulator. Department of Telecommunications. Budapest University of Technology and Economics, 2003, 9 p.

7. Ложковский А. Г., Каптур В. А., Вербанов О. В. Математическая модель пакетного трафика // Вестник национального политехнического университета «ХПИ». 2011. № 9. С. 113–119.

Статья представлена заведующим кафедрой, доктором технических наук, профессором Б. С. Гольдштейном.

УДК 621.391.63

НЕЛИНЕЙНАЯ ОБРАБОТКА ОПТИЧЕСКОГО СИГНАЛА В ВОЛОКОННО-ОПТИЧЕСКИХ ЛИНЕЙНЫХ ТРАКТАХ

С. В. Чистяков, А. В. Яковлев

Академия Федеральной службы охраны Российской Федерации

Высокая скорость и дальность передачи в современных волоконно-оптических системах передачи вызывают различные искажения оптического сигнала, снижающие качество передачи информации. В статье рассматривается математическая модель корректора на основе нелинейной формирующей системы и предлагается методика оптимизации ее коэффициентов.

волоконно-оптические системы передачи, цифровая обработка сигналов, нелинейная коррекция.

Эффективное управление государством невозможно без отлаженной системы управления, базирующейся на современной телекоммуникационной инфраструктуре. Потребности органов государственной власти в оперативной, объективной и достоверной информации о состоянии различных сфер общества, процессах, происходящих в нем, постоянно растут. Данный факт, в свою очередь обуславливает рост нагрузки на сеть связи. Топологические особенности построения сети, обусловленные расположением крупных городов России, определяют требования к пропускной способности, дальности и достоверности передачи информации по волоконно-оптическим линиям связи, входящим в состав транспортной сети связи.

Высокая скорость и дальность передачи информации в совокупности с передачей гетерогенного трафика в различных спектральных каналах приводят к функционированию волоконно-оптических систем передачи (ВОСП) в нелинейном дисперсионном режиме. При этом эволюция импульса при распространении по оптическому волокну характеризуется искажениями, связанными с ослаблением, хроматической и поляризационной модовой дисперсиями (ПМД), а также влиянием нелинейных эффектов.

Большая часть искажений, вызванных указанными факторами, в настоящее время может быть компенсирована средствами цифровой обработки сигналов (ЦОС) в приемнике [1, 2]. Однако существующие схемы компенсаторов функционируют на основе линейных моделей ЦОС, точность коррекции которых существенно зависит от длины модели. Таким образом,

может оказаться, что достигнуть приемлемой точности возможно при неприемлемой задержке обработки сигнала. Кроме того, дальнейшее увеличение символьной скорости приводят к ПМД высших порядков, которые не могут быть устранены такими компенсаторами [3, 4]. Данное противоречие возможно устранить на основе нелинейной обработки оптического сигнала.

Предложенная в [5] математическая модель нелинейной формирующей системы основана на многомерном аппроксимирующем полиноме (1):

$$a_i = \sum_{j_1=0}^{n_1} \dots \sum_{j_m=0}^{n_m} C_{j_1,\dots,j_m} x_1^{j_1} \dots x_m^{j_m}, \qquad (1)$$

где m – структурный параметр, определяющий длину модели; $n_1,..., n_m$ – величины, определяющие степень нелинейности оператора; $\vec{C}$ – вектор коэффициентов m-мерного аппроксимирующего полинома. При этом $j_1 \neq j_2 \neq \dots \neq j_m \neq 0$ одновременно [6].

Тогда с учетом (1) можно записать:

$$\hat{X}_c = \begin{bmatrix} \sum_{j_1=0}^{n_1} \dots \sum_{j_m=0}^{n_m} C_{j_1,\dots,j_m}[t] \cdot x_1^{j_1}[1] \cdot \dots \cdot x_m^{j_m}[1] \\ \sum_{j_1=0}^{n_1} \dots \sum_{j_m=0}^{n_m} C_{j_1,\dots,j_m}[t] \cdot x_1^{j_1}[2] \cdot \dots \cdot x_m^{j_m}[2] \\ \vdots \\ \sum_{j_1=0}^{n_1} \dots \sum_{j_m=0}^{n_m} C_{j_1,\dots,j_m}[t] \cdot x_1^{j_1}[K] \cdot \dots \cdot x_m^{j_m}[K] \end{bmatrix}, \qquad (2)$$

где K – количество отсчетов сигнала на тактовом интервале; $\{x_1[i],\dots,x_m[i]\}_t$ – совокупность отсчетов «искаженного» сигнала; $\hat{X}_c$ – восстановленный сигнал.

Форма многомерного аппроксимирующего полинома позволяет непосредственно построить функциональную схему нелинейного корректора, пример которой представлен на рис. 1 (см. ниже).

На рисунке нелинейная часть цифровой структуры выделена пунктирными линиями.

Для определения параметров модели требуется оптимизировать коэффициенты $\vec{C}$ нелинейного корректора.

Воспользовавшись среднеквадратическим критерием точности, сформулируем задачу компенсации искажений в волоконно-оптическом линейном тракте в виде наилучшего приближения последовательности отсчетов

импульса на выходе корректора формирующей системы и последовательности отсчетов «идеального» импульса $\vec{A}_c$ так, чтобы среднеквадратическая ошибка D^2 стремилась к минимуму:

$$D^2 = \left[\vec{A}_c(t),\ F(\vec{X}_c(t), \vec{C}_{j_1,\ldots,j_m}(t)) \right] \to \min_{\vec{C}_{j_1,\ldots,j_m}[t]}. \quad (3)$$

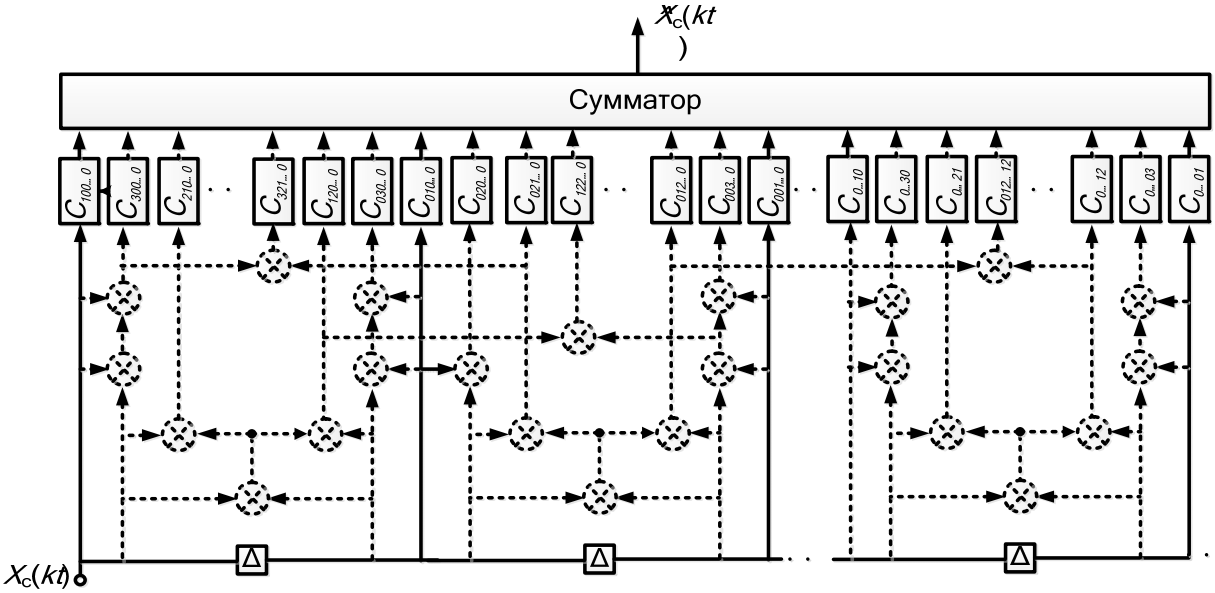


Рис. 1. Пример структуры нелинейного корректора

Выражение (3) для функции среднеквадратической ошибки (СКО), принятой в качестве меры искажения, представим в виде:

$$\left[\vec{A}_c\left(kT\right) - \hat{\vec{X}}_c(kT, \vec{C}_{j_1,\ldots,j_m}) \right]^{\mathrm{T}} \left[\vec{A}_c\left(kT\right) - \hat{\vec{X}}_c(kT, \vec{C}_{j_1,\ldots,j_m}) \right] \to \min_{\vec{C}_{j_1,\ldots,j_m}}, \quad (4)$$

С учетом (2) задача (4) может быть записана подробнее, как выполнение оценки сигнала $A_c(t)$ путем наилучшей оценки по всем его K отсчетам:

$$\sum_{i=1}^{K} \left[a_{ci} - \sum_{j_1=0}^{n_1} \ldots \sum_{j_m=0}^{n_m} C_{j_1,\ldots,j_m} x_1^{j_1}(i) \ldots x_m^{j_m}(i) \right]^2 \to \min_{\vec{C}_{j_1,\ldots,j_m}}. \quad (5)$$

Таким образом, задача компенсации искажений сводится к оптимизационной задаче поиска коэффициентов нелинейного корректора.

Для ее решения продифференцируем левую часть выражения (5) по каждому из коэффициентов $C_{j_1,\ldots,j_m}$ и приравняем частные производные к нулю. Перебором всевозможных комбинаций индексов l_1, l_2, …, l_m, отличающиеся хотя бы одним элементом, находятся все алгебраические уравнения системы на основе (6), из решения которой определяется $\vec{C}_{j_1,\ldots,j_m}$, минимизирующий оптимизируемый функционал (5):

$$\sum_{j_1=0}^{n_1}\dots\sum_{j_m=0}^{n_m} C_{j_1,\dots,j_m} x_1^{j_1+l_1}[i]\dots x_m^{j_m+l_m}[i] = \sum_{i=1}^{K} A_c(t) x_1^{l_1}[i]\dots x_m^{l_m}[i]. \quad (6)$$

Недостатком представленной математической модели является экспоненциальный рост числа коэффициентов системы при линейном росте длины модели. То есть можно получить приемлемую точность коррекции при неприемлемой вычислительной сложности модели и/или стоимости ее реализации.

Например, структура, показанная на рис. 2, лишена этого недостатка и реализует трансверсальную схему нелинейного корректора второго порядка.

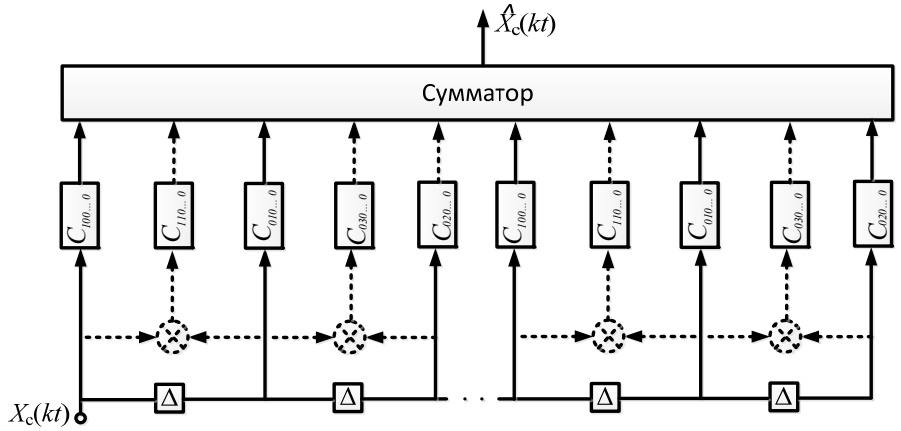


Рис. 2. Структура нелинейного корректора второго порядка

Число коэффициентов такой модели характеризуется выражением $m + (m - 1)$, а система уравнений строится исходя из матрицы вида:

	$C_{10\dots0}$	$C_{01\dots0}$	$\cdots$	$C_{00\dots1}$	$C_{110\dots0}$	$C_{011\dots0}$	$\cdots$	$C_{00\dots11}$
$l_1=1$	x_1^2	x_1x_2	$\cdots$	x_1x_m	$x_1^2x_2$	$x_1x_2x_3$	$\cdots$	$x_1x_{m-1}x_m$
$l_2=1$	x_1x_2	x_2^2	$\cdots$	x_2x_m	$x_1x_2^2$	$x_1^2x_3$	$\cdots$	$x_2x_{m-1}x_m$
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
$l_m=1$	x_1x_m	x_2x_m	$\cdots$	x_m^2	$x_1x_2x_m$	$x_2x_3x_m$	$\cdots$	$x_{m-1}x_m^2$
$\frac{l_1=1}{l_2=1}$	$x_1^2x_2$	$x_1x_2^2$	$\cdots$	$x_1x_2x_m$	$x_1^2x_2^2$	$x_1x_2^2x_3$	$\cdots$	$x_1x_2x_{m-1}x_m$
$\frac{l_2=1}{l_3=1}$	$x_1x_2x_3$	$x_2^2x_3$	$\cdots$	$x_2x_3x_m$	$x_1x_2^2x_3$	$x_1^2x_3^2$	$\cdots$	$x_2x_3x_{m-1}x_m$
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
$\frac{l_{m-1}=1}{l_m=1}$	$x_1x_{m-1}x_m$	$x_2x_{m-1}x_m$	$\cdots$	$x_{m-1}x_m^2$	$x_1x_2x_{m-1}x_m$	$x_2x_3x_{m-1}x_m$	$\cdots$	$x_{m-1}^2x_m^2$

Решение данной системы и есть искомый вектор $\vec{C}_{j_1,\ldots,j_m}$ параметров нелинейного корректора.

Особенностью предлагаемого подхода является возможность коррекции временных параметров оптического сигнала различной формы.

Реализация представленного в статье математического аппарата в виде элементов фурье-оптики, делает возможным коррекцию формы импульсов без электронной обработки.

Дальнейшее совершенствование научно-методического аппарата в данном направлении позволит за счет нелинейной корректирующей системы компенсировать мешающее влияние большей части нелинейных эффектов, в том числе, проявляющихся при передаче высокоскоростных сигналов в многоволновых волоконно-оптических системах передачи.

Список используемых источников

1. Tianhua X., and al. Chromatic dispersion compensation in coherent transmission system using digital filters // Optics Express. 2010. Vol 18. No 15. PP. 1–15.

2. Ip E. M., Kahn J. M. Fiber impairment compensation using coherent detection and digital signal processing // Journal of lightwave technology. 2010. PP. 502–519.

3. Li Y., Eyal A. Measurement of high-order polarization mode dispersion // IEEE Photonics technology letters. 2000. Vol 12. No 7. PP. 861–863.

4. Мусакаев М. Р., Султанов А. Х. Математические модели поляризационной модовой дисперсии высших порядков для кварцевого анизотропного оптического волновода // Компьютерная оптика. 2012. Том 36. № 2. С. 165–172.

5. Чистяков С. В., Яковлев А. В., Мясин К. И. Методика оптимизации характеристик компенсатора поляризационно-модовой дисперсии // Сборник материалов XI Межведомственной конференции «Научно-техническое и информационное обеспечение деятельности спецслужб», посвященная 70-летию Нечаева А. А. 3–6 февраля 2016. Том 8. С. 69–73.

6. Ланнэ А. А. Нелинейные динамические системы: синтез, оптимизация, идентификация. Л. : ВАС, 1985. 240 с.

A N N O T A T I O N S

INFORMATION AND COMMUNICATION NETWORKS AND SYSTEMS

Avramenko V. Method of Constant Authentication of Users in Automated Systems on the Basis of Information Handwriting. – PP. 4–9.
One of problematic issues of access control to information in automated systems of different function is support of constant control of authenticity of users throughout all session. In article the method of constant authentication on the basis of information handwriting of the user characterizing specific features of his operation on the automation equipment is considered.
Key words: automated systems, user, authentication, information handwriting, sensomotorny component, sign.

Avramenko V., Bobreshov-Shishov D. Analysis of the Problem of Detection of Computer Attacks, Implemented Using Exploits. – PP. 9–14.
One of the acute problems of modern infocommunication systems is the protection against computer attacks using exploits. The article presents an analysis of typical attacks using exploits, an original approach is proposed to protect against such attacks.
Key words: infocommunication system, security threat, exploit, vulnerability.

Agievich S., Dvornikov S., Sevidov V., Econom V. The Determination of the Coordinates of Sea Objects in Distress with the use of Unmanned Aircraft Systems. – PP. 14–20.
Issues of location of Maritime objects in distress, are a priority for rescue, therefore, all vessels are equipped with navigation equipment. Meanwhile, often there are situations when this equipment fails, so the problem of determining the location of objects in such conditions is of particular importance. In particular, a method of determining the coordinates of ships in distress with the use of unmanned summer-tional units of the rescue service.
Key words: sea object location identification, unmanned aerial vehicle, vessel in distress.

Akishin V. Customer Experience in the Cognitive Model of Operator's Network Management. – PP. 20–24.
Customer experience is a concept that includes a set of impressions that a customer receives from interaction with telecom operator. But nowadays, there isn't any formal model describing how the customer experience is formed in the specifics of the operator's activity, in particular how the network characteristics, the quality of the provided service, the level of development of the OSS landscape and other aspects of the telecommunications environment can influence it. The paper considers a variant of a functional model, which is based on a cogni-

tive map model. The model describes how customer experience can be influenced by different operations KPI and network characteristic. The functional model is based on the TM Forum recommendations.
Key words: customer Experience, cognitive map, TM Forum.

Alexandrova E., Kovzur M. The Violator Model Building in the IEEE 802.11 Wireless Networks. – PP. 24–28.
Wireless networks are widely used both in modern corporate networks and in home networks. IEEE 802.11 wireless interfaces are very popular and installed in the users' mobile terminals, portable and desktop computers, media devices. The document describes the main threats specific to wireless networks, possible attacks on IEEE 802.11 wireless networks and combinations of attacks that an active attacker can take into account according to current level of hardware and software available. Violator model in wireless networks is developed based on this possible attacks.
Key words: Wi-Fi, wireless networks, violator model, IEEE 802.11

Amelyanovich A., Muthanna A. Testing SDN Implements for WLAN Network Based on Model Network. – PP. 29–31.
Article presents test methods for software-defined wireless area network based on model network of the The Bonch-Bruevich Saint-Petersburg State University of Telecommunications. In the course of the experiment the interaction between access points and SDN controller is considered. The network topology can be controlled via OpenDaylight graphical user interface. As a result, the performance of the access point in the test environment of the wireless local area network was measured.
Key words: SDN controller, Access Point (AP), WLAN.

Andreev V., Bourdine A., Burdin V. Method for Computing of Precision Positioning Scheme Parameters for MDM Channels Placement on Optical Fiber Core End. – PP. 32–37.
This work presents method for computing of precision spatial positioning scheme parameters for mode division multiplexing (MDM) system channels placement on excited optical fiber core end. We demonstrate results of calculations performed for 5-channel MDM system launching into few-mode optical fiber core end with reduced differential mode delay and core diameter 42 μm. It is noted that particular combination of injected mode field radius and precision offset provides transferring of the almost total lunched mode power to only one excited desired guided fiber mode with the same azimuth order.
Keywords: mode division multiplexing, few-mode optical fibers, few-mode regime of optical signal transmission, mode field spatial positioning, differential mode delay, precision offset, mode field diameter, mode coupling coefficients.

Andreyanov Y., Andrianov V., Vitkova L., Potehin I. Information Security in the Activities of Government Departments. – PP. 37–41.
More and more people of the planet began spending more time in social networking sites and other projects that unite people on the Internet. The number of such projects is growing year by year, and this means that the problem of identifying the information and psychological influencet in the information infrastructure is becoming more urgent for the state. The preservation of information is of particular relevance in the government departments. On the one

hand, they accumulate a huge amount of personal information of citizens, and on the other - their activities are related to the security of the country and therefore not all information can go beyond them.
Key words: monitoring, social networking sites, BigData, SERM, ORM, information and psychological influence, information war.

Andrianov V., Chekolov A. Research Botnet Network Capabilities and Methodology of Protection from Unauthorized Access. – 41–46.
This article discusses: What is a botnet; the process of its formation; what opportunities have botnets. The main methods of detection and repel attacks using botnets.
Key words: botnets, exploits, clickers, grabbers, framer.

Anikevich E., Vitkova L., Satsuk E., Sergeeva I. Leak Prevention Confidential Data in Information Systems. – PP. 46–51.
Control and monitoring of events and incidents increasingly become a priority in information security. More and more number of companies is suffering losses because of theft of information. Imprudence, indiscretion of ordinary employee, the lack of skills and knowledge in the field of information security increase the risks and become major sources of threats in information systems. In this article the authors consider some popular methods of security provision.
Key words: threat, vulnerability, malicious software, hacker, damage, attack, BYoD, DLP-systems, SIEM.

Anufrenko A., Bucev S., Kanaev A., Koputin A. Simulation Model of Traffic Distribution on the Section of the Transport Network – PP. 51–54.
The development of technologies of transport networks, increasing demands for its functioning necessitate a detailed understanding of the processes occurring in the transport network. A good way to do this is simulation. The paper presents the essence of the developed simulation model of the transport network.
Key words: transport communications network, simulation, GPSS World.

Anufrenko A., Vasiliev E., Goidenko V., Kanaev A. A Simulation Model of the Aggregation Node in a Telecommunication Network – PP. 54–56.
From the operation of the aggregation node of a communication network depends on the nodes of the transport network node and access network. Development of simulation models of node aggregation allows to perform their complex structure. The paper presents a model of the aggregate node, the program developed in the "Advanced editor GPSS World".
Key words: aggregation node of a communication network, simulation, GPSS World.

Anufrenko A., Kanaev A., Login E. Multi-Agent Approach to Structure Formation System of Management of Transport Networks Based on Carrier Ethernet Technology. – PP. 57–59.
The growth of a variety of digital equipment, increase in its monitored parameters requires control system ability to work with distributed objects with a large set of variables. Because this is a multi-agent approach to structure formation control system.
Key words: control system of the transport network, multi-agent approach, Carrier Ethernet.

Arsaev R., Gydkov M., Koryakin D., Nigamatullin A. Study design and tools software defined networking. – 60–62.
Discusses the technology and basic design tools software defined networking based on OpenFlow Protocol.
The rapid development of computing power, memory and capabilities of high-speed data transmission has led to the development of new technologies of constructing network infrastructures.
Key words: data transmission, protection of information, networks, Internet.

Akhrameeva K., Gruzinskiy B. Geometric Hashing and Its Applications in Information Security. – PP. 63–67.
The article discusses the possibility of applying geometric hashing algorithms in Information Security and proposes different practical usage cases of these algorithms, such as automated content filtering, automated surveillance feed analysis and biometric authentication.
Key words: geometric hashing, content filtering, emergency notification systems, authentication.

Ahrameeva K., Skorodumov S. SteganRTP in IP-Telephony. – PP. 68–70.
The article discusses the use of SteganRTP's method in IP telephony to view the incoming stream, or forward RTP packets to the desired device, to further immerse the hidden information and retrieve it. A description of the program is given in several modes of operation, which gives a variation in the use of this method. An analysis of the advantages and disadvantages of the method has been made, and the features and technical requirements for using the program have been revealed.
Key words: digital steganography, IP-telephony, RTP, SteganRTP.

Ahrameeva K., Treskin N. Using Perceptual Hash-Functions in Information Security. – PP. 71–74.
This article include researching result of deferent perceptual hash–functions types, analysis of practical usage (ability to define authentic and similarity images of deferent types) and algorithm calculation speed. Examined usage options of perceptual hash–functions to improve modern information security, in particular, to blocking unwanted images on the Internet web sites.
Key words: perceptual hash–functions, content filtration, notification system, authentication.

Babynin E., Zadurova A. The use of Mathcad to Simulate the Physical Processes in the Mobile Means of Informing and Warning. – PP. 75–78.
Device speakers installed on the roof of the mobile systems of notification, which transmits audio information to the population, play a very important role in emergency situations. Modelling of physical process of oscillation of the metal diaphragm in a horn loudspeaker with the help of computer systems and is discussed in this article.
Key words: a horn speaker, computer system modeling, MathCad Bessel equation, membrane.

Belaidi M., Bylina M. Study of the Opportunity of Application of the EDFA with Removable Pumping. – PP. 78–83.
The work present, the results of a study of the possibilities of using EDFA optical amplifiers based on fibers doped with erbium ions with remote pumping. The study was carried out using the GainMaster program, which simulates the work of EDFA.
Key words: Optical amplifier, fiber doped with erbium ions, EDF, EDFA, gain.

Belozercev I., Elagin V. OTT Services in LTE. – PP. 83–88.
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: LTE, CS Fallback, IMS, OTT.

Birikh E., Vitkova L., Gorelenko V., Kazakov D. Protection of Information in Databases. – PP. 89–92.
One of the most effective ways to store and work with large amount of data is database. High usage of this technology make database resource problem relevant. Exist some method of hold confidential of database information. In this article author, review its information security methods (base and additional).
Key words: DBMS, SQL, threat, access rights, encryption, password, security labels.

Birih E., Vitkova, L., Levin V., Chmutov M. The Development of Standards and Manuals in the Field of Cloud Computing. – PP. 92–95.
Throughout the world there is active development of cloud computing and documents on their implementation. The study and use of international standards and guidelines in this area will allow to reduce terms of development of domestic instruments and to improve their quality. Cloud resources and technologies have great potential, but when they are used, you may encounter a number of problems that the authors explore in their work.
Key words: cloud, cloud computing, information security, interoperability.

Birih E., Vitkova L., Sakharov D., Sergeeva I. A Method of Increasing the Security of a Distributed Computing System Based on DSS and Taking Into Account Forecasting. – PP. 96–100.
The urgency of improving the security of distributed computing systems connected with the increase in the number of attacks on information system, particularly related to public authorities. With the constant emergence of new vulnerabilities, the system is not able to detect and prevent attacks, that is, to resist changing conditions. There is a need to create tools for automatic search of attacks, capable of accumulating the experience of neutralization of the existing threats and to adapt the system for new. Thus, the creation of a method of using the system of support of decision-making, taking into account predict the state of the distributed computing system in the near future.
Key words: DSS, attack, security, information system, DSS.

Birih E., Vitkova L., Saharov D., Shashkin V. Big Data Algorithms and Monitoring of IT Infrastructures of Enterprises. – 100–103.
Management and control over events and incidents are increasingly becoming a priority in information security. More and more organizations are suffering losses because of the theft of information. Control over the entire infrastructure of the enterprise can reduce the risks of unauthorized intrusions and track the main trends of threats.
Key words: control, BIG DATA, Large data, monitoring, damage, resource allocation, failure, information security.

Birikh E., Ryabov E., Sakharov D. Methodology of Formation the Model of Information Systems Security Threats. – PP. 103–107.
This article describes the concept of information systems threat model, features of this formation. Article provides the analysis of the existing legislation devoted to this subject. Need of creating the threat model is proved. The article suggests an approach to its implementation.
Key words: threats model, information system, information security, methodic, personal data.

Biryukov A., Izrailov K. The comparative analysis of models of threats of information security for the benefit of applicability for multi-stage schemes of the attacks. – PP. 108–112.
Authors consider the existing models of threats of the information security. The description and purpose of models is given. The main merits and demerits are allocated. A conclusion concerning insufficiency of models for the solution of a number of urgent problems of IB, such as forecasting of new threats, finding of possible ways of realization of the attacks and their probabilities is proved. The new model solving the specified problems and constructed on the new principle is offered.
Key words: threat model, information security, multi-stage attack.

Buzykov L., Ermakova T. Studying of Signals of Hemodynamics and Usage of Mutual Information. – PP. 113–116.
A comparison analysis of used methods for processing hemodynamic signals has been performed. All the advantages and drawbacks have been highlighted. It's suggested to use Mutual information for avoiding such disadvantage as Time-Lag amount. It is known, that in Information theory Mutual information is used for assessment of mutual dependency between random values. Mutual information is a similarity measurement of two variables.
Key words: self-similarity, hemodynamic, mutual information.

Bulatov N., Vitkova L., Shashkin V. Theoretical Aspects of Information Security Management in a Business Organization. – PP. 117–122.
All the classified information in the facility should be monitored, tracked and in case of the illegal transfer, be blocked. The majority of organizations lose their substantial profit due to irresponsible employees who for any reason (accidental or on purpose) are leaking authorized data outwards business network. This article considers basic systems and their security methods of data leak prevention.
Key words: DLP, SIEM, threat, vulnerability, attack, malware, data leak, incidents.

Bylina M., Popova S. Chromatic Dispersion Compensation Methods in Optical Linear Tracts. – PP. 122–127.

The report considers chromatic dispersion compensation methods and suggests methods for calculating the length of the regenerative section of fiber optic links with dispersion compensators based on a special DCF fiber, a fiber Bragg grating with a variable period and a photonic crystal PCF.

Key words: length of the regenerative section, chromatic dispersion, dispersion compensation fiber, fiber Bragg grating, photonic crystal.

Vasilishin N., Dubrovin N., Ushakov I., Chechulin A. Techniques for Network Traffic Gathering and Analysis Based on Big Data Technologies. – PP. 127–131.

Currently application of the big data technology for the fast processing of the large unstructed datasets, such as network traffic flow, grows. Big data technology is based on the methods and algorithms of data gathering and analysis. These methods and algorithms allow to obtain results of analysis on the base of the predefined conditions in the required format. The format is convenient for the perception and decision-making. The paper reviews methods of network traffic gathering and analysis using big data technology.

Keywords: Big data, techniques for data gathering and analysis, computer attack detection, network traffic.

Veremiychuk I., Elagin V. Analysis of SIP-Network Vulnerability to Fraud-Threats Based on Imitation of Attacks on SIP-Service Provider's Network. – PP. 131–135.

Each year the number of telecom operators, allowing various companies and institutions to connect to the PSTN by the SIP protocol, is increasing. The article considers the basic schemes of interaction between SIP-telephony operators and their clients and possible attacks from intruders that can be implemented on various sections of the NGN network.

Key words: SIP-telephony, fraud, SBC, protection against fraud.

Vikulov A., Paramonov A. Wlan Client Diversity Analysis. – PP. 136–139.

In modern Wi-Fi networks, design challenges more and more often require accurate network throughput estimation. This needs to understand the client device abilities as well as the characteristics of generated traffic. This is not trivial because vendors` recommendations are quite rough. Here is this work, a 30-day monitoring of Wi-Fi access network has been carried out, client abilities has been gathered and analyzed with following conclusion of its adequacy to WLAN market leaders` recommendations.

Key words: IEEE 802.11, Client abilities, Traffic characteristics, Wi-Fi.

Vintenkova Y., Kozlov S. The Efficiency of ant Colony Optimization Algorithm in the Collective Dynamic Routing Task. – PP. 140–142.

Article represents the development and modeling of heuristic ant colony optimization algorithm to decrease sophistication of collective dynamic routing method that is used to reduce the intra-system interference impact on wideband radio access networks performance.

Key words: routing, ant colony optimization algorithm, collective dynamic routing, integer programming.

Vitkova L., Denisov E., Ryabova O., Sakharov D. The risks of developing projects based on open data from viewpoint of new doctrine of information security. – PP. 143–147.
Open Data actively develop in all over the world. And our country isn't an exception. Interest in open Data is showing including state. However at this moment the threats to information security are increasing. In article discusses the actual possible problems of further development of open data in terms of a new doctrine of information security.
Key words: Open Data, Big Data, Doctrine, Information Security, SIEM.

Vitkova L., Dudnikova M., Levin M. Investigation of Incidents of Information Security During the Exploitation of Zero-Day Vulnerability. – PP. 147–152.
In this report, the authors analysis the cryptographic virus in the target attack. The virus signatures are shown; the code of the executable file is given; the process of the no_more_ransom virus operation is described; consequences of infection and ways to prevent infection of the computer are described.
Key words: virus, 0-day attack, target attack, Information Security.

Vitkova L., Ivanov A., Sergeeva I. Development and Researching Methods for Assessing Risks in Cloud Technologies. – PP. 152–155.
The development of the Internet has led to a great popularity of cloud technologies. Their introduction into business-processes brings in itself different pluses and minuses. In order to make a decision – you need to analyze the possible risks that may arise due to the transition to the cloud. In that article the author examines the most topical methods of risk assessment regarding for cloud computing.
Key word: cloud computing, risk management, information technologies, risks.

Vitkova L., Makhova I., Sakharov D. Searching of the Packet Transport Technologies in a Hybrid Environment SD-WAN. – PP. 156–160.
Nowdays, networks have become a strategically important asset, which has led to the need to switch on the software-defined WAN networks. Modern technologies allow solving problems of the network administration.In this paper, the authors consider the possibilities of implementing SD-WAN technology in hybrid networks.
Key words: SD-WAN, Distributed network, traffic, hybrid network, performance.

Vitkova L., Petrova A., Sakharov D. Management of Information Security Distributed Systems Storage and Handling of Funds. – PP. 161–165.
In today's world of online banking, electronic cash, wallets and other innovations create the illusion of confidence that the money earned is safely tucked away from intruders. However, the evolution in the banking sector gave impetus to the development of methods of illegal profit, and other threats of financial fraud, so the relevance of this topic is increasing day by day. The authors explore the concepts of distributed storage and processing of funds. Describes the concepts, type's electronic submission of funds and consider existing the most typical vulnerabilities and threats to information security.
Key words: data-storage systems, distributed systems, e-money, big data.

Vitkova L., Potekhin I., Sakharov D. The Problem of Identifying Information-Psychological Influence in the Information Infrastructure of the Russian Federation. – PP. 166-170.
An increasing number of people began to gather in social networks and other various projects, uniting people on the Internet. The number of such projects is growing from year to year, this means that the problem of identifying information-psychological influence in the information infrastructure is becoming more urgent for the state.
Key words: monitoring, social networking, BigData, SERM, ORM, information-psychological impact, information warfare.

Vitkova L., Ryabova O., Sakharov D., Tikhonova E. A Study of Methods of Control of Information Security of Open Data. – PP. 170–174.
In the modern world of open data are an integral part of everyday life, whereby they are subjected to various kinds of illegal and unfair use. The authors analyze the threats, assess risks and examine ways of ensuring the security of open data.
Key words: open data, public data, public data, open content, information security.

Vikhrov M., Fedorchenko A., Chechulin A. Approaches for Rules Representations for Security Events Correlation in Cyber-Physical Systems. – PP. 175–179.
Currently information technology are widely applicable in various spheres of life and their distribution continues to grow. In its turn distribution of the cyber-physical systems resulted in increased relevance of their security. Information correlation is one of the essential stages of security data processing. This paper is devoted to the research of implementations of rules-oriented approach for the information correlation in the various security devices. We describe rules specifications, ways of their representation, and examples for the specific security systems. We also provide comparison of the cybernetic (information) and physical security tools. It allows to specify features of construction of security mechanisms for the cyber-physical systems.
Keywords: security event correlation, rule-based approach, information security, cyber-physical systems.

Vladimirov S., Mukhametshina D. The Research of the Software for Automatic Developing of .Reyhani-Masoleh Multiplier over Galois Field. – PP. 180–184.
The paper presents the results of research of the software for task of automatic source code developing for Reyhani-Masoleh multiplier over binary Galois fields. It contains the requirements for the developing software and software operating procedure and example. Also the paper introduces the tendencies of the software development.
Key words: development automation, automatic source code developing, Galois field, Galois field elements multiplication, Reyhani-Masoleh multiplier, C programming language.

Volkov A., Muthanna A. S. Development of the Method for Testing of the Internet of Things Management System in Smart City Concept Based on SDN Network. – PP. 185–190.
The paper devoted to testing of the Internet of Things Management System based on SDN network. As a method investigating the behavior of management and network infrastructure Systems were also tested traffic of the Internet of things. The paper deals with model of the "Smart City" on example of the Central District of St. Petersburg. During the test it was

defined parameters such as: RTT, packet delay in the network. The conclusion on the use of the SDN, as the basic network infrastructure in the conditions of IoT traffic. In order to the consideration of the management system IoTDM as a service for the "Smart City", was conducted full-scale experiment on the developed model, which in turn reflects the possibility of specific distribution scheme of monitoring and control systems for the Central District of St. Petersburg.
Keywords: Internet of thingd, IoT, delay, HTTP, SDN, API, RTT, Smart City, Data Managment.

Volkov I., Ivanov C. Leak Acoustic Channel Speech Occurs when its Companion Transmission over Fiber-Optic Communication Lines. – PP. 191–194.
Fiber-optic lines are becoming more common, and the methods to intercept data on the communication channel, are constantly being improved, so it is necessary to continuously improve the methods and the protection of information from leakage through technical channels of communication tools.
Key words: channels of information leakage, the protection of the acoustic information, the fiber-optic communication lines.

Volkogonov V., Golubev V., Ushakov I. The Problem of Cryptographic Protection in Cisco Devices when Using Current Firmware. – PP. 194–198.
This article discusses the problem of data encryption on Cisco devices when using encryption keys with the default key length.
In the course of the work, a popular way of building virtual private networks will be considered, as well as a lower threshold of cryptographic protection, where it will be possible to say that the network is resistant to the "man in the middle" attack.
Keywords: cryptography, security information, digital certificate, public key, private key, traffic analysis.

Vorozhbitova A., Elagin V. Analysis of Traffic Management Features in SDN. – PP. 198–201.
This article examines the traffic management features of Software Defined Network (SDN). The management is realized by OpenFlow protocol using tables that describe flows (flow table, group table, meter table). There are messages that are used for configuration flows and their type depends on the initiator (controller or switch). The messages are analyzed and now you can understand how to change the tables in the switch for traffic management.
Key words: SDN, OpenFlow, flow table, OpenFlow message, traffic management.

Vorontsov V., Koryakin D. The Implementation of Mechanisms for the Prioritization of Packet Traffic in Special-Purpose Networks. – PP. 201–204.
Network military use have a complex structure. They include various "competing" objects such as signals, instructions, orders. Packet traffic to the switching centers are divided into priority and not priority traffic. Processing of packets each queue is organized according to the algorithm for processing route processor, and the main resource is directed to a higher priority queue. Because of the specificity of the organization of communication networks for military use there is a need to address issues with prioritizing the many alternatives to se-

lect a preferred option. Therefore, need priority model, taking into account the importance of speed, volume of data transmitted, the class of each individual priority of the stream, and the arrival time of the packet in the queue.
Key words: prioritization of network traffic, QOS, TOS.

Visotskiy S., Elagin V., Pryazhnikov V. Technical Aspects of DPI in SDN. – PP. 205–209.
This article explains the SDN network. Due to the insufficient development of the network lacks a lot of services on the network. The paper describes the possibility of using DPI technology for the expansion of network functionality.
Key words: software defined network, traffic, deep packet inspection.

Gagarina S., Diubov A., Mikutavichaite D. Impact of PMD on Performance of Optical Communication System. – PP. 209–214.
The article presents the results of modeling a fiber-optic communication system taking into account the influence of polarization mode dispersion (PMD) in single mode fibers. Characteristic of distortion caused by PMD in the propagation of pulses through optical fibers are shown. The simulation is performed using the OptiSystem software.
Key words: optical fiber, polarisation mode dispersion, fiber-optic communication system, differential group delay.

Gerling E., Kulishkina E. Model of Violators of Information Security. – PP. 214–219.
In this article probable violators are analyzed, standard models of violators which purpose was plunder of confidential information by the attacks to local computer networks are offered. On the example of a calculation formula of probability of information leakage assessment of probability of information leakage in case of the attack directed to the personal computer equipped with the antivirus software is made. On the basis of the offered classification of violators a row of methods of protection of an information system is given.
Key words: Information security, violator's model, probability of information leakage, antivirus software.

Glagolev S, Dotsenko S, Durov L, Yalunina T. Investigation of the Influence of Nonlinear Effects on Signal Transmission Processes in Fiber-Optic Processing Systems with DWDM. – PP. 219–224.
In single-mode fiber-optic, nonlinear interaction of several optical waves can occur, as a result of which combination harmonics appear. One of these effects is four-wave mixing of FWM. The name of the effect is due to the fact that four waves participate in the interaction. This effect plays an important role in DWDM. It is strongly manifested in the simultaneous propagation of several quasi-monochromatic waves with close frequencies and polarizations with single-mode fiber-optic.
Key words: FOCL, DWDM, nonlinear effects, four-wave mixing.

Glagolev S., Polyakova E., Yalunina T. Position of Photonics in Promising Infocommunication Technologies. – PP. 225–230.
Nowdays, most of promising infocommunication technologies are built on the principles of photonics: from optical disks to the creation of sensors that register light streams in ac-

cordance with the slightest change in the environment. Photonics covers many sciences and technologies related to the generation, control and detection of photons. These include: optics, laser physics, quantum electronics, spectroscopy, optoelectronics, quantum technologies, bio-, nano- and radiophotonics and much more.
Key words: integrated optics, radio of fiber, RoF, reconfigurable multiplexer, ROADM, radiophotonics, perspective infocommunication technologies.

Golubev A. Blockchain Technology: Prospects, Applications, Educational Vacuum. – PP. 230–234.
A general description of blochain-based systems is provided. The features which are most important when determining the scope of applications are highlighted. Applications are considered. An interest from governmental and financial institution is noted. The near absence of educational courses is mentioned. A set of competencies expected from a blockcahin engineer is investigated. Blockchain engineer course syllabus is mapped out.
Key words: blockchain, distributed ledger, decentralized database, higher education course.

Grishin I., Diubov A., Hrichkov V., Yalunina T. Choosing Elements Framework for Visible Spectrum Data Transmission Systems Development. – PP. 235–240.
Currently, the technology of data transmission using visible light is considered as one of the possible solutions to the impending problem of radio frequencies spectrum crisis, the article examines the technical parameters of the basic functional elements included in the visible light communication systems.
Key words: transmission systems with visible light, VLC technology, Li-Fi, RGB-LEDs.

Gromov V., Elagin V. The Study of Face-Recognition Algorithms' Features Based on the Example of Computer Vision Library. – PP. 240–245.
Computer vision is a rapidly growing field, partly because of the affordable hardware (cameras, processing power) and partly because vision algorithms are starting to mature. This field started with the motivation to study how computers process images and how to apply this knowledge to develop useful programs. This study belongs to the fields of computer vision. The key objectives of this paper are that: 1) MegaFace Benchmark challenge for face-recognition algorithms; 2) new developments in the fields of SDK (Software Development Kit); 3) OpenCV library for face recognition. Also we carry out the research of the following face-recognition algorithms represented in OpenCV library: Viola–Jones object detection, Eigenfaces, Fisherfaces and Local Binary Patterns Histograms. This paper focuses on the crucial importance of face-recognition algorithms' studies. These researches help the novice investigators to study of computer vision algorithms.
In the future, it seems appropriate for the following researches to shift the focus on face-recognition methods using neural networks instead of OpenCV methods.
Key words: face recognition, MegaFace, OpenCV, Viola–Jones object detection, Eigenfaces, Fisherfaces, Local Binary Patterns Histograms.

Dao N., Paramonov A. Methods of Organizing a Communication Network Based Unmanned Aerial Vehicles. – PP. 245–249.
This article describes different methods of organizing a communication network based on unmanned aerial vehicles. Considering the main network architecture in order to choose

the main node for the group UAVs. The algorithm of clustering forel is used in modeling software Mathcad. The results obtained make it possible to choose the optimal method for organizing a UAV network.
Key words: unmanned aerial vehicles, centralized network, decentralized network.

Desnitsky V., Kotenko I., Lauta O., Saenko I. An Approach to the Cyber-Resilience Assessment on the Basis of Topological Conversion of Stochastic Networks. – PP. 250–255.
The paper considers the method of computer network cyber-resilience evaluation based on analytical simulation of the computer attacks by means of stochastic networks and their subsequent topological conversion. Metrics and analytical expressions for a cyber-resilience assessment are offered. Results of the experimental assessment of the offered models and a method are discussed. The proposals on search of counteraction measures against the computer attacks leading to increase in computer network cyber-resilience are formulated.
Key words: cyber security, attack modeling, computer network cyber-resilience, computer attacks, resilience, stochastic networks, Laplace transform.

Desnitsky V., Ostroushchenko N. A Model of the Secure Mobile Communication Network for Support and Operational Management in Emergency Situations. – PP.255–260.
The paper proposes a model of a secure mobile communication system for support and operational management in emergency situations. The model is built on the basis of XBee software/hardware modules that support the operation of ZigBee wireless communication protocol. Prototypes of network devices have been developed, and the analysis of cyber-physical security incidents has been carried out.
Key words: Operational management, XBee, mesh network, intruder model.

Dinh D. Kirichek R. Approaches to the Organization of Heterogeneous Mobile Gateways Based on Unmanned Aerial Vehicles. – PP. 260–265.
In the last several years, unmanned aerial vehicles (UAVs) have been used in many spheres of activities. In connection with the development of power supply technologies, the battery life of the UAV has increased significantly and is currently 2-3 hours. According to forecasts of the International Telecommunication Union (ITU) in 2020, the fifth generation mobile networks (5G, IMT-2020) will be exploited ubiquitously. In the concept 5G, seamless communication between devices of the Internet of things which interact on the basis of various technologies is supposed. Ensuring such connectivity requires covering completely areas with a large number of devices. For these purposes, it is intended to use a UAV with a gateway on board. Such a gateway will serve as a base station between subscribers (devices, cellular telephones, etc.) and a public communication network. The article considers approaches to the organization of heterogeneous mobile gateways based on unmanned aerial vehicles, as well as models of such interaction.
Key words: flying sensor network, internet of thing, IoT, 5G, UAV, drone, gateway.

Dmitrieva E., Krasov A., Filippov O. Development of Software for the Interception Control Unmanned Aerial Vehicles on the Example of the Model V686 from the Company WLtoys. – PP. 266–270.

In following article, we consider the possibility and the practical application of reverse engineering data transfer protocol between the remote control and the UAV from companies WLtoys model V686. Also, the study of radio frequency channels, the potential Denial-of-service attack of the UAV, remote control interception.
Key words: UAV, RTL-SDR HackRF, Reverse Engineering, GNU Radio, nmap.

Dunaytsev R., Korotkin K. Wi-Fi Site Surveys, Planning and Design. – PP. 270–274.
This paper provides an overview of such aspects of the WLAN life cycle as pre- and post-deployment site surveys, predictive design and analysis. Throughout the discussion, special emphasis is placed on site survey and design guidelines for deployment of industrial outdoor Wi-Fi networks.
Key words: Wi-Fi, IEEE 802.11, WLAN, site survey, planning, design.

Dunaytsev R., Kulebiakina O. An Overview of Modern Multi-Core Processor Architectures and the Network-on-Chip Technology. – PP. 274–277.
Over the last years, multi-core processor architectures have become a hot research topic in the development of computer technologies. However, technology development in this area cannot move further because of several difficulties: increasing the frequency is no longer available and increasing the number of cores above 8 has more disadvantages than benefits. In this paper, we provide an overview of modern multi-core processor architectures and discuss their advantages and drawbacks.
Key words: SoC, NoC, WiNoC, multi-core processor.

Dunaytsev R., Moskaliuk A. An Overview of Traffic Sniffers and Analyzers for High-Speed Data Flows. – PP. 277–281.
Data transfer speeds are growing exponentially. Due to huge amounts of traffic, previous methods of packet capture and analysis have a low efficiency. As a result, there is a need for new packet capturing technologies that can deal with speeds higher than 1 Gbit/s. In this paper, we provide an overview of modern traffic sniffers and analyzers, and discuss their benefits and drawbacks.
Key words: traffic analysis, traffic capture, flows, high-speed traffic.

Dunaytsev R., Naumicheva D. A Wireless Site Survey of SUT Dormitory “Lesnoye”. – PP. 281–285
In this paper, the results of a wireless site survey of SUT dormitory “Lesnoye” are presented. Using Ekahau Site Survey, the following information has been collected and charted: the total number of access points installed by tenants, the Wi-Fi channels used in the 2.4 GHz and 5 GHz frequency bands, the security protocols and amendments to IEEE 802.11 supported by the detected access points.
Key words: Wi-Fi, IEEE 802.11, WLAN, site survey, access point.

Dunaytsev R., Romanova O. An Overview of Cloud Gaming Services. – PP. 285–290.
In this paper, we provide an overview of cloud gaming services starting from the very beginning and up to these days, analyze the reasons of their rise and fall. We also outline drawbacks and benefits of such services.
Key words: OnLive, Playkey, LiquidSky, cloud game, remote play.

Dunaytsev R., Tampio A. A Wireless Site Survey of SUT Dormitory “Rybatskoye”. – PP. 290–295.
In this paper, the results of a wireless site survey of SUT dormitory “Rybatskoye” are presented. Using Ekahau Site Survey, the following information has been collected and charted: the total number of access points installed by tenants, the Wi-Fi channels used in the 2.4 GHz and 5 GHz frequency bands, the security protocols and amendments to IEEE 802.11 supported by the detected access points, the download and upload speeds achievable through Ethernet and Wi-Fi connections.
Key words: Wi-Fi, IEEE 802.11, WLAN, site survey, access point.

Durov L., Diubov A. Nonlinear Effects in Semiconductor Optical Amplifiers. – PP. 296–300.
The article describes the design and operation of semiconductor optical amplifiers. A feature of this class of devices is the presence of strong nonlinear effects. The results of the simulation of non-linear effects of four-wave mixing and cross modulation in a semiconductor amplifier shown the application of these effects to perform wavelength conversion. Modeling done in OptiSystem.
Key words: semiconductor optical amplifier, computer simulation, non-linear effect, four-wave mixing, cross modulation.

Diubov A., Tsaregorotsev A. Performance Analysis of Coherent Optical OFDM Communication Systems. – PP. 301–304.
Orthogonal frequency division multiplexing with direct and coherent reception method is currently regarded as the most promising for the organization of long optical communication channels. The article describes the simulation of OFDM communication system based on the schema project, part of the software Optisystem. Given the calculated signal constellation electric signals (before and after passing through the communication channel), characterizing the reliability of information transmission.
Key words: orthogonal frequency division multiplexing, optical communication system, optical fiber, signal constellation, OFDM.

Elagin V., Onufrienko A. The Study of the Statistical Aspects of the use of DPI Technology to Identify the Traffic and Ensure the QoS of OTT-services. – PP. 304–310.
In this paper, the authors introduce the definition of OTT-services, give the description of these services and a brief comparison with the services of traditional managed services. There are presented the main indicators of network performance necessary providing the specified quality of service in the provision and transfer of different types of traffic. This article describes the problems associated with the emergence of OTT-services on the operator's network. As a promising option to monetize OTT-services, the authors present the approaches and procedures for DPI, which provide the necessary requirements for QoS in the provision of resources of its network to OTT-services. In conclusion, the authors sum up the main advantages from the introduction of DPI technology in the operator's network to transmission of defined user-generated content.
Keywords: Over The Top, OTT-service, OTT-provider, DPI, Deep Packet Inspection, QoS, quality of service.

Elagin V., Sorokin V. Technical Aspects of Lawful Interception of Traffic in SDN. – PP. 310–314.

Traditional networks are not always able to respond effectively to the new needs of the user. The existing network architecture requires modernization. SDN is one of the promising directions of development of information networks. The article discusses the concept of SDN networks ,legal requirements for public networks and the current difficulties encountered in the implementation of lawful interception of traffic in networks SDN.

Keywords: lawful interception, software defined network, SDN, DPI.

Zhulanov V., Muthanna A. Software-Defined Networks Architecture for Cellular Networks 5G. – PP. 314–319.

Most researchers in this sphere suggest that future 5G systems will become an infrastructure for the deployment of Internet of Things. The device-to-device interaction D2D is the key communication paradigm that supports the connection of heterogeneous objects among themselves and provides a number of important advantages. One of the main goals and challenges for 5G cellular systems is the design of flexible network architectures that can be implemented on the principles of software-defined networks. Existing commercial cellular systems are based on closed and hard-management architectures, based on hardware in both the radio access interface and the core network. These problems significantly delay the adoption and implementation of new standards; impose significant difficulties in implementing new methods to increase the network capacity. This article is discussed the advantages of the SDN architecture for 5G networks.

Keywords: SDN controller, architecture, radio access, interface, software-defined network, wireless.

Zhuravel E., Isupova E. Structural Model of Resources of a Multiservice Communication Network of Limited use. – PP.319–322.

The structural model of resources of a multiservice communication network of limited use is considered, technologies of creation of the resources making it are given, approach to their formalization is offered, need of specification of models of sources of threats, threats and influences for formation of adequate models of counter-measures is justified.

Key words: multiservice communication network of limited use, communication network resources.

Zhurkin D., Ryabova O., Sakharov D. Aspects of Information Security at the Creation of Applications Based on Open Data. – PP. 323–327.

In the work are given definitions to open data, described regulatory legal acts, considered possible vulnerabilities and disadvantages of publication of open data. An effective way of using open data is offered - a prototype of its own application using a set of open data published on the website of the Federal Service for Supervision in the Sphere of Communications, Information Technology and Mass Communications - Register of operators processing personal data.

Key words: Open data, public data, open data formats, open data disclosure vulnerabilities, open data applications.

Zagorelsky V, Korchagin M, Frolova Y. What is a DWDM System. Its Major Components. The Relevance of the Use and Further Development of the Russian Federation. – PP. 328–332.

The problem of providing the growing demand for information exchange. The need for high speed transmission of information over long distances, while maintaining communication reliability. The variant of solving this problem, based on the principle of dense wavelength division multiplexing.

Key words: dense wavelength division multiplexing, channel capacity, multiplexer, transponder, amplifier, regenerator.

Zarubin A., Koval A., **Moshkin V., Filippov A.** Application of Linked Knowledge Approach in Tasks of Semantic Analysis of Semi-Structured Information Resources. – PP. 333–337.

Research devoted to solving the problem of the approach Linked Knowledge in tasks of semantic analysis of semi-structured resources. This approach is based on the use of an ontological model of knowledge representation about the subject, given the diversity of semantic contexts. The paper presents the structure of the knowledge base, developed on the basis of the proposed model.

Key words: semantics, ontology, Linked Knowledge, text resources.

Zakharova T., Tcvetkov A. The Analysis of the Existing Regulating Documents for Forming of Security Policy Into the Electronic Document Management System of Higher Educational Institution. – PP. 337–343.

Consider the concept of electronic document management system. Identified the main Russian standards, and it identified the need for recommendations for the introduction of electronic document management system and the formation of the security for different types of organizations. It showed a possible way of protection on the basis of existing legal instruments of information in the field of electronic document on the example of a higher education institution.

Key words: electronic document management system, information security, data protection, regulatory documents, access control, authentication, e-signature, smart card.

Zimin A., Kosov N. Ensuring Information Security for Computer Programs During Process of it's Creation and Employment. – PP. 343–348.

This work is related to such aspects as ensuring information security for computer programs during process of it's creation and employment as an object of intellectual property. Description of organizational, law and technical information security of computer programs is given. Issues of securing computer programs copyright during it's employment are analyzed. Practical solution of solving copyright issues on a technical level are suggested.

Key words: intellectual property, computer program, copyright, watermark.

Zueva E., Yakovlev V. Analysis of Methods to Forma Shared Key for Pairing Mobile Devices. – PP. 348–353.

An analysis of authentication methods for a pair of mobile user devices was carried out to form a shared key for creating a secure communication between them. The methods considered in this research, based on the use of additional channels, are as follows: visual,

acoustic, vibrational and magneto metric. A system of indicators and criteria were developed to compare these methods, taking into account the ease of their operation by users
Key words: authentication, mobile devices, additional channel.

Ivanov V., Koryakin D. Features of Functioning of Modern Automated Monitoring Systems for Telecommunication Networks. – PP. 353–356.
Today, in conditions of continuous development and constant improvement of the complexity of telecommunication systems, ensuring reliable operation of the info-communication processes and services that allow the user to organize the effective work is a key objective of the network administrator. Given the importance of this process requires constant monitoring of the work of the entire communications network, which includes many different telecommunication and server equipment. Control mechanisms have found themselves in the automated monitoring systems, the use of which allows for real-time tracking of the status of availability and performance of the telecommunications network components, regardless of the network architecture mode, analyze and optimize the loading of equipment, as well as to predict the occurrence of emergencies and to signal the detection of critical errors.
Key words: SNMP, monitoring, agent.

Ivanov V., Patric O. Capacity Twisted Pair of Cable SCS Calculation. – PP. 356–361.
This article is contented calculations methods analysis of twisted pair capacity. Calculations results is compared with measured results of cable SCS category 5e American firm «Siemon».
Key words: Structural cable system, twisted pair capacity, SCS cable category 5e.

Ilina O., Kupchinenko O., Pantyuhin O., Skoropad A. Analysis of Modern Technologies of Building Multiservice Networks. – PP. 361–366.
Technologies ATM, TCP/IP, MPLS, such as IP MPLS, are becoming increasingly popular to build multiservice networks. If this technology IP MPLS find a preferred application on the high-speed backbone networks, and ATM in the access networks, interacting at different levels of the reference model for open systems interconnection and providing the required quality of service.
Key words: multiservice networks, backbone networks, access networks, quality of service.

Ilina O., Kupchinenko O., Pantiuhin O., Skoropad A. Using Model of Rasch to Assess the Quality of Students' Knowledge. – PP. 366–370.
One of the main quality control technologies in education is to test. Currently, statistical testing methods are used most commonly. The article examines the use of the one-parameter Rasch model to assess the effectiveness of tests that show the use of this model for different test items.
Key words: one-parameter model, testing, difficulty task, level of preparedness.

Isakov A., Kovzur M. Deployment of the Certificate Authority on Astra Linux to support PKI. – PP. 371–375.
Currently, Windows operating systems are widely used to support the Public Key Infrastructure in the accredited Certificate 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 the deployment of the CA based on the Astra Linux operating system.
Key words: public key infrastructure, certificate authorities, certificate, *astra linux.*

Kablukov D. Variations Encryption Based on the Cryptogram Taman Shud. – PP. 375–378.
This article discusses option decrypt cryptographic puzzles associated with the murder of an unknown – Taman shud. Analyzed the frequency reference to the letters in the ciphertext and the proposed scenario, as well as evidence and possible murderer. On the basis of the data decryption proposed variations encryption algorithm – a new type of highly resistant creating texts for use in the transmission of messages.
Key words: encryption, cryptography, data protection.

Kanaev A., Lukichev M. Methods of Forming the Routes of Information Transfer in Telecommunications Network. – PP. 379–381.
The issues of flow routing in the telecommunication networks are not simple. Correct routing method provides a more efficient functioning of the telecommunication network. In the proposed approach for obtaining the required number of efficient routes, taking into account the developed procedure routing.
Key words: telecommunication network, multi-choice routing.

Kanaev A., Lukichev M. Model of Distribution of the Traffic in the Next Generation Network, Considering the Support of the Quality of Service Indicators. – PP. 381–383.
Determining values of parameters of telecommunication networks, characterizing the quality of service is a great complexity. Presented in a simulation model of a telecommunication network allows to reproduce the process of its operation and calculate the values of the parameters that are important from the point of view of quality of service
Key words: telecommunications network simulation, routing.

Kirichek R., Savenko M. Design and Research of Model Flying Network Based on UAV`s. – PP. 383–387.
Flying sensor networks are the one of the IoT aplications nowadays. Such networks consists of flying and surface segments. Flying part is formed by UAV`s. They perform experimental research and testing on the model network. The result of such researching can be used in design of the FSN.
Key words: FSN, tests methods, testing.

Kirichek R., Pham V. D. Semantic MQTT-Gateway for LoRaWAN. – PP.387–392.
This paper presents the results of a semantic MQTT gateway for wireless LoRA technology. To conduct the study, a block diagram was developed for the network interaction and a software architecture for the semantic MQTT gateway. As a hardware platform, the Semtech SX1276 module and the Raspberry Pi 3 microcomputer are considered, which receives data from remote LoRa nodes and transmits data to the Internet using the MQTT

protocol. The MQTT protocol is the most widely spread protocol today for Internet of Things devices.. In the course of the experiment, the latency, CPU load and RAM load were determined, which in turn depend on the number of serviced LoRa nodes.
Key words: Internet of Things, protocol, MQTT, LoRa, semantic gateway.

Kiseljov A. Sazonov M. Conceptual going near research of infocommunication network. – PP. 392–397.
Methodological approach of consideration of infocommunication network is in-process presented within the framework of analysis of the systems. Rich in content part of the article is sanctified to opening of informal, rich in content signs of the system: divisibility, integrity, tie-up and nonadditiveness.
Key words: analysis of the systems, approach of the systems, of infocommunication network.

Kislyakov S., Kormanovskaya A. Approach to Implementation the Concept of CEM within the Framework of the Domain Assurance Maps TAM. – PP. 397–401.
Customer Experience Management – a concept that includes a set of methods, processes and technologies that allow monitoring, measure and manage customer experience in the process of customer interaction with the company. One of the most important aspects forming a positive customer experience is the competent organization of processes of interaction with the client at various points of his contact with the company, in particular within the Assurance TAM domain. The report examines the approach to the implementation of the concept of CEM in OSS systems, which belong to the Assurance domain, using the example of the communication operator processes.
Key words: Customer Experience, Customer Experience Management, TAM, OSS/BSS, Assurance.

Kislyakov S., Pletneva N. Interaction Model of Communications Service Provider and IoT Analysis. – PP. 402–405.
This article discusses communication models of IoT and main interaction models of the service provider with IoT environment. Relevance of the subject is determined by smart gadgets popularity boost and lack of processes and basic business model at the IoT market.
Key words: Internet of Things, IoT, communications service provider, business model, monetization, QoS.

Kislyakov S., Savich V. Building Functionality of the Modern Fault Management System Requirements in Telecommunication Networks. – PP. 405–410.
Progress in infocommunication technologies requires new solutions for the troubleshooting at communications networks. The article presents the results of the analysis on FM software and business functions standardized by TM Forum, and identifies new problems in fault management. Based on the analysis were made, the requirements for the functionality of a modern FM system were formulated. There was based on the analysis performed and the system requirements identified, the functional architecture of the complex FM system was proposed for discussion.
Key words: Fault management, troubleshooting, proactive monitoring, functional model

Kobzev, S., Kuleshov A., Ushakov I. Design and Implementation of Prototype System for Centralized Collection, Storage and Processing System Logs. – PP. 410–416.
The article discusses the technology and architectural decisions, based on which we developed a software prototype system for the collection, storage and analysis of telemetric data of various components of information systems and formed the criteria for typical technical problems of a comparative analysis with third-party solutions.
Key words: Elastic Stack, Elasticsearch, Logstash, Kibana, a comparative analysis of the systems of collection, storage and analysis of system logs.

Kozachok A., Kochetkov S. Some Features of the Critical Information Infrastructure Protection. – PP. 416–420.
Recently, the protection of the information on objects of critical information infrastructure is becoming increasingly important. In this paper, the basic normative-legal acts regulating the requirements on security of information processing for such objects, also some peculiarities measures implementation peculiarities of information security of critical information infrastructure objects with respect to real-time systems.
Key words: information security, critical information infrastructure.

Korzhik V., Kropivko I. Experimental Investigation of Stegosystem with Signal Transmission Through Audio Channels with External Noises. – PP. 420–424.
Stegosystem with the use of echo signals transmitting over audio channel in the presence of external acoustic noises is investigated. It is showed that with appropriated stegosystem parameters selection, the embedded information can be reliably extracted even under the conditions when external noises (speech and music) are presented. The distance between transmitter (loud speaker) and receiver(portable microphone) can be taken about 10–30 m. This method can be used in order to transmit secret information during meetings in the open air or for embedding of digital "watermarks" to prevent a pirate copy of musical works.
Key words: stegosystem, echo-signals, cepstral analysis, acoustic noises.

Korolev I., Savkin K., Khatyrev N. Network Protocol Analyzers Calibration by Data Transfer Rate Measurements in Fiber Optic Channel. – PP. 424–429.
Possibility of network protocol analyzer calibration by measurements of data transfer rate in fiber optic synchronous networks was discussed. Relevance of this kind of mesurements were analyzed. Uncertainties occured due to clock recovery devices were studied.
Key words: fiber optic, fiber-optic communication, SDH, data rate.

Koryakin D., Popkov D., Soshnikov I., Stepanova E. The Analysis of Technology Software-Defined Networks. – PP. 429–434.
Software-Defined Networks at the moment are a hot topic on network infocommunication community. The reasons for this purpose a little, and they become more and more every day. The most demanded feature of SDN, is its potential capability to make network directly programmable and to build network completely on the basis of the virtualized devices.
Key words: Software-Defined Networks, virtualization of network devices, OpenFlow.

Koryakin D., Popkov D., Soshnikov I., Stepanova E. Features of use of OpenFlow Technology in Software-Defined Networks. – PP. 434–437.
Development of technologies has resulted in need of processing of large volumes of information. Recently the concept of information processing has changed and the network becomes the main limiter of development of computing systems. The reason is that the network is static. The existing methods of addressing, logical division and ways the configuration of the corresponding equipment in similar networks becomes inefficient. The concept Software-Defined Networks has been developed for the solution of these problems.
Key words: Software-Defined Networks, OpenFlow, out – of – band, in – band.

Kostyrin A., Krasov A. An Overview of the Opportunities of Channel Steganography Based on Network and Transport Layers Protocols of OSI Model. – PP. 437–443.
There is a classification channel (network) steganography on various grounds in this work. Reviewed the feasibility of methods of channel steganography based on the modification of the headers of such protocols as IP, TCP, ICMP. Also, classified and provided information about the appropriateness of a particular method and the difficulty of detection of the fact of information hiding
Key words: channel steganography, information hiding, classification of types of steganography, data transmission network.

Kostyrin A., Krasov A. Implementation of the Method of Channel Steganography Using ICMP Protocol. – PP. 443–448.
In this paper, we consider the practical realization of information hiding in the network Protocol ICMP. Provides information on designed and written for covert remote control of computers, experimental results are presented on remote management computers with concealment of transmitting control data in ICMP Protocol.
Key words: Channel steganography, information hiding, classification of types of steganography, data transmission network.

Krasov A., Lokhanko N., Podolyak R. Protection of the Data Network with OpenDNS Technology. – PP. 448–453.
This article is devoted to OpenDNS technology. The article describes the algorithm of this technology and how it is used to protect the network from various attacks. OpenDNS is a solution that can be used in the network on the "first line of defense". Protection from DNS is a universal way to protect against the fact that the DNS service is one of the fundamental Internet services. The peculiarity of DNS protection is that it does not depend on the port and protocol (http, torrent, ftp, etc.), ie, at the time when a user or an infected computer requests access to a domain, Session, it refers to the DNS.
Key words: network security, OpenDNS, DNS.

Krasov A., Savinov N., Ushakov I. Using Application Centric Infrastructure of Cisco Systems Inc. in modern data center networks. – PP.453–457.
This article provides an overview of Cisco Systems Inc. technology – ACI, used to build data center networks. The principles of the construction of these networks: topology Leaf-and-Spine, hardware and software of the ACI-fabric, the use of APIC controller, policy enforce-

ment, and application profiling. The advantages of the implementation of ACI-fabric from the point of view of information security. The comparison of ACI concept and SDN concept.
Key words: data center, information security, application centric infrastructure ACI, Cisco Systems, ACI-fabric, APIC controller, policy, application profile.

Kuznetsov S., Ostroumov O., Sukhorukova E., Teslya S. The Variant of Information Telecommunication Net Functioning Sustainability Increasing. – PP. 458–463.
The article is dedicated to the telecommunications nets functioning sustainability. The brief analysis of the threats to such nets is carried out and the protection method of the information telecommunication nets logical structure is presented. The variant of the logical structure protection is proposed, which one allows to increase the security and the secrecy of the channels work by means of addresses defining procedure complicating.
Key words: information telecommunication net, lineal systems, sustainability, external threats.

Kuleshov I., Shevchenko V. Interconnected Network Radio, Radio-Relay, Tropospheric and Satellite Communications in the Arctic. – PP. 463–466.
In the article the analysis of factors affecting communication in the Arctic, developed interconnected network radio, radio-relay, tropospheric and satellite communications for the Arctic zone, which can form the basis (as a sample) communication on the island and mainland bases, and made a proposal for the application of advanced Wi-Fi technology.
Key words: Arctic, radio, radio relay, and tropospheric communication, satellite communication, radio on medium and short waves, interconnected network radio, Wi-Fi technology.

Kushnir D., Pavlukovich M. The Method of Protecting Cash Based on Quantum Cryptography. – PP. 467–471.
Today popular paper money. Appeared a necessity to new security conditions for the authenticity of money. Offered a new method based on the principles of quantum cryptography. This article describes the method, analyzes the protection way and considers the links for use.
Key words: quantum banknote, quantum optical money, quantum cryptography.

Kushnir D., Shemyakin S. Reverse Number in Simple Field. – PP. 471–476.
*Asymmetric cryptographic systems require to find the reverse number for **a** in a simple field. The module in a simple field in cryptographic applications is large enough. This leads to the need to consider algorithms that reduce computing costs.*
*We propose a modification of the Euclidean algorithm, does not require a cyclical operations. The algorithm is based on the behavior of residues of multiple serial numbers for **a** and exceeding the module value before to bring the module.*
Key words: asymmetric cryptographic systems, number theory, Euclidean algorithm, finding of reverse number.

Levin M., Fostach E. A Survey of the Protected Access Problem to Cloud Data Storage. – PP. 476–481.
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. Introduction to Secure SCTP. – PP. 481–486.
The Secure SCTP protocol provides transport-level security functions without the need for other security protocols, such as TLS or IPSec. This article can be considered as a brief introduction to the protocol with a view to acquaintance with the new commands necessary for integrating cryptographic functions directly into the basic SCTP protocol.
Key words: SCTP, S-SCTP, Secure SCTP.

Lokhan'ko N., Podolyak R., Ushakov I. The Main Threats Types of Compromotetion of Switch in SDN. – PP. 487–491.
Software-defined Networking – is a new approach to build an architecture of computer networks. It divides network control layer and data transport layer, also it transports network control functions from routers and switches to applications that running on remote server – controller. This article contains an overview of the most common attacks that targets network control channel SDN, targets which hackers wants to achieve and ways to prevent theese threats.
Key words: SDN, dataplane, controlplane, controller.

Lytaev M. On Application of Non-Local Boundary Conditions for Tropospheric Radiowave Propagation Problems. – PP. 491–496.
In this research we are concerned with the method of non-local transparent boundary conditions for the numerical modeling of radiowave propagation near the Earth's surface. A modification of this approach to wide-angle parabolic equation is presented. The considered method does not require manual selection of the artificial parameters depending on the initial data. A comparison analysis with split-step Fourier method is given.
Key words: tropospheric radiowave propagation, inhomogeneous medium, parabolic equation, transparent boundary conditions.

Malykh A., Yurkin D. Probabilistic Approach for Effectiveness Increase in Automated Systems Evaluation for Compliance with Cybersecurity Objectives. – PP. 496–500.
The paper covers issues of effectiveness increase in automated systems evaluation for compliance with cybersecurity objectives. The approach is based on Signal Flow Graphs (SFG). SFG is a tool for analysis and modeling of discrete-time systems. Automated systems compliance with cybersecurity objectives evaluation is modeled. Branches from the graph represent evaluation (tests) and nodes refer to a state of a process (cybersecurity objectives). This ap-

proach is based on function weighting and conversion rule implementation. Average time and evaluation success probability are the factors for effectiveness increase.
Key words: automated systems, cybersecurity, Signal Flow Graph, transition function, course-of-value function, function weighting, path, circuit circle graph conversion.

Makhova I., Potekhin I., Sakharov D. Searching of the Traffic Engineering in the MPLS Networks. – PP. 500–505.
This article is devoted to the technology of MPLS-based traffic engineering. The article discusses methods, tasks and ways to restore traffic. The technology under consideration is relevant at present, since the switching mechanism based on labels is based on the principle of the separation of control functions and packet forwarding, which allows to increase the scaling and speed of the traffic processing.
Key words: MPLS, Traffic Engineering, LSP-tunnel, Virtual Private Network, Routing.

Muthanna A., Khakimov A. Testing of SDN Core on the Basis of Mikrotik Switches. – PP. 505–508.
SDN is the ideology of building networks, in which all the intelligence of the network is placed on a separate hardware / software basis, and all traffic management is based on special protocols (for example, OpenFlow) that operate with the concept of flow and can perform various actions with it Allow, prohibit, redirect, rewrite fields in packages, etc.). In fact, the controller determines the network management policy based on the specified rules, as well as the work of specialized applications (for example, emulating the work of STP or routing protocols). The final result is transferred to the switches via the OpenFlow protocol in the form of flow-tables containing information about where, how and what traffic to transmit. On the one hand, this approach gives more flexibility in network management, on the other hand, greatly simplifies administration, in part, and the architecture of the network. In our work on the basis of the model network SPbGUT raised the network, where the core consisted of three logical switches manufacturer mikrotik supporting the protocol openflow v1.0. Having created a network based on the opendaylight controller, we tested the speed of the switching table for the switches. Operability of the controller for different types of traffic, including for IoT traffic. Also, the controller's behavior was monitored for the operation of the IoTDM service over the SDN network.
Key words: OpenFlow, SDN, mikrotik, switche.

Novikov A., Saltykov A. Dynamic Bandwidth Allocation in PON Networks. – PP. 509–514.
Dynamic bandwidth allocation in passive optical networks presents a one of key issues for providing efficient and fair utilization of the PON upstream bandwidth. In this paper DBA procedure organization was considered within the two major standards for PONs, GPON (ITU-T G.984) and EPON (IEEE 802.3ah).
Key words: DBA, GPON, EPON, ONT, OLT.

Paramonov A., Trinh H. Research of the Impact of Wireless Self-Organizing Networks Parameters on the Quality of Service. – PP. 514–519.
This article presents the main quality of service parameters of traffic in wireless self-organizing networks. Presents analysis of the route length's dependence (by distance and by hop) on the structural parameters BSS based on the developed simulation model

in Mathcad and using the COOJA tool in the operating system Contiki. Also, presents analysis efficiency performance of the protocol RPL in various density of nodes in BSS, using modeling in OS Contiki.
Key words: wireless self-organizing network, route length, Mathcad, operating system Contiki, COOJA, RPL.

Reshetov A., Filippov O., Sterenberg S. Development of System for Modeling Communication Channel in GSM Standard, Based on Arduino and Single-Board Raspberry Computer. – PP. 519–525.
In following article you can see methods for implementing of GSM standard in designed communication channel, based on Arduino microcontrollers and single-board Raspberry computers. The main goal of this scientific work is development of working module for experimental works to ensure information security in GSM standard.
Key words: Arduino, Raspberry, RFID, GSM, information security.

Pestov I., Saharov D., Sergeeva I., Chernoborodov I. The Detection of the Security Threats to Information Systems. – PP. 525–527.
Throughout the history of computer technology, the security of information systems and data warehouses has always been an urgent problem. There are various methods and approaches to assessing the threats of information systems, but it is not always possible to clearly define what needs to be used, since there is no one method that suits all information systems. The paper explores various approaches to assessing threats to information systems, compares methods and describes their application.
Key words: Information security, pentest, analysis, threats, information systems.

Sakharov D., Sergeeva I., Teregulov T. Analysis of Vulnerability of Processes of Information Processing in Government Information Systems. – PP. 528–531.
An overview of potential vulnerabilities affecting the processing of information in government information systems was made. Vulnerabilities were identified, the level of likelihood of implementing the threat was assessed using the appropriate vulnerability. Classification of vulnerabilities is also presented. A private threat model is described, which reflects the possible consequences of the threat
Key words: vulnerability, information security threats, risk analysis, threat model, government information systems.

Tikhonov S. A Universal Method of Protecting Block Ciphers from Side Attacks on Power Circuits. – PP. 531–534.
A new method for protecting hardware-based block ciphers from side-by-side attacks on differential-type power supplies (DPA) is proposed. The cipher algorithm is complemented by two protected transformations: before and after encryption. Due to the simplicity of the transformations, high speed is provided with minimal requirements for additional hardware resources. In this case, the method is universal and is applicable to the protection of any block ciphers.
Key words: secret key, hardware implementation of the cipher, S-box, attack on the power circuit, differential power analysis (DPA).

Fitsov V. DPI System Simulation Model in Omnet++. – PP. 535–539.
This article describes the research questions of the work simulation model of the system DPI. As the simulation environment used Omnet++ software. Simulation model based on the general architecture of the DPI system. The algorithm of the model is given.
Key words: DPI, QoS, Omnet++, queuing system (QS), queuing network, signature.

Chistyakov S., Yakovlev A. Nonlinear Optical Signal Processing in Fiber-Optic Linear Path. – PP. 540–544.
High speed and transmission distance in modern fiber-optic transmission systems can cause distortion of the optical signal, reducing the quality of information transfer. The article considers the mathematical model of the corrector based on nonlinear forming system and the technique of optimizing its coefficients.
Key words: fiber-optic transmission system, digital signal processing, nonlinear correction.

АВТОРЫ СТАТЕЙ

АВРАМЕНКО Владимир Семенович — кандидат технических наук, доцент, профессор кафедры автоматизированных систем специального назначения Военной академии связи имени Маршала Советского Союза С. М. Буденного, vsavr@yandex.ru

АГИЕВИЧ Сергей Николаевич — доктор технических наук, инженер Военной академии связи имени Маршала Советского Союза С. М. Буденного, practicdsv@yandex.ru

АКИШИН Владимир Андреевич — аспирант кафедры инфокоммуникационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, akishin_vova@mail.ru

АЛЕКСАНДРОВА Екатерина Сергеевна — студентка группы ИКТЗ-33 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, meowmewmeowmew@gmail.com

АМЕЛЯНОВИЧ Алексей Вадимович — студент Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, lexer0596@gmail.com

АНДРЕЕВ Владимир Александрович — доктор технических наук, профессор, Президент Поволжского государственного университета телекоммуникаций и информатики, заведующий кафедрой линий связи и измерений в технике связи, andreev@psati.ru

АНДРЕЯНОВ Ярослав Владимирович — студент Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, yaroslav.andreyanov94@gmail.com

АНДРИАНОВ Владимир Игоревич — кандидат технических наук, доцент, профессор кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, vladimir.i.Andrianov@gmail.com

АНИКЕВИЧ Елена Александровна — кандидат технических наук, начальник отдела организации научно-исследовательской работы и интеллектуальной собственности Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, confsut@gmail.com

АНУФРЕНКО Александр Викторович — адъюнкт кафедры «Военные системы многоканальной электрической и оптической связи» Военной академии связи имени Маршала Советского Союза С. М. Буденного, leroi88@mail.ru

АРСАЕВ Ринат Вадимович — оператор научной роты Военной академии связи имени Маршала Советского Союза С. М. Буденного, krickray@gmail.com

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

БАБЫНИН Евгений Сергеевич — курсант Санкт-Петербургского университета государственной противопожарной службы МЧС России, ezemifort@inbox.ru

БЕЛАИДИ Мурад — магистрант кафедры фотоники и линий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, Belaidi.mourad.ru@gmail.com

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

БИРЮКОВ Артём Андреевич — магистрант кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, biryukov.artand@gmail.com

БОБРЕШОВ-ШИШОВ Даниил Игоревич — курсант Военной академии связи имени Маршала Советского Союза С. М. Буденного, dbober94@gmail.com

БУЗЮКОВ Лев Борисович — кандидат технических наук, профессор кафедры программной инженерии и вычислительной техники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, levbuz@mail.ru

БУЛАТОВ Никита Алексеевич — студент группы ИКТЗ-33 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, bulatov.nre@gmail.com

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

БУРДИН Владимир Александрович — доктор технических наук, профессор, проректор по науке и инновациям Поволжского государственного университета телекоммуникаций и информатики, профессор кафедры линий связи и измерений в технике связи, burdin@psati.ru

БУЦЕВ Сергей Федорович — кандидат технических наук, доцент, доцент кафедры «Военные системы многоканальной электрической и оптической связи» Военной академии связи имени Маршала Советского Союза С. М. Буденного, bucev@mail.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

ВАСИЛИШИН Николай Сергеевич — магистрант кафедры защищённых систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, v.ns@hotmail.com

ВАСИЛЬЕВ Евгений Леонидович — начальник лаборатории кафедры «Военные системы многоканальной электрической и оптической связи» Военной академии связи имени Маршала Советского Союза С. М. Буденного, nz_jeck@mail.ru

ВЕРЕМИЙЧУК Иван Юрьевич — студент Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, инженер группы сетей NGN и сетей доступа отдела технической поддержки компании ООО «НТЦ Протей», ourfury.1@gmail.com

ВИКУЛОВ Антон Сергеевич — аспирант кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, asv012016@gmail.com

ВИНТЕНКОВА
Юлия Сергеевна — аспирант кафедры радиоэлектронных и телекоммуникационных систем Института радиоэлектроники и телекоммуникаций Казанского национального исследовательского технического университета им. А. Н. Туполева – КАИ, vintenkova.yulia@gmail.com

ВИТКОВА
Лидия Андреевна — аспирант, ассистент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, lidia@glorystory.ru

ВИХРОВ
Михаил Николаевич — студент Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, moongoose2007@yandex.ru

ВЛАДИМИРОВ
Сергей Сергеевич — кандидат технических наук, доцент кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, vladimirov.opds@gmail.com

ВОЛКОВ
Артем Николаевич — студент Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, v.artem.nikolaevich@yandex.ru

ВОЛКОВ
Иван Александрович — оператор научной роты Военной академии связи имени Маршала Советского Союза С. М. Буденного, Volk165@mail.ru

ВОЛКОГОНОВ
Владимир Никитич — кандидат технических наук, доцент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, vladimir.volkogonov@gmail.com

ВОРОЖБИТОВА
Александра Игоревна — магистрант кафедры инфокоммуникационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, avorozhbitova@gmail.com

ВОРОНЦОВ
Владислав Александрович — старший оператор научной роты Военной академии связи имени Маршала Советского Союза С. М. Буденного, vorontsovbrb@gmail.com

ВЫСОЦКИЙ
Сергей Анатольевич — студент группы ИКТМ-54м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, sa.vysotskiy@gmail.com

ГАГАРИНА Софья Андреевна — студентка группы ИКТО-42 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, sonka1603@mail.ru

ГЕРЛИНГ Екатерина Юрьевна — кандидат технических наук, доцент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, gerlingeu@gmail.com

ГЛАГОЛЕВ Сергей Федорович — кандидат технических наук, доцент, заведующий кафедрой фотоники и линий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, glagolevsf@yandex.ru

ГОЙДЕНКО Владимир Константинович — адъюнкт кафедры технического обеспечения связи и АСУ Военной академии связи имени Маршала Советского Союза С. М. Буденного, lglvl@yandex.ru

ГОЛУБЕВ Артур Петрович — магистрант кафедры программной инженерии и вычислительной техники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, sut@golubev.email

ГОЛУБЕВ Василий Сергеевич — магистрант кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, vas_gol@icloud.com

ГОРЕЛЕНКО Виталий Витальевич — магистрант кафедры инфокоммуникационных сетей Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, titov.vitaliy2014@yandex.ru

ГРИШИН Илья Владимирович — кандидат технических наук, доцент кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, i.v.grischin@gmail.com

ГРОМОВ Владимир Владимирович — студент группы ИКПИ-32 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, gromov@vladimir.one

ГРУЗИНСКИЙ Борис Анатольевич — студент Санкт-Петербургского государственного университета Телекоммуникаций им. проф. М. А. Бонч-Бруевича, gruzinskiy.b@gmail.com

ГУДКОВ
Михаил Александрович — кандидат технических наук, заместитель начальника научно-исследовательского отдела научно-исследовательского центра Военной академии связи имени Маршала Советского Союза С. М. Буденного, vas@mil.ru

ДАО
Чонг Нгиа — аспирант кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, daotn88@mail.ru

ДВОРНИКОВ
Сергей Викторович — доктор технических наук, профессор Военной академии связи имени Маршала Советского Союза С. М. Буденного, practicdsv@yandex.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, доцент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, desnitsky@comsec.spb.ru

ДИНЬ
Чыонг Зюи — аспирант кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, duydt.sut@gmail.com

ДМИТРИЕВА
Екатерина Викторовна — магистрант кафедры защищенных систем связи Санкт-Петербургского государственного университета им. проф. М. А. Бонч-Бруевича, dmitrieva.ekaterina94@gmail.com

ДОЦЕНКО
Сергей Эдуардович — аспирант кафедры фотоники и линий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, 0472895@gmail.com

ДУБРОВИН
Никита Дмитриевич — магистрант кафедры защищённых систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, nikita.dubrovin.dm@gmail.com

ДУДНИКОВА
Мария Николаевна — магистрант кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, dudmashhh@gmail.com

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

ДУРОВ
Лев Юрьевич — студент группы ИКТО-31 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, durov-l@mail.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

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

ЕРМАКОВА
Татьяна Вячеславовна — аспирант кафедры программной инженерии и вычислительной техники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, t.ermakova89@gmail.com

ЖУЛАНОВ
Владимир Борисович — студент Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, exo_tech@mail.ru

ЖУРАВЕЛЬ
Евгений Павлович — кандидат технических наук, главный специалист производственно-научного центра АО «НИИ «Рубин», eshur@rubin-spb.ru

ЖУРКИН
Денис Вячеславович — студент группы ИКТБ-58м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, zhurkindenis@gmail.com

ЗАГОРЕЛЬСКИЙ
Владимир Валерьевич — начальник цикла-старший преподаватель учебного военного центра института военного образования Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, vladimir.zagorelsckij@yandex.ru

ЗАДУРОВА
Анастасия Алексеевна — курсант Санкт-Петербургского университета государственной противопожарной службы МЧС России, ezemifort@inbox.ru

ЗАРУБИН Антон Александрович — кандидат технических наук, доцент кафедры инфокоммуникационных систем, проректор по информатизации Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, azarubin@sut.ru

ЗАХАРОВА Татьяна Евгеньевна — студентка группы ИКБ-31 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, zakharova.tatiana95@gmail.com

ЗИМИН Александр Евгеньевич — магистрант кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, a.zimin@tools4brokers.com

ЗУЕВА Елена Олеговна — магистрант кафедры защищенных систем связи Санкт-Петербургского государственного университета им. проф. М. А. Бонч-Бруевича, zuevaelation94@mail.com

ИВАНОВ Александр Игоревич — магистрант кафедры защищенных систем связи Санкт-Петербургского государственного университета им. проф. М. А. Бонч-Бруевича, ivalex70@gmail.com

ИВАНОВ Василий Геннадьевич — кандидат военных наук, доцент 41 кафедры «Организации связи» Военной академии связи имени Маршала Советского Союза С. М. Буденного, wasj2006@yandex.ru

ИВАНОВ Владимир Степанович — кандидат технических наук, доцент кафедры фотоники и линии связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, vsivanovspb@yandex.ru

ИВАНОВ Сергей Александрович — кандидат технических наук, старший научный сотрудник НИЛ-1 Военной академии связи имени Маршала Советского Союза С. М. Буденного, Volk165@mail.ru

ИЗРАИЛОВ Константин Евгеньевич — ведущий специалист отдела научно-исследовательской работы студентов Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, konstantin.izrailov@mail.ru

ИЛЬИНА Ольга Борисовна — кандидат географических наук, старший преподаватель кафедры автоматизированных систем специального назначения Военной академии связи имени Маршала Советского Союза С. М. Буденного, nastik94@yandex.ru

ИСАКОВ Артём Сергеевич — студент группы ИКТБ-68м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, isakowww@yandex.ru

ИСУПОВА Екатерина Анатолиевна — старший преподаватель кафедры почтовой связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, kat_isupova@list.ru

КАБЛУКОВ Дмитрий Евгеньевич — аспирант кафедры радиолокации и радионавигации Всероссийского научно-исследовательского института радиоаппаратуры, kablokov@gmail.com

КАЗАКОВ Дмитрий Борисович — начальник управления информатизации Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, dkazakov@spbgut.ru

КАНАЕВ Андрей Константинович — доктор технических наук, доцент, заведующий кафедры «Электрическая связь» Петербургского государственного университета путей сообщения Императора Александра I, kanaenak@mail.ru

КИРИЧЕК 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

КИСЕЛЕВ Алексей Алексеевич — кандидат технических наук, доцент, начальник сектора Публичного акционерного общества «Информационные телекоммуникационные технологии», Санкт-Петербург, kiseljovorl@yandex.ru

КИСЛЯКОВ Сергей Викторович — кандидат технических наук, доцент кафедры инфокоммуникационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, s.kislyakov@argustelecom.ru

КОБЗЕВ Сергей Александрович — студент Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, caandspb@gmail.com

КОВАЛЬ
Альбина Рафиковна
главный специалист управления информатизации Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, akoval@sut.ru

КОВЦУР
Максим Михайлович
кандидат технических наук, старший преподаватель кафедры защищенных систем связи, Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, maxkovzur@mail.ru

КОЗАЧОК
Александр Васильевич
кандидат технических наук, сотрудник Академия Федеральной службы охраны Российской Федерации, totrin@mail.ru

КОЗЛОВ
Сергей Владимирович
доктор технических наук, доцент, профессор кафедры радиоэлектронных и телекоммуникационных систем Института радиоэлектроники и телекоммуникаций Казанского национального исследовательского технического университета им. А. Н. Туполева – КАИ, ks16v@yandex.ru

КОПЫТИН
Александр Николаевич
кандидат технических наук, преподаватель кафедры «Военные системы многоканальной электрической и оптической связи» Военной академии связи имени Маршала Советского Союза С. М. Буденного, koputin@list.ru

КОРЖИК
Валерий Иванович
доктор технических наук, профессор кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, val-korzhik@yandex.ru

КОРМАНОВСКАЯ
Анастасия Александровна
студентка Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, Stacy35@mail.ru

КОРОЛЁВ
Иван Станиславович
научный сотрудник лаборатории метрологии малоинтенсивного лазерного излучения и волоконно-оптических систем Всероссийского научно-исследовательского института оптико-физических измерений, korolev@vniiofi.ru

КОРОТКИН
Константин Федорович
студент Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, korotkink@mail.ru

КОРЧАГИН
Мстислав Сергеевич
студент Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, korchagin.mstislav@mail.ru

КОРЯКИН Денис Дмитриевич — командир научного взвода - младший научный сотрудник Военной академии связи имени Маршала Советского Союза С. М. Буденного, koryakinen@gmail.com

КОСОВ Никита Алексеевич — магистрант кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, Kosov.n.a@mail.ru

КОСТЫРИН Алексей Сергеевич — студент Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, alex.kostirin@ya.ru

КОТЕНКО Игорь Витальевич — доктор технических наук, профессор, заведующий лабораторией проблем компьютерной безопасности Санкт-Петербургского института информатики и автоматизации, ivkote@comsec.spb.ru

КОЧЕТКОВ Евгений Викторович — сотрудник Академия Федеральной службы охраны Российской Федерации, mr.Koch91@mail.ru

КРАСОВ Андрей Владимирович — кандидат технических наук, доцент, заведующий кафедрой защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, krasov@inbox.ru

КРОПИВКО Иван Валерьевич — студент группы ИКТБ-58м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ivalkrop@gmail.com

КУЗНЕЦОВ Сергей Иванович — кандидат технических наук, доцент Военной академии связи имени Маршала Советского Союза С. М. Буденного, ksi-2016@yandex.ru

КУЛЕБЯКИНА Ольга Романовна — студентка Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, olgaromanovn@mail.ru

КУЛЕШОВ Артем Андреевич — студент Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, gart9515@gmail.com

КУЛЕШОВ Игорь Александрович — кандидат военных наук, доцент, заместитель генерального директора по научной работе ПАО «Информационные телекоммуникационные технологии», KuL-igor@yandex.ru

КУЛИШКИНА Елена Игоревна — магистрант кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, kulishkina_94@mail.ru

КУПЧИНЕНКО Ольга Павловна — преподаватель кафедры автоматизированных систем специального назначения Военной академии связи имени Маршала Советского Союза С. М. Буденного, k-olga102@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, соискатель Санкт-Петербургского института информатики и автоматизации, laos-82@yandex.ru

ЛЕВИН Марк Вадимович — аспирант кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, m.va.levin@gmail.com

ЛЕЙКИН Антон Владиславович — старший преподаватель кафедры инфокоммуникационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, a.v.leykin@gmail.com

ЛОГИН Элина Валерьевна — ассистент кафедры «Электрическая связь» Петербургского государственного университета путей сообщения Императора Александра I, elinabeneta@yandex.ru

ЛОХАНЬКО Никита Олегович — магистрант кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, byorn.gosu@yandex.ru

ЛЫТАЕВ Михаил Сергеевич — аспирант кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича mikelytaev@gmail.com

МАЛЫХ Алексей Валентинович — магистрант кафедры защищенных систем связи Санкт-Петербургского университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, avmalykh@yandex.ru

МАХОВА Ирина Олеговна — студентка Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, Ira-irk-ira@mail.ru

МИКУТАВИЧАЙТЕ Диана Сергеевна — студентка группы ИКТО-42 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, mikutavichaite@bk.ru

МОСКАЛЮК Алексей Алексеевич — студент Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, aam@amg-spb.ru

МОШКИН Вадим Сергеевич — ассистент кафедры «Информационные системы» Ульяновского государственного технического университета, v.moshkin@ulstu.ru

МУТХАННА Аммар Салех али — кандидат технических наук, ассистент кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ammarexpress@gmail.com

МУХАМЕТШИНА Дина Фаиловна — студентка группы ИКВТ-31 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, undinakamec@gmail.com

НАУМИЧЕВА Дарья Андреевна — студентка ИКТК-36 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, da.sh.a@mail.ru

НИГАМАТУЛЛИН Артем Радикович — оператор научной роты Военной академии связи имени Маршала Советского Союза С. М. Буденного, arnigo2012@mail.ru

НОВИКОВ Александр Владимирович — студент Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, n1aleksandr@yandex.ru

ОНУФРИЕНКО Анастасия Валентиновна — магистрант кафедры инфокоммуникационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, anastasia.4991@mail.com

ОСТРОУМОВ Олег Александрович — кандидат технических наук, преподаватель Военной академии связи имени Маршала Советского Союза С. М. Буденного, oleg-26stav@mail.ru

ОСТРОУЩЕНКО Николай Александрович — студент группы ИКТЗ-61М Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, kolyaostr22@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 автоматизированных систем специального назначения Военной академии связи имени Маршала Советского Союза С. М. Буденного, 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

ПАТРИК Олег Гарриевич — кандидат технических наук, доцент кафедры фотоники и линии связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, oleg.patric@gmail.com

ПЕСТОВ Игорь Евгеньевич — старший преподаватель кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, pestovie@outlook.com

ПЕТРОВА Айаана Николаевна — магистрант кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, Ayaana95@mail.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

ПОЛЯКОВА Елена Валерьевна — старший преподаватель кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, e.v@inbox.ru

ПОПКОВ
Дмитрий Васильевич
старший оператор научной роты Военной академии связи имени Маршала Советского Союза С. М. Буденного, dpopkov1994@mail.ru

ПОПОВА
Светлана Сергеевна
магистрант кафедры фотоники и линий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, svetochka.popova@mail.ru

ПОТЕХИН
Игорь Юрьевич
кандидат математических наук, заместитель руководителя Управления Роскомнадзора по Северо-Западному федеральному округу, I.Potehin@rkn.gov.ru

ПРЯЖНИКОВ
Владимир Сергеевич
студент группы ИКТМ-54м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, avyeloc1@gmail.com

РЕШЕТОВ
Алексей Юрьевич
Студент Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, alexey.reshetov.rc@gmail.com

РОМАНОВА
Ольга Дмитриевна
студентка Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, romashka1804@yandex.ru

РЯБОВ
Евгений Юрьевич
студент Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, ev.ryabov.mail@ya.ru

РЯБОВА
Ольга Николаевна
консультант отдела Управления Роскомнадзора по Северо-Западному федеральному округу, ebolshinova@yandex.ru

САВЕНКО
Максим Игоревич
студент группы ИКТИ-53м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, maxivast@gmail.com

САВИНОВ
Никита Владимирович
студент Санкт-Петербургского государственного университета телекоммуникаций им. М. А. Бонч-Бруевича, nick.cavin191@gmail.com

САВИЧ
Валерий Владиславович
студент Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, инженер группы контроля качества ООО «НТЦ АРГУС», v.savich@argustelecom.ru

САВКИН Константин Борисович — кандидат технических наук, начальник лаборатории метрологии малоинтенсивного лазерного излучения и волоконно-оптических систем Всероссийского научно-исследовательского института оптико-физических измерений, savkin@vniiofi.ru

САЕНКО Игорь Борисович — доктор технических наук, профессор, ведущий научный сотрудник лаборатории проблем компьютерной безопасности Санкт-Петербургского института информатики и автоматизации, ibsaen@comsec.spb.ru

САЗОНОВ Михаил Александрович — кандидат военных наук, доцент, начальник кафедры военных систем космической, радиорелейной, тропосферной связи и навигации Военной академии связи имени Маршала Советского Союза С. М. Буденного, masazonov@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 — студентка Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, sk_evgeniya@mail.ru

СЕВИДОВ Владимир Витальевич — преподаватель Военной академии связи имени Маршала Советского Союза С. М. Буденного, practicdsv@yandex.ru

СЕРГЕЕВА Инна Юрьевна — аспирант кафедры безопасности информационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, Sergeeva501@yandex.ru

СКОРОДУМОВ Сергей Андреевич — студент Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, serge.a.skor@mail.ru

СКОРОПАД Александр Витальевич — ведущий инженер-электроник НИЛ №4231, НИО №423, НТЦ №42 Санкт-Петербургского филиала «Ленинградское отделение научно-исследовательского института радио» (Филиал ФГУП НИИР-ЛОНИИР), sav01236@yandex.ru

СОРОКИН Владимир Андреевич — студент группы ИКТМ-54м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, vildam29@gmail.com

СОШНИКОВ Игорь Олегович — старший оператор научной роты Военной академии связи имени Маршала Советского Союза С. М. Буденного, BRG1218@gmail.com

СТЕПАНОВА Елена Александровна — адъюнкт НИЦ Военной академии связи имени Маршала Советского Союза С. М. Буденного, stepanovaelena-86@mail.ru

СУХОРУКОВА Елена Валерьевна — кандидат технических наук, старший преподаватель Военной академии связи имени Маршала Советского Союза С. М. Буденного, sukhorukova_lena@mail.ru

ТАМПИО Анна Владимировна — студентка группы ИКТУ-37 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, tampio.anna@mail.ru

ТЕРЕГУЛОВ Тимур Радикович — магистрант кафедры безопасности информационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, teregulov.t.r@yandex.ru

ТЕСЛЯ Сергей Петрович — старший преподаватель Военной академии связи имени Маршала Советского Союза С. М. Буденного, ksi-2016@yandex.ru

ТИХОНОВ Сергей Викторович — аспирант кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, tikhonovc@yandex.ru

ТИХОНОВА Эльвира Никитична — магистрант кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, miss.tiny@mail.ru

ТРЕСКИН Никита Леонидович — магистрант кафедры безопасности информационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, PzFireFly@gmail.com

УШАКОВ Игорь Александрович — старший преподаватель кафедры защищённых систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ushakovia@gmail.com

ФАМ Ван Дай — студент Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, daipham93@gmail.com

ФЕДОРЧЕНКО Андрей Владимирович — аспирант, младший научный сотрудник Санкт-Петербургского института информатики и автоматизации Российской академии наук, fedorchenko@comsec.spb.ru

ФИЛИППОВ Алексей Александрович — кандидат технических наук, доцент кафедры «Информационные системы» Ульяновского государственного технического университета, al.filippov@ulstu.ru

ФИЛИППОВ Олег Борисович — студент группы ИКБ-31Санкт-Петербургского государственного университета им. проф. М. А. Бонч-Бруевича, fil9bob@gmail.com

ФИЦОВ Вадим Владленович — старший преподаватель кафедры инфокоммуникационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, noldi@bonch-ikt.ru

ФОСТАЧ Елена Сергеевна — студент Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, elena.fostach@gmail.com

ФРОЛОВА Юлия Аркадьевна — студентка Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, fr95juli@mail.ru

ХАКИМОВ Абдукодир Абдукаримович — студент Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, abdukadir94@mail.ru

ХАТЫРЕВ Николай Петрович — кандидат технических наук, начальник сектора лаборатории метрологии малоинтенсивного лазерного излучения и волоконно-оптических систем Всероссийского научно-исследовательского института оптико-физических измерений, khatierev@vniiofi.ru

ХРИЧКОВ Валентин Александрович — преподаватель кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, hrichkovv@gmail.com

ЦАРЕГОРОДЦЕВ Андрей Владимирович — магистрант группы ИКТФ-51м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, northsouth1704@gmail.com

ЦВЕТКОВ Александр Юрьевич — старший преподаватель кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, alexander.tsvetkov89@gmail.com

ЧЕКАЛОВ Александр Александрович — студент Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, alexch.spb@yandex.ru

ЧЕРНОБОРОДОВ Иван Сергеевич — магистрант кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, skich1984@gmail.com

ЧЕЧУЛИН Андрей Алексеевич — кандидат технических наук, доцент, старший научный сотрудник Санкт-Петербургского института информатики и автоматизации Российской академии наук, chechulin@comsec.spb.ru

ЧИНЬ Ба Хуи — магистрант кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, trinhbahuy.telecom@gmail.com

ЧИСТЯКОВ Сергей Владимирович — кандидат технических наук, доцент кафедры многоканальной электросвязи Академии Федеральной службы охраны Российской Федерации, chis_serg@mail.ru

ЧМУТОВ Михаил Валериевич — студент Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, frost32.ru@yandex.ru

ШАШКИН Владислав Сергеевич — студент группы ИКБ-31 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, penb69@gmail.com

ШЕВЧЕНКО Василий Васильевич — кандидат военных наук, доцент, начальник лаборатории ПАО «Информационные телекоммуникационные технологии», Vasily.Shevchenko2014@yandex.ru

ШЕМЯКИН Сергей Николаевич — кандидат технических наук, доцент кафедры защищённых систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, S4421764@yandex.ru

ШТЕРЕНБЕРГ Станислав Игоревич — аспирант кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, sterenberg.stanislaw@yandex.ru

ЭКОНОМ Виталий Пантелеевич — старший научный сотрудник Военного учебно-научного центра Военно-Морского Флота «Военно-морская академия им. Адмирала Флота Советского Союза Н. Г. Кузнецова», practicdsv@yandex.ru

ЮРКИН Дмитрий Валерьевич — кандидат технических наук, доцент кафедры защищенных систем связи Санкт-Петербургского университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, dvyurkin@yandex.ru

ЯКОВЛЕВ Алексей Викторович — кандидат технических наук, старший преподаватель кафедры многоканальной электросвязи Академии Федеральной службы охраны Российской Федерации, chis_serg@mail.ru

ЯКОВЛЕВ Виктор Алексеевич — доктор технических наук, профессор кафедры защищенных систем связи Санкт-Петербургского государственного университета им. проф. М. А. Бонч-Бруевича, viyak@bk.ru

ЯЛУНИНА Татьяна Рудольфовна — студентка группы ИКТО-31 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, rudanichek@yandex.ru

АВТОРСКИЙ УКАЗАТЕЛЬ